La Quadrature du Net

Projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024 :

dossier d'analyse de la vidéosurveillance automatisée

Version du 21 janvier 2023

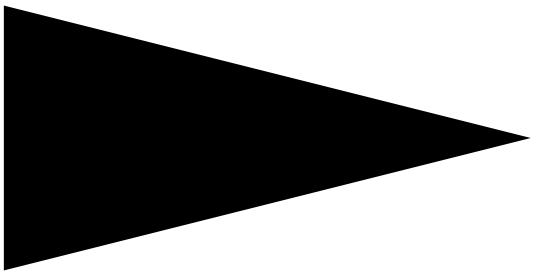

Table des matières

Introduction

Le projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 que vous allez examiner contient un article 7 visant à légaliser – via un cadre dit « d'expérimentation » - le déploiement et la mise en œuvre des dispositifs de vidéosurveillance automatisée (ou algorithmique — VSA).

La présente note vise à fournir à l'ensemble des parlementaires des ressources et informations techniques et juridiques, ainsi qu'un état des lieux du contexte économique et politique dans lequel les technologies de vidéosurveillance automatisée s'insèrent, **afin que vous puissiez appréhender concrètement leur fonctionnement et prendre l'entière mesure des graves conséquences qu'elles ont et auront dans un régime dit démocratique.**

Depuis plusieurs années, dans le cadre d'une initiative appelée « Technopolice », La Quadrature du Net documente l'installation des technologies sécuritaires dans l'espace public. Ce travail s'est rapidement concentré sur la vidéosurveillance automatisée, celle-ci faisant l'objet d'un déploiement fulgurant dans les villes de France en dépit de leur illégalité. Cette note est donc en grande partie le fruit de cette documentation commencée en 2019.

Au préalable, il convient de revenir brièvement sur le contexte dans lequel le gouvernement choisit de proposer d'ancrer durablement ces technologies. En effet, le choix des Jeux Olympiques et Paralympiques de 2024 n'est pas anodin. Le milieu de la recherche observe et analyse depuis longtemps les Jeux Olympiques comme un « méga-évènement » qui, par sa dimension exceptionnelle, permet la mise en œuvre et l'accélération de politiques tout aussi exceptionnelles. Ces évènements créent un terrain pour des innovations législatives et les lois accompagnant les Jeux Olympiques concernent le plus souvent la mise en œuvre d'un maintien de l'ordre strict, une militarisation de l'espace public et l'intensification des mesures de surveillance[1].

1 Matheus Viegas Ferrari, 2022, « *Test, swarm, normalize: how surveillance technologies have infiltrated Paris 2024 Olympic Games*» accessible sur https://www.scielo.br/j/cm/a/zcKnN9ChT9Wqc4hfGWKSk4d/?lang=en

Ainsi, pour le professeur Philip Boyle, spécialiste des “Olympic Studies”, les Jeux Olympiques incarnent un « spectacle de sécurité »[2]. Le chercheur Jules Boykoff[3] compare quant à lui ce phénomène d'accélération législative à la « théorie du choc » dégagée par Naomi Klein où les gouvernement utilisent une catastrophe ou un trauma social pour faire passer des mesures basées sur la privatisation et la dérégulation, là où il n'y en avait pas auparavant. Ce chercheur analyse ainsi les Jeux Olympiques comme un accélérateur de politiques exceptionnelles, mais cette fois-ci en prenant appui sur un moment de fête ou de spectacle, par essence « extra-ordinaire », où les règles politiques peuvent être temporairement suspendues, pour faire progresser des politiques qui auraient été impossible à mettre en place en temps normal.

Ainsi, à titre d'exemple, le gouvernement brésilien a utilisé les Jeux olympiques de 2016 à Rio pour mener des opérations[4] quasi militaires/violentes dans les favelas ou expulser[5] expulser des personnes de leur logement. De la même manière, pour les Jeux olympiques de Tokyo, le gouvernement japonais a utilisé cet évènement pour faire passer une loi « anti-conspiration »[6] qui était en réalité voulue de longue date, les gouvernements nippons successifs ayant auparavant tenté à trois reprises de faire adopter une législation analogue. Cette loi a été très critiquée[7], notamment par les Nations Unies, au regard des atteintes aux libertés qu'elle créait et aux pouvoirs de surveillance qu'elle conférait à l'État.

En parallèle, les méga-évènements sportifs sont qualifiés de « vitrines sécuritaires »[8] ou de « catalyseurs de l'action publique en matière de sécurité numérique »[9] par le milieu académique. Ils permettent d'une part d'être des moments de **laboratoire** et **d'expérimentation** des technologies et, d'autre part, de jouer sur ce moment exceptionnel pour atténuer les mesures de surveillance **et les rendre plus acceptables**. Ainsi, les Jeux Olympiques per-

2 Références dans l'article précité de Matheus Viegas Ferrari : BOYLE, P. (2012). “*Securing the Olympic Games: exemplifications of global governance” et LENSKYJ, H.; WAGG, S. (orgs.):«The Palgrave Handbook of Olympic Studies*». Londres, Palgrave MacMillan.

3 Jules Boykoff, Les Jeux Olympiques, le capitalisme de fête et la réponse des activistes, accessible sur https://saccage2024.noblogs.org/files/2021/07/boykoff-v5.pdf

4 Huffington Post, « *Jeux Olympiques de Rio 2016: Quand le Brésil "pacifie" ses favelas, cela n'a rien de pacifique* », publié le 1er août 2016 et consultable ici https://www.huffingtonpost.fr/actualites/article/jeux-olympiques-de-rio-2016-quand-le-bresil-pacifie-ses-favelas-cela-n-a-rien-de-pacifique_82336.html

5 Le Monde, « *A un an des JO, Rio rase ses favelas indésirables* », publié le 28 juillet 2015 et accessible à https://www.lemonde.fr/ameriques/article/2015/08/04/a-un-an-des-jeux-olympiques-rio-rase-ses-favelas-indesirables_4711093_3222.html

6 Les Echos, « *Le Japon adopte une loi sécuritaire controversée* », publié le 16 juin 2017 et accessible à https://www.lesechos.fr/2017/06/le-japon-adopte-une-loi-securitaire-controversee-172489

7 Challenges, « *Adoption au Japon d'une loi anti-conspiration très critiquée* », publié le le 15 juin 2017 et accessible à https://www.challenges.fr/monde/adoption-au-japon-d-une-loi-anti-conspiration-tres-critiquee_480340

8 Références dans l'article précité de Matheus Viegas Ferrari : Bennett, C. J. et Haggerty, K. D. (dir.). 2011. « *Security Games. Surveillance and Control at Mega-Events* », New York : Routledge

9 Myrtille Picaud, « *Les grands événements, olympiades de la sécurité urbaine numérique ?* », accessible sur https://metropolitiques.eu/Les-grands-evenements-olympiades-de-la-securite-urbaine-numerique.html

mettent d'accompagner et légitimer une « exceptionnalité » à travers leur dimension hors du temps. Ce processus permet aux gouvernements des pays hôtes de capitaliser sur la nouveauté pour eux-même innover légalement et techniquement, et ainsi étendre et normaliser cette « exception » dans une temporalité plus longue, notamment à travers la notion d'héritage des jeux[10].

La demande d'« expérimentation » de la vidéosurveillance automatisée présente à l'article 7 du projet de loi que vous allez étudier répond exactement à ce schéma. Alors qu'aucune documentation publique et scientifique n'existe sur l'efficience de cette technologie, ces dispositions ne font que s'insérer dans un projet politique plus large de développement et de pérennisation de ces dispositifs de VSA. Ce projet est matérialisé par la volonté exprimée depuis plusieurs années par le secteur industriel, les institutions policières et les politiques publiques de recherche d'utiliser massivement ces dispositifs à l'occasion des Jeux Olympiques. Nous reviendrons sur les limites techniques et politiques qu'implique une « expérimentation » mais, au-delà des volontés précitées, **il est parfaitement clair que si cette technologie est légalisée au travers du projet de loi qui vous est soumis, elle ne sera pas abandonnée après 2025.** L'histoire législative récente illustre parfaitement le caractère fallacieux de ces « expérimentations » de papier : nous pourrions évoquer l'exemple de la pérennisation des « boites noires » en matière de renseignement (article L. 851-3 du code de la sécurité intérieur) ou celle des mesures d'état d'urgence, mesures sécuritaires censées être initialement temporaires et exceptionnelles et systématiquement inscrites dans le droit commun par la suite.

Une fois ces éléments de contexte posés, il faut donc voir les dispositions de l'article 7 dans leur essence : un tremplin juridique opportuniste pour rendre durable l'utilisation de la vidéosurveillance automatisée qui transforme drastiquement les pratiques de surveillance policière et marque un véritable passage à l'échelle répressif. Ce projet inscrit la France dans les premiers pays du monde à adopter ces outils en embrassant une fuite en avant dans le solutionnisme technologique sécuritaire.

Nous appelons donc le Parlement à jouer pleinement son rôle de garde-fou démocratique et à prendre connaissance de la réalité de ces technologies, afin de rejeter l'article 7 du projet de loi.

10 Article de Matheus Viegas Ferrari, précité

I. Qu'est ce que la VSA techniquement :

A. Définitions

De quoi s'agit-il lorsqu'on parle de vidéosurveillance algorithmique ? Techniquement, il s'agit de **l'automatisation du travail d'analyse des images de vidéosurveillance grâce à un logiciel qui se charge de produire des notifications lorsque qu'il détecte un événement qu'on l'a entraîné à reconnaître**. Ce travail d'analyse était jusque là effectué par des humains (des agents municipaux dans les centre de supervision urbain (CSU) dans le cas des caméras de vidéo surveillance publiques ou des agents de sécurité privée dans les supermarchés et autres établissements privés). Ces logiciels sont basés sur des algorithmes dits de «computer vision» (vision assistée par ordinateur), une technologie basée sur l'apprentissage statistique permettant d'isoler des informations signifiantes à partir d'images fixes ou animées. Pour parvenir à isoler ces informations, les **algorithmes sont entraînés à détecter automatiquement, à partir des flux vidéos issus des caméras de vidéosurveillance**, certaines catégories d'objets (une valise, des ordures), de **personnes** (personnes allongées sur le sol, graffeurs, personnes statiques) ou d'**événements** (franchissement d'une ligne).

Ainsi, selon la CNIL, la « *vidéo augmentée désigne ici des dispositifs vidéo auxquels sont associés des traitements algorithmiques mis en œuvre par des logiciels, permettant une analyse automatique, en temps réel et en continu, des images captées par la caméra.* ».

Aussi appelée vidéosurveillance « intelligente » ou « augmentée », nous préférons pour notre part les termes de vidéosurveillance « algorithmique » ou « automatisée » (VSA). Les usages de ces logiciels qui permettent d'analyser automatiquement des flux vidéos sont très diversifiés et vont de la « détection de comportement suspect », au « maraudage » (le fait d'être statique dans l'espace public), en passant par le « dépassement d'une ligne ou d'un périmètre » par des individus, le suivi et l'identification de personnes via ses caractéristiques physiques et vestimentaires, la détection d'objet abandonné, d'une bagarre, d'un vol, le comptage de foule ou la détection de regroupements de personnes.

Grâce à cette capacité de classification d'objets, de personnes ou de situations en catégories, les logiciels de VSA proposent différents types de fonctionnalités. Les deux fonctionnalités les plus mises en avant sont la production d'alerte en temps réel, l'automatisation de recherche et de « résumés vidéo » a posteriori dans les archives vidéos :

- les alertes « en temps réel », à destination des policiers en poste au CSU, permettent à une plus petite équipe de visionner une grande quantités de flux vidéos : le logiciel relève de manière automatique des situations perçues comme suspectes ou risquées et notifie les agents.

- s'il est très facile d'effectuer une recherche dans un document texte, la tâche s'avère plus compliquée lorsqu'il s'agit d'effectuer une recherche dans un flux vidéo. La VSA permet l'automatisation des recherches dans des archives vidéo. Cela consiste à lancer des requêtes de reconnaissance d'image afin de faire remonter l'ensemble des bandes vidéos correspondant à certains critères thématiques : par exemple l'ensemble des hommes portant un t-shirt jaune et un pantalon noir repérés dans une zone géographique donnée durant les dernières 24h.

- Visionner des vidéos est long et chronophage pour la police (par exemple dans le cadre de ses enquêtes). Un des usages de la VSA particulièrement mis en avant est celui permettant de condenser des heures ou des jours de vidéos en quelques minutes. Le rôle de la VSA dans cet usage est de sélectionner les passages susceptibles d'intéresser la police et de faire ellipse sur le reste du temps de vidéo.

Certains acteurs sont tentés de faire une distinction entre **les usages en direct de la VSA et les usages a posteriori** (c'est une distinction notamment mise en avant par la CNIL dans sa position sur les caméras augmentées). **Cette distinction n'a pas lieu d'être d'un point de vue technique** car les spécificités (les réglages des algorithmes) menant les logiciels de VSA à prendre des décisions telles que : isoler un « événement suspect » en direct pour envoyer une notification aux agents de CSU, ou isoler un « suspect » a posteriori dans le cadre d'une recherche ou pour l'intégrer dans un « résumé » vidéo sont strictement similaires.

À titre d'exemple, voici les évènements dont la détection est prévue par différents projets de vidéosurveillance automatisée.

- Extrait du manuel de la société Briefcam :

Filtre appliqué	Objets de cas inclus
Plage horaire	Objets correspondant à des plages horaires spécifiques.
Source	Objets provenant de synopsis vidéo spécifiques (si aucune source n'est sélectionnée, les objets de toutes les sources seront affichés).
Classe	Objets correspondant aux classes suivantes : Personnes : homme, femme, enfant. Véhicules deux roues : vélo, moto. Autres véhicules : voiture, pickup, camionnette, camion, autobus, train, avion, bateau. Animaux : chien, chat, oiseau, cheval.
Attributs	Objets ayant les attributs suivants : Sacs : sacs à dos, sacs à main. Chapeaux : avec ou sans chapeaux. Vêtements - haut : manches courtes / sans manches, manches longues. Vêtements - bas : long, court.
Couleur	Objets correspondants à n'importe quelle combinaison de marron, rouge, orange, jaune, vert, vert clair, cyan, violet, rose, blanc, gris et noir.
Taille	Objets correspondants à une plage de tailles d'histogramme.
Vitesse	Objets correspondants à une plage de vitesses d'histogramme.
Maraudage	Objets ayant maraudé pendant une période spécifiée par l'utilisateur ou plus.
Direction	Objets s'étant déplacés dans une direction spécifiée.

- Extrait du marché public conclu avec la ville de Vannes :

3.12.2 Identification « Piétons »

L'expérimentation a pour objet, pour les piétons, leur identification, leur classification et le comptage selon les types reconnus parmi les métadonnées suivantes :

- Taille et forme du corps ;
- Habillements (écharpe, gants, chapeau, couleur du haut, couleur du bas, chaussure, etc.) ;
- Equipements associés (sac, parapluie, cartable, etc.) ;
- Comportemental (marchant, courant, debout, assis, baissé, accroupi, etc.)

Elle sera à mettre en œuvre sur le port de Vannes, place Gambetta qui est aujourd'hui équipée d'un mât.

Pour cette expérimentation, il est souhaité par la ville de Vannes le prêt des fournitures sur une durée d'au moins 3 mois.

A l'issue, la ville de Vannes se réserve le droit de ne pas déployer la solution.

CR 15	Le soumissionnaire détaillera les fonctionnalités offertes par la solution d'IA proposée pour la reconnaissance des piétons, indiquera les limites fonctionnelles, si celle-ci est conforme aux profils T&M du standard OnVif et précisera les fournitures mises en œuvre pour la réalisation de cette expérimentation. Par ailleurs, il devra être également présenté le mode économique pour l'acquisition de la solution et notamment les descriptifs exhaustifs des matériels et des licences associées.

- Extrait du programme fonctionnel technique accompagnant le marché public de la ville de Marseille

Les fonctionnalités :

Fonctionnalités	Événements/Objectifs
Analyse de scène statique	• Objets abandonnés • Individu au sol • TAG • Dépose sauvage d'ordures • Vol/Disparition/Destruction de mobilier urbain
Comptage de personnes/véhicules	
Détection périmétrique	• Franchissement de ligne/zone • Présence sur zones
Analyse de densité de foule	• Regroupements • Attroupement • Surveillance de manifestation sur jauge ..

Fonctionnalité	Événements/Objectif
Détection sonore	• Explosion • Coup de feu • Clameur de foule / Cris
Reconstitution d'événements (différé)	• Reconstituer le parcours d'un individu ou d'un véhicule à partir des archives de plusieurs caméras
Comportements anormaux	• Bagarre / Rixe • Maraudage • Agression
Lecture de plaques immatriculation LAPI / RAPI	• Recherche de véhicules sur critère minéralogique

B. Comment fonctionnent ces algorithmes ?

Dans cette partie, nous allons détailler la construction et le fonctionnement des algorithmes utilisés pour faire de la VSA, d'abord en mettant en exergue les choix politiques qu'impliquent la fabrication et l'usage de tels logiciels (1) et ensuite en identifiant les contraintes imposées par la complexité et l'état de l'art de ces technologies (2).

1. Les choix politiques que nécessitent la construction d'un algorithme de VSA

Cette partie a été rédigée avec la participation de l'ingénieur-chercheur Julien Girard.

Au préalable, il convient de noter que la notion de « **traitement algorithmique** » - utilisée à l'article 7 du projet de loi - recouvre un très vaste champ de techniques allant de calculs statistiques simples comme une régression linéaire, à des opérations très complexes utilisant de nombreuses couches de calculs.
Les algorithmes ayant pour but de reconnaître une information sur une image sont généralement basés sur de **l'apprentissage automatique**, aussi appelé « **machine learning** ». Ces techniques recouvrent des réalités différentes en matière de collecte et utilisation de données, mais surtout de la maîtrise de l'exploitation de ces données comme nous allons le voir.

Les vidéos sont constituées de successions d'images définies par une quantité plus ou moins grande de pixels de couleurs. **Pour pouvoir faire de la reconnaissance sur ces flux vidéos, il convient de traduire ces informations** (nombre de pixels, position, couleur et leurs évolutions dans le temps) **en informations statistiques plus intelligibles et manipulables qu'on appelle caractéristiques.** Imaginons que l'on veuille trouver les éléments les plus probables dans l'image d'un chat.

Le statisticien (ou le programme, de manière autonome) va alors analyser et identifier des caractéristiques spécifiques aux images de chats (ces caractéristiques spécifiques peuvent être les mêmes que celles qui permettent aux humains de reconnaître un chat en repérant, par exemple des moustaches ou des oreilles pointues, mais il peut aussi s'agir d'autres caractéristiques moins perceptibles pour les humains mais plus faciles à identifier via des calculs, comme par exemple le contraste entre les pixels produits par un pelage, voire des caractéristiques complètement impossibles à identifier en tant qu'humain, ou des éléments qui ne sont pas du tout liés à ce qu'on pensait : par exemple un fond toujours de la même couleur pour des images de chats d'une même race. Plus on a de caractéristiques pertinentes, plus le modèle statistique sera précis.

La délimitation des caractéristiques n'est effectuée par un humain que dans des cas relativement simples, le cas de la reconnaissance biométrique automatique est quant à lui assez compliqué. Dans ce cas, c'est souvent le programme qui extrait des caractéristiques pertinentes pour l'accomplissement d'une tâche.

Pour avoir une meilleure compréhension des enjeux de l'usage de l'intelligence artificielle dans le cadre de la VSA, **commençons par décrire les différentes phases qui mènent à la mise en place d'une telle technologie** :
- le choix du jeu de données et de la labellisation (a)
- le choix définitif des caractéristiques du modèle de l'algorithme et la phase d'apprentissage (b)
- le choix d'utiliser cet algorithme à des fins particulières (c)

Il est important de noter que chacune de ces étapes représente des choix et que chacun de ces choix auront des conséquences sur le fonctionnement final de la technologie. Cela aura donc une conséquence sur les événements notifiés aux agents dans les CSU ou sur les événements mis en avant lors de la production d'un « résumé » vidéo utilisé dans le cadre d'une enquête policière.

Dans chacune des parties qui vont suivre, il sera donc important de garder à l'esprit la question : qui fait ces choix ? pourquoi ?

a. Choix du jeu de données et de la labellisation

- **Choix du jeu de données**

L'entraînement d'un algorithme nécessite une très grande quantité de données. Pour reconnaître un chat, il faut non seulement une grande quantité d'images de chats, mais aussi d'autres images (par exemple de tigres, de chiens etc) car pour savoir ce qu'est un chat, l'algorithme doit connaître également ce qui n'en est pas un. Entraîner un algorithme de computer vision de manière efficace exige donc **un gros volume d'images**.

Un principe central dans dans le droit des données personnelles est le **principe de minimisation** : lorsque l'on collecte des données on doit veiller à ce que celles-ci soient nécessaires et à en collecter le moins possible. **L'entraînement des algorithmes de machine learning nécessitant de gros jeux de données, il entre en contradiction avec ce principe fondamental de minimisation.**

D'après l'article 7 du projet de loi, les données doivent « *demeurer accessibles et être protégées tout au long du fonctionnement du traitement* ». Il est très compliqué d'assurer la protection des données personnelles. C'est pour cela qu'est prévu le principe de minimisation des données. Prévoir une disposition qui exige à la fois leur protection et leur accessibilité est un non-sens car le seul moyen de protéger efficacement une donnée personnelle

est de la supprimer dès que cela est possible. On verra cependant dans le **3.** ci-après que supprimer les données personnelles après l'entraînement de l'algorithme ne suffit pas pour autant forcément à protéger ces mêmes données.

Pour la vidéosurveillance automatisée, **ce sont donc des millions d'heures d'images de personnes et donc de traitements de données personnelles qui doivent être collectées, rassemblées et traitées pour entraîner les algorithmes**. Les images sur lesquelles sont entraînés les algorithmes doivent être aussi diversifiées que les images auxquelles les algorithmes seront effectivement exposées. Dans le cas de la VSA, il s'agit donc des flux vidéos de lieux publics ou privés. Ces données seront utilisées pour définir le modèle même si elles ne sont pas concernées par l'objet que l'on cherche (les images de cyclistes sont nécessaires pour apprendre aux modèles qu'il ne s'agit pas de personnes en trottinette).

Le choix du jeu de données influence fortement les décisions finales de l'algorithme. Deux jeux différents produiront des résultats différents. La construction du jeu de données est faite par l'activité humaine et reproduit donc les choix effectués par les humains par le passé. Dans le cas du logiciel COMPAS[11] utilisés par certaines polices américaines, l'objectif était de détecter les possibilités de récidives en fonction des éléments d'un dossier policier. Le programme avait appris sur un jeu de données qui embarquait les décisions racistes du dispositif de police américain concerné, et avait déduit qu'une des caractéristiques principales liée à la récidive était la couleur de peau. Le choix d'utiliser un jeu de données contenant des décisions prises par des humains vient valider ces décisions et les inscrire dans le programme. **Le fait de graver ces décisions politiques dans le marbre en choisissant un jeu de données représente un choix comparable à l'action du législateur.**

Labellisation

Il existe différentes manières d'entraîner un algorithme. Lorsque l'on cherche à reconnaître un chat, nous sommes dans une logique de classification. La méthode employée est alors celle de **l'apprentissage supervisé**. Pour cela, on fournit un jeu de données dites « labellisées », c'est-à-dire que chaque image a préalablement été observée par un œil humain qui a déterminé si oui ou non l'image représente un chat.
À partir de ces jeux de données, l'algorithme choisit lui-même les éléments lui permettant de savoir avec le plus de précision si l'image représente bien un chat en établissant des corrélations : par exemple, il repère la forme créée par l'enchaînement de pixels permettant d'identifier une forme d'oreille de chat.

11 « *How We Analyzed the COMPAS Recidivism Algorithm* », Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, Mai 2016 https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

La labellisation est une étape importante politiquement car c'est un moment d'intervention humaine : dans le cas d'une image de chat, l'enjeu politique est faible, mais lorsqu'il s'agit de labelliser un comportement délictuel, ou nécessitant l'intervention de la police **la labellisation est comparable à l'action d'un juge.**

b. Choix définitif des caractéristiques du modèle de l'algorithme et phase d'apprentissage

L'apprentissage est la procédure qui vise à faire converger le programme d'un état initial vers un état final. Pour ce faire, il faut définir une fonction mathématique qui décrit l'erreur que fait le logiciel; des algorithmes dits d'optimisation se chargent d'identifier les éléments du programme qui provoquent le plus d'erreurs, et de les modifier jusqu'à ce que l'erreur atteigne un seuil satisfaisant. **L'optimisation ne peut être guidée finement à ce niveau de complexité, et peut parfois entraîner des comportements imprévus.** Une expérience de pensée permet d'illustrer le type de comportements auxquels on peut aboutir : l'usine à trombones[12]. Dans cette expérience, une IA est programmée pour maximiser la quantité de trombones dans l'univers, et finit par consommer toute ses ressources, y compris les utilisateurs de trombones pour parvenir à cette fin.

Le modèle issu de l'apprentissage fournit un ensemble de caractéristiques à rechercher, déterminé par les jeux de données qu'on lui a fournis précédemment pour retrouver le même objet (le chat) sur des images inconnues.

Sur de nouvelles images, on pourra donc appliquer ce modèle pour trouver l'objet : en pratique, l'algorithme aura pour rôle d'afficher un cadre autour de l'objet à identifier (par exemple, un chat sur une photo d'animaux). Pour les vidéos, d'autres modèles doivent être ajoutés puisque les images bougent et les objets aussi (le chat marche ou s'allonge). **Cette étape consiste donc à choisir quelles caractéristiques sont les plus pertinentes pour les repérer à nouveau sur l'image (une texture, une couleur, un mouvement).**

Pour la vidéosurveillance automatisée, les variables seront liées aux caractéristiques du corps humain ou les vêtements qui seront analysés, classés... pour parfois ne pas être retenues non plus. Cette étape nécessite énormément de traitements d'analyse, car le but est de répéter le plus possible l'apprentissage pour arriver au résultat le plus précis pour reconnaître avec le plus possible de certitude un objet, un comportement (une personne debout, assise, qui court, vêtue de noir...). Il s'agit donc d'un travail très long et coûteux en puissance de calcul.

12 Explication de de l'experience de pensée de l'usine à tombones https://www.lesswrong.com/tag/paperclip-maximizer

Nous évoquions précédemment l'impact du choix humain lors de la sélection du jeu de données et de la labellisation, ici c'est l'impact du choix des caractéristiques qui importe. Ces caractéristiques étant dans la majorité des cas déterminées par l'algorithme lui-même, il ne peut se poser aucune question quant à la sensibilité des données prises en compte : le programme infère à partir des données qu'il a à disposition de manière indistincte. **Par exemple, si l'algorithme considère que la couleur d'un animal est pertinente et efficace pour déterminer qu'il s'agit d'un chat, on prend la décision de ne potentiellement pas reconnaître un chat dont la couleur sortirait de la moyenne statistique des chats.** Ici encore, si on parle d'un chat l'enjeu politique est faible, en revanche, si on parle de décision sur l'activité humaine, l'enjeu prend une plus grande envergure.

Si l'on décide de reconnaître des comportements suspects et que les bases de données contiennent beaucoup de personnes en survêtement en train de commettre lesdits actes, le programme infèrera que porter un tel survêtement est un facteur de risque, même si ce choix pas été explicitement décidé par les concepteurs.

c. Choix d'usage de l'algorithme

Une fois que l'algorithme est prêt, il faut le lier à une application dans un logiciel. Par exemple, placer des carrés de couleur bleue quand c'est un chat, de couleur rouge quand c'est un chien. Ici, ce sont donc les concepteurs de l'application finale qui doivent lier au modèle une règle pratique. Depuis le début de cet exposé, nous prenons les exemples de la reconnaissance de chat et de la vidéosurveillance automatisée en mettant en avant la différence d'enjeu politique entre les deux.

Pour la vidéosurveillance automatisée, l'enjeu politique est grand, c'est ici que s'opèrent les choix d'évènements qui généreront une alerte. Par exemple : quelqu'un qui court, un groupe qui se rassemble, une personne allongée, une personne qui écrit sur un mur... Le choix de demander à l'algorithme de repérer ces comportements à un sens et des conséquences sur l'action policière.[13]

On ne parle ici que d'algorithmes qui ont un objectif de détection précis. Ce type d'algorithmes est utilisé uniquement lorsqu'il s'agit d'une détection récurrente pour laquelle il existe suffisamment de données permettant à l'algorithme de mettre en évidence des caractéristiques.
D'autres modèles dits "end-to-end" intègrent la reconnaissance d'objets et ont pour but d'émettre un diagnostic ("suspect"/"non suspect") une seule exécution. Ils permettent d'identifier des comportements inhabituels sans avoir été entrainé à reconnaitre un type de comportement particulier.

13 Voir l'expérimentation VSA à Châtelet-les-halles avec la détection de maraudage https://institutparisregion.fr/fileadmin/NewEtudes/000pack2/Etude_2310/NR_833_web.pdf

Ensuite, les algorithmes sont intégrés dans un logiciel (lui-même installé dans les CSU ou directement embarqué sur les caméras pour la vidéosurveillance automatisée) pour être testés puis utilisés en conditions réelles.

On comprend donc que le résultat de toutes ces opérations - au regard du travail fourni et du temps passé - a énormément de valeur. **Aussi bien le modèle seul que le duo « modèle-règle d'application » ont donc vocation à être ensuite vendus à un ensemble de clients.** Dans le cas d'une commande ou une expérimentation pour un besoin A, une fois arrivée au résultat, le concepteur de l'algorithme disposera d'une offre sur le marché de ce besoin A grâce à cette première commande. Aussi, si un modèle est d'abord commandé pour un usage X (repérer une personne statique sur la chaussée), ce même modèle pourra ensuite être décliné pour un usage Y (repérer une personne statique sur le trottoir pour **orienter les contrôles policiers contre la mendicité**).

Ainsi, on comprend qu'il importe peu que les **données d'entraînement soient supprimées, le résultat auquel elles ont permis d'aboutir sera conservé et pourra servir à une multitude d'applications** qui peuvent être différentes du contexte premier d'expérimentation.

De même, essayer d'anonymiser les données d'entraînement ne peut suffire à garantir que l'algorithme final sera respectueux des droits et libertés puisque l'ensemble des choix d'apprentissage et de règles associées est également très problématique et porteur de choix politiques ou discriminants. **Il n'existe pour l'instant aucune preuve ou consensus sur le fait que les méthodes d'anonymisation permettent de masquer entièrement les données d'entraînement sensibles.** Ainsi, des techniques telles que l'attaque d'inférence, ou l'inversion de modèle permettent de récupérer des données utilisées pour l'entraînement à partir du programme même. Certains programmes massifs (les Large Language Models, dont chatGPT est la plus récente émanation) mémorisent des éléments de leur ensemble d'apprentissage, ce qui représente une atteinte potentiellement grave à la vie privée qui, en outre, peuvent reposer sur le détournement du consentement de toute personne dont les données ont été utilisées pour l'entraînement de tels programmes.[14]

14 Lire notre article « Les Suresnois·es : nouveaux cobayes de la technopolice » https://technopolice.fr/blog/les-suresnois%C2%B7es-nouveaux-cobayes-de-la-technopolice/

2. Les implications techniques dues à l'usage d'algorithmes de VSA

a. Impossibilité technique de protéger les données sensibles

Le projet de loi olympique prévoit dans l'article 7 que les données d'apprentissage (c'est-à-dire les images sur lesquelles l'algorithme va apprendre à détecter les évènements) dites « de validation et de test » choisies soient « pertinentes, adéquates et représentatives ». Comme exposé ci-dessus, pour entraîner un algorithme, on part toujours d'un volume énorme de données, sans forcément savoir lesquelles sont pertinentes, pour ne retenir à la fin que quelques variables. **Ces exigences de la loi olympique sont donc en total décalage avec la réalité technique et ne peuvent s'appliquer à des techniques de machine learning**.

L'algorithme ne connaît pas la nature ou la sensibilité des données qu'il traite, il ne fait que chercher des corrélations entre des variables. Une image contenant des données biométriques (très sensibles par essence) ou une image d'un objet seront traitées de la même manière. Étant donné que l'apprentissage statistique repose sur des corrélations, on peut facilement se retrouver à utiliser des informations sensibles pour reconnaître une image. Lorsque l'on parle d'un chat, il y a peu d'enjeu politique. Dans le cadre de la VSA, si un algorithme a été entraîné à repérer des personnes susceptibles d'écrire sur un mur à partir d'un jeu de données, **celui-ci va se servir de toutes les informations à sa disposition** pour repérer ce type de profil. Si dans le jeu de données initial il y a davantage d'hommes, davantage de personnes jeunes, davantage de personnes à la peau foncée par exemple, l'algorithme pourra être amené à utiliser ces critères comme un élément différenciant pertinent pour prédire si une personne est un potentiel grapheur.

L'article 7 prévoit également que le traitement de ces données doit être « *loyal, objectif et de nature à identifier et prévenir l'occurrence de biais et d'erreurs.* » À nouveau, comme nous l'avons expliqué, les raisonnements et chemins d'apprentissage qui permettent de parvenir à un modèle final ne peuvent jamais être maîtrisés totalement. **Cette condition de prévention des biais et d'erreurs est donc illusoire et vide de substance** : comme nous l'avons dit précédemment, ces "biais" ne sont rien d'autre que le fruit de décisions politiques passées qui se retrouvent statistiquement dans les jeux de données. L'algorithme ne fait pas d'erreur, il apprend sur des données qui comporte de base une orientation. La seule solution pour aboutir à un algorithme "non biaisé" serait de le faire fonctionner de manière aléatoire, ce qui serait contraire à l'intention "d'aide à la prise de décision" qui lui est conférée.

b. Opacité due à la complexité des calculs

Il existe différents niveaux de complexité dans le machine learning. La vision assistée par ordinateur nécessite d'avoir recours au "deep learning", ou "apprentissage profond" car les flux vidéos contiennent de très grandes quantités de variables, ce qui implique de nombreux calculs. Une simple image HD compte plus de 2 millions de pixels, ce qui est d'une complexité monstre à analyser et même à concevoir pour un oeil humain et il n'est pas imaginable que toutes les dimensions que nécessite son analyse soient chapeautées par un humain.
Pour parvenir à effectuer tous les calculs que nécessite l'analyse de telles images, ils sont effectués dans différentes couches de réseaux de neurones. Chaque couche a un rôle et permet de pondérer l'algorithme pour lui faire adopter différents comportements.

Certains algorithmes comportent énormément de couches, ce qui les rend totalement opaques dans leur fonctionnement y compris pour les data scientists qui les manipulent, et qui souvent les utilisent à tâtons sans avoir de réelle conscience de pourquoi tels réglages fonctionnent mieux que tel autre : on se retrouve face à un divorce entre l'intention du programmeur et ses a priori, et ce que la machine produit effectivement comme programme.

La complexité des calculs et la sensibilité des informations contenues dans les flux vidéos de la vidéosurveillance, ne permettent pas d'avoir une utilisation respectueuse des droits des personnes.

L'article 7 prévoit que soient automatiquement enregistrés les « *évènements permettant d'assurer la traçabilité du fonctionnement de l'algorithme* ». Comme exposé précédemment, les ingénieurs ne peuvent en effet avoir la main que sur la correction d'erreurs du résultat (est-ce une personne qui court) et non sur la manière dont le résultat est créé (comment l'algorithme a compris qu'il s'agissait d'une personne qui courrait), surtout dans les technologies de deep learning. Cette garantie légale est donc inopérante.

C. Qui fabrique ces algorithmes ?

1. Des entreprises privées définissent la normalité dans l'espace public

Ce sont des entreprises privées qui vendent ces logiciels aux collectivités et ainsi qui définissent ce qu'il est possible de détecter avec la VSA. Il s'agit donc d'une certaine forme de **délégation de la définition l'ordre public** qui est entre les mains du privé et qui va régir les libertés publiques. En donnant le pouvoir aux entreprises de définir ce qui est « normal» ou « anormal » au sein de l'espace public, c'est donc à des fins marchandes et décorrélées de l'intérêt général que nous déléguons la sécurité.

Le marché de la sécurité est en pleine expansion en France, et dans le monde entier. Et particulièrement la vidéosurveillance, qui représente un marché très lucratif, est un secteur en constante expansion (10% de croissance par an de prévus) : il représentait 45 milliards d'euros en 2020 et pourrait représenter jusqu'à 75 milliards d'ici 2025 d'après les prévisions[15].

2. La vidéosurveillance : un marché économique en plein boom

La vidéosurveillance algorithmique contribue à rendre cette surveillance attractive. Comme le montre Myrtille Picaud dans ses recherches[16], le marché numérique de la sécurité urbaine est investi par **une panoplie hétérogène d'acteurs** : il y a d'abord, **des grandes multinationales provenant du domaine des TIC** comme IBM, à Toulouse, qui a équipé une trentaine de caméras de vidéosurveillance de la métropole d'un logiciel de vidéosurveillance automatisée. Ensuite, il y a les **industriels de la sécurité**, largement soutenus par les subventions publiques qui se sont intéressés à cette numérisation de ce marché. Par exemple, Thalès, avec l'expérimentation Safe City à Nice et à La Défense ou encore la SNEF[17] à Marseille.

Enfin, **les start-ups** ne sont pas en reste. Certaines se sont soit créées spécifiquement pour le marché de la sécurité urbaine comme Aquilae[18], start up provenant d'un projet universitaire qui déploie de la VSA en partenariat avec la préfecture de police de Paris, labellisé JOP 2024. D'autres start-up, au contraire, ont fait une reconversion comme Two-I[19]. À la base, cette entreprise était spécialisée dans la reconnaissance d'émotion, d'ail-

15 Telquel, « *Ce que pèse le marché mondial de la vidéosurveillance* », publié le 2 juillet 2021 et accessible à https://telquel.ma/2021/07/02/ce-que-pese-le-marche-mondial-de-la-videosurveillance_1727755

16 Myrtille Picaud « *Peur sur la ville. La sécurité numérique pour l'espace urbain en France* », Chaire "Villes et numérique", Ecole urbaine de Sciences Po. 2021, accessible à https://hal.science/halshs-03138381/

17 Voir la documentation collectée sur l'outil collaboratif « Carré Technopolice » et accessible à https://carre.technopolice.fr/#51642543

18 Voir la description sur https://technopolice.fr/aquilae/

19 Voir la description sur https://technopolice.fr/two-i/

leurs elle devait mener une expérimentation à Nice dans les tramways qui a été abandonnée depuis. Aujourd'hui, elle a mis au point des algorithmes de reconnaissance faciale, testés sur les supporters du stade de foot de Metz ainsi qu'une plateforme d'hypervision, permettant le pilotage à distance de la ville. Enfin, même si les JO 2024 représentent une occasion pour structurer la filière des entreprises de la surveillance, les **entreprises étrangères** ne sont pas en reste. Une des solutions de vidéosurveillance algorithmique les plus répandu en France est celle proposée par Briefcam[20], dont pas moins de 35 villes françaises seraient dotées, avec une option de reconnaissance faciale, que les élus à la sécurité sont très impatients d'enclencher[21].

3. L'opacité inquiétante des projets de VSA

Lorsque nous avons commencé à documenter le déploiement de la VSA depuis 2019, nous avons effectué d'innombrables demandes d'accès à des documents administratifs afin d'en savoir plus sur les technologies installées sur le territoire français. Malgré nos efforts, relances, saisines de la CADA, nombres de nos demandes sont restées sans réponses. C'est une des caractéristiques de la Technopolice : l'opacité des projets mis en place dans nos espaces publics. Par exemple, la municipalité de Dijon n'a jamais répondu à nos demandes en plus de deux ans. De son côté la ville de Marseille, qui refuse méticuleusement de nous fournir des informations sur l'expérimentation de la VSA en dépit des avis favorables de la CADA, alors même que Marseille est une ville pionnière dans le développement illégal de ces technologies.

À cette opacité bien pratique, s'ajoute le fait que les collectivités n'ont pas besoin de justifier des objectifs poursuivis par ces déploiements : si personne n'est au courant, pas besoin de réaliser des études et recherches sur la pertinence de tels dispositifs. Comme pour la vidéosurveillance, où le nombre d'études sur l'effet des caméras et leur efficacités se compte sur les doigts de la main et ne va pas dans le sens du Ministère de l'intérieur (comme nous l'exposons dans la partie II de cette note), la VSA n'est le produit que d'un discours des acteurs du marché de la sécurité, sans qu'aucune évaluation ne soit mise en place ou systématisée.

4. La recherche publique finance des technologies illégales

S'agissant en particulier des Jeux Olympiques 2024, **l'Agence Nationale de la Recherche (l'ANR) a financé la vidéosurveillance automatisée à hauteur de plusieurs millions d'euros**. Dans cet appel à projet «« Flash » de 2020 que nous avons pu nous procurer[22], nous y apprenons que six projets ont

20 Voir la description sur https://technopolice.fr/briefcam/

21 17. Sciences Critiques, « *À Nîmes, la reconnaissance faciale dévoile son vrai visage* », publié le 20 février 2022 et accessible à https://sciences-critiques.fr/a-nimes-la-reconnaissance-faciale-devoile-son-vrai-visage/

22 Lire notre analayse « *JO2024 : l'Agence nationale de la recherche planifie la technopolice* », publié le 8 avril 2021 et accessible à https://technopolice.fr/blog/jo2024-lagence-nationale-de-la-

été sélectionnés, pour un financement à hauteur de 500 000€ maximum. Ces projets visent à développer des algorithmes capables, lors des JO 2024, de détecter des comportements anormaux au sein d'une foule, d'extraire des données du réseau social Twitter ainsi que des données téléphoniques de l'opérateur Orange, pour « détecter en temps réel les situations atypiques ou critiques » ou même de sécuriser l'accès aux infrastructures olympiques via la reconnaissance faciale.

5. L'État incite et finance le déploiement de la vidéosurveillance et de la VSA

Aussi, le ministre de l'intérieur incite à installer des caméras de vidéo-surveillance dotées de ces technologies illégales en les finançant à travers le fonds interministériel de prévention de la délinquance (ci-après le « FIPD »). Créé en 2007, ce fond est « destiné à financer la réalisation d'actions dans le cadre des plans de prévention de la délinquance et dans le cadre de la contractualisation mise en œuvre entre l'État et les collectivités territoriales en matière de politique de la ville ». Chaque année, une circulaire du ministère de l'Intérieur fixe les orientations du gouvernement en matière de politiques publiques de prévention et indique quels sont les projets susceptibles de recevoir ces subventions. **Depuis la création de ce fond en 2007, le FIPD incite les communes à installer des caméras de vidéosurveillance en subventionnant** dans de grandes proportions leur mise en place.

Ainsi, la circulaire du 11 février 2022 relative aux orientations budgétaires des politiques de prévention de la délinquance et de la radicalisation pour 2022[23] **incite clairement les collectivités locales à doter leurs dispositifs de vidéosurveillance de traitements algorithmiques des flux d'images**. En effet, l'instruction complémentaire à la circulaire indique que (cf. p. 8 de la circulaire précitée) :

> **« Sera au contraire privilégiée l'amélioration de la technologie, conformément à la SNPD 2020-2024 qui incite à expérimenter le traitement automatisé de l'image, dans les limites légales rappelées (ex. recours possible au traitement permettant d'identifier une situation dangereuse : mouvement de foule inhabituel, cris soudains, intrusion dans un espace interdit, départ d'incendie, etc.). »**

recherche-planifie-la-technopolice/fr/blog/jo2024-lagence-nationale-de-la-recherche-planifie-la-technopolice/

23 Extrait de l'audition de M. Gérald Darmanin sur la sécurité des jeux Olympiques et Paralympiques de 2024 accessible ici : https://video.lqdn.fr/w/m7tt1cpdvc8nKA4eMumfoZ

Cette exigence est en effet une mise en œuvre concrète de la **proposition 26 de la stratégie nationale de prévention de la délinquance** (SNPD) 2020-2024 qui précise[24] : « *En matière de vidéoprotection : expérimenter le traitement automatisé de l'image, dans le respect des libertés individuelles* ». Cette action, dont il est précisé que l'État en est un des pilote et partenaire, consiste à tester la « connexion avec des logiciels de détection de situations comportant un danger manifeste : mouvement de foule inhabituel, cris soudains, intrusion dans un espace interdit, départ d'incendie, etc. ».

Ainsi si le ministre de l'Intérieur se targue devant la commission des lois du Sénat de sa prétendue exemplarité en affirmant que le ministère ne « met en place des choses que si la loi expressément nous l'autorise, ce qui est à mon sens une bonne chose »[25], on voit bien depuis plusieurs années l'incitation très forte par l'Intérieur de déploiement de ces technologies via des subventions ou des textes directeurs. Le Livre blanc de la sécurité intérieure[26], qui dresse la feuille de route du ministère pour les prochaines années est très clair la-dessus dans son titre III **Porter le Ministère de l'Intérieur à la frontière technologique** avec des dispositions qu'on retrouve dans le rapport annexé[27] à la LOPMI (casques et lunettes augmentée de policiers-robot, de l'exploitation d'une multitude de données par intelligence artificielle, ou de casques de « réalité augmentée » permettant d'interroger des fichiers en intervention).

Si la question de la légalisation de la vidéosurveillance vous est aujourd'hui posée avec ce projet de loi, il y a en réalité des années que différents organismes publics travaillent de concert avec les industriels pour mettre au point et expérimenter ces technologies en tâchant d'échapper autant que faire se peut au débat public.

24 Voir page 39 de la stratégie nationale de prévention de la délinquance, tome 2, accessible à https://www.cipdr.gouv.fr/wp-content/uploads/2020/03/Tome-2-SNDP-E%CC%81XE%CC%81-INTERACTIF.pdf

25 Extrait disponible sur https://video.lqdn.fr/w/m7tt1cpdvc8nKA4eMumfoZ

26 Voir cet article publié le 19 novembre 2020 et accessible à https://www.laquadrature.net/2020/11/19/la-technopolice-moteur-de-la-securite-globale/

27 Lire le communiqué de l'Observatoire des libertés et du numérique publié le 19 novembre 2022 et accessible à https://www.laquadrature.net/2022/10/28/examen-de-la-lopmi-refusons-les-policiers-programmes/

II. La VSA , un outil de surveillance de masse

A. Aspects économiques et sociétaux

La volonté de généraliser la vidéosurveillance algorithmique intervient dans un contexte où l'infrastructure socio-technique à laquelle se greffent ces algorithmes — à savoir la vidéosurveillance dite « classique » — s'est démultipliée. Le dernier décompte du nombre de caméras de vidéosurveillance par la CNIL date de 2012 et fait état de plus de 800 000 caméras sur le territoire national, qu'elles soient dans des espaces publics ou privés, chiffre qui a sans nul doute au minimum doublé ou triplé depuis. Quant au budget public consacré par l'État et les collectivités locales à l'installation et la maintenance des équipements de vidéosurveillance classique, il reste secret mais se chiffre sans doute à plusieurs milliards d'euros. Or, comme pour toute politique publique, **il devrait exister des évaluations fiables de l'efficacité ou l'utilité de la vidéosurveillance classique**. Mais les services de l'État se refusent à les produire. **Les rares études indépendantes menées sur le sujet pointent toutes vers le caractère dérisoire du rapport coût/bénéfice de la vidéosurveillance.** Enfin, on note **l'échec retentissant des tentatives d'encadrement de cet outil**. Cet échec patent des politiques en matière de vidéosurveillance classique devrait à lui seul justifier le rejet de la VSA.

1. Une absence criante d'évaluation publique concernant la vidéosurveillance

Le projet de loi propose d'expérimenter la vidéosurveillance automatisée alors même qu'**aucune évaluation publique des dispositifs actuels de vidéosurveillance n'existe, qu'aucun besoin réel n'a été identifié ni une quelconque utilité scientifiquement démontrée**. Le projet du gouvernement est donc de passer à une nouvelle étape de la surveillance de masse, en fondant la légitimité d'une technologie très intrusive sur l'intensification de la surveillance via l'automatisation de l'analyse des images, alors que l'utilité des caméras de vidéosurveillance pour lutter contre la délinquance n'a jamais fait ses preuves. Contrairement au principe qui voudrait que toute politique publique soit périodiquement évaluée, la vidéosurveillance — et sa nouvelle version automatisée — se développe sur le seul fondement des croyances défendues par les personnes qui en font commerce et qui la déploient. De fait aucune étude d'impact préalable à l'installation de dispositifs de VSA n'est mise en place et les rares études dans le domaine soulignent au contraire l'inefficacité et le coût faramineux de tels dispositifs.

2. De rares études pointent unanimement vers l'inutilité de la vidéosurveillance

Le rapport de la Cour des comptes de 2020 rappelle[28] 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[29] 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* ». Plus récemment, les recherches[30] du chercheur Guillaume Gormand, commandées par la gendarmerie, concluent elles aussi à une absence d'effet sur la commission d'infraction et à une utilité résiduelle pour l'élucidation des infractions commises (1,13 % des enquêtes élucidées ont bénéficié des images de caméras sur la voie publique).

3. Le coût faramineux de la vidéosurveillance

En outre, petit à petit, la vidéosurveillance a fait exploser les budgets publics qui lui étaient consacrés. Sur le court terme, ces dispositifs impliquent le développement ou l'achat de logiciels de gestion du parc de caméras (système de gestion vidéo sur IP, ou VMS), l'installation de nouvelles caméras, la transmission de flux, des capacités de stockage des données, des machines assez puissantes pour analyser des quantités de données en un temps très rapide. Sur le temps long, ils nécessitent la maintenance, la mise à niveau, le renouvellement régulier des licences logicielles, l'amélioration du matériel qui devient très vite obsolète et enfin les réparations du matériel endommagé.

À titre d'illustration, le ministère de l'Intérieur évoque pour les Jeux Olympiques l'installation de 15 000 nouvelles caméras, pour 44 millions d'€ de financement du FIPD. Une caméra de vidéosurveillance coûte[31] à l'achat aux municipalités entre 25 000 et 40 000 euros l'unité, sans prendre en compte le coût de l'entretien, du raccordement ou du potentiel[32] coût d'abonnement 4G/5G (autour de 9 000 € par an et par caméra).

28 Rapport de la Cour des comptes « Les polices municipales », 20 octobre 2010, page 70, accessible à https://www.ccomptes.fr/fr/publications/les-polices-municipales

29 « *Comment la vidéosurveillance se développe-t-elle dans les villages ?* », Antoine Courmont et Jeanne Saliou, 19 novembre 2021, disponible sur https://linc.cnil.fr/fr/comment-la-videosurveillance-se-developpe-t-elle-dans-les-villages

30 L'étude en question n'est pas disponible mais résumé dans cet article du Monde « *Une étude commandée par les gendarmes montre la relative inefficacité de la vidéosurveillance* » publié le 22 décembre 2021 et accessible à https://www.lemonde.fr/societe/article/2021/12/22/une-etude-commandee-par-les-gendarmes-montre-la-relative-inefficacite-de-la-videosurveillance_6106952_3224.html

31 La Dépêche, « *Toulouse : bientôt des caméras de vidéoprotection "à la demande" pour les quartiers* » publié le 13 septembre 2021 et accessible à https://www.ladepeche.fr/2021/09/13/toulouse-bientot-des-cameras-de-videoprotection-a-la-demande-pour-les-quartiers-9787539.php

32 Actu Toulouse, « *Toulouse. Comment la Ville veut aller plus loin contre la délinquance avec des caméras mobiles* » publié le 18 juin 2021 et accessible à https://actu.fr/occitanie/toulouse_31555/toulouse-comment-la-ville-veut-aller-plus-loin-contre-la-delinquance-avec-des-cameras-mobiles_42726163.html

Avec l'ajout d'une nouvelle brique technologique à ces systèmes, la VSA contribue d'ores et déjà à l'explosion des budgets consacrés à la vidéosurveillance. À terme, outre l'achat de nouvelles licences logicielles aux start-ups et industriels du secteur, la VSA incitera les pouvoirs publics à se doter de nouvelles caméras haute définition, à disposer de capacité de calcul supplémentaires pour faire tourner les algorithmes d'analyse. Elle participera donc à la croissance des budgets déjà colossaux consacrés à la vidéosurveillance. S'agissant des enjeux budgétaires des JO, notons que le rapport de la Cour des comptes de 2022 épingle la préfecture de police de Paris pour des irrégularités dans l'attribution du marché public de vidéosurveillance lié à l'évènement, et pour le coût exorbitant de ces dispositifs — qui atteindrait[33] « *433 à 481 millions € » (soit +92 %, voire +114 %) en fonction des scénarios retenus* » au lieu des 225 millions prévus — et recommande, comme dans ses précédents rapports de 2011 et 2020 d'« engager sans tarder une évaluation de l'efficacité du PVPP (plan de vidéoprotection de la préfecture de police de Paris) dans la prévention de la délinquance et l'élucidation des délits ».

Rappelons enfin que le budget de la sécurité des Jeux olympiques de Paris 2024 n'était ni prévu, ni chiffré dans le dossier de candidature et ne fait aujourd'hui qu'augmenter pour atteindre à ce jour[34] 319,6 millions d'euros.

4. La VSA : une nouvelle étape dans le mythe de l'efficacité de la vidéosurveillance

La vidéosurveillance algorithmique est présentée comme une manière de rendre plus efficace l'exploitation policière de la multitude de caméras installées sur le territoire. Il existerait trop de caméras pour qu'on puisse les utiliser efficacement avec du personnel humain, et l'assistance de l'intelligence artificielle serait inévitable et nécessaire pour faire face à la quantité de flux vidéo ainsi générée.

> **« Il y aura toujours plus de caméras et toujours plus d'utilisation de l'intelligence artificielle »** à Nice, affirme[35] Estrosi pour **« gérer la circulation, les risques de pollution, les risques majeurs, pour lutter contre le trafic de drogues, les rodéos urbains et pour anticiper toutes les menaces »**

33 Cour des Comptes « *Le plan de vidéoprotection de la préfecture de police de Paris », 10 février 2022* » disponible ici : https://www.ccomptes.fr/fr/publications/le-plan-de-videoprotection-de-la-prefecture-de-police-de-paris

34 Libération, « *Jeux olympiques de Paris 2024 : la facture fait un bond de 10 %*» publié le 12 décembre 2022 et accessible à https://www.liberation.fr/sports/jeux-olympiques/jeux-olympiques-de-paris-2024-la-facture-fait-un-bond-de-10-20221212_MCG26H5O6JARNL4GUZDGHQAVXA/

35 Nice Matin en date du 10 janvier 2022 consultable ici : https://www.nicematin.com/sciences/il-y-aura-toujours-plus-de-cameras-et-toujours-plus-dutilisation-de-lintelligence-artificielle-a-nice-affirme-estrosi-738572sciences/il-y-aura-toujours-plus-de-cameras-et-toujours-plus-dutilisation-de-lintelligence-artificielle-a-nice-affirme-estrosi-738572

Dominique Legrand, président fondateur de l'AN2V, l'association nationale de la vidéoprotection évoque, à propos de la centralisation de CSU :

> **« L'objectif de la création d'un tel dispositif est de pouvoir assurer le visionnage en temps réel de manière centralisée, en un même lieu (cyber) sécurisé, de l'ensemble des caméras des communes et intercommunalités [...] L'AN2V a déjà évangélisé cette idée sur plusieurs départements et régions ! »** cité dans le guide PIXEL 2023[36] édité par l'AN2V.

Le fiasco du Stade de France en mai 2022 est un bon exemple de l'instrumentalisation de faits-divers à des fins de promotion de dispositifs de surveillance. C'est d'abord la reconnaissance faciale[37], puis ensuite la vidéosurveillance algorithmique[38] qui sont pointées comme des solutions afin de masquer la désorganisation et les violences de la police lors de la finale de la Ligue des champions. Or la vidéosurveillance dans ce cas-là a été particulièrement inutile. Au contraire, afin de trouver une solution, ces commentateurs auraient pu regarder dans le savoir dégagé depuis des décennies en matière de gestion de foule, tel que l'aménagement de l'espace afin d'éviter de trop fortes densités de personnes. **En d'autres termes, il faut toujours avoir à l'esprit que les problématiques de « sécurité » ont toujours fait l'objet de politiques ne nécessitant ni surveillance ni contrôle technologique, et que l'on peut continuer ainsi.**

Cette idée que l'automatisation permettrait de rendre la vidéosurveillance enfin efficace s'inscrit dans une vieille logique du « bluff technologique » de la vidéosurveillance. Depuis des années, les industriels du secteur ne cessent de promettre que l'efficacité de la vidéosurveillance dépend d'un surcroît d'investissement : il faudrait plus de caméras disséminées sur le territoire, il faudrait que celles-ci soit dotées d'une meilleure définition, qu'elles offrent une champ de vision plus large (d'où l'arrivée de caméras 360, pivot), etc. Il a aussi souvent été dit qu'il fallait davantage d'agents dans les CSU pour scruter les flux vidéo à la recherche d'actes délinquants commis en flagrance.
Au fil des années ces multiples promesses de la vidéosurveillance n'ont pas été tenues. En l'absence de toute évaluation ou étude préalable, la généralisation de la VSA ne serait qu'une perte de temps et d'argent, en plus de constituer une profonde remise en cause de nos droits et libertés.

36 Le guide est commandable sur le site de l'AN2V : https://an2v.org/
37 Citation de Christian Estrosi issu d'un article du Parisien du 31 mai 2022 et accessible à https://www.leparisien.fr/politique/stade-de-france-christian-estrosi-prone-la-reconnaissance-faciale-31-05-2022-XRMWO6X7MRDWRCOH2R4SLHQ7LA.php
38 Voir la présentation de la loi sur le site « *Vie publique* »: https://www.vie-publique.fr/loi/287639-jo-de-2024-projet-de-loi-olympique-2022

De fait, mêmes les opérateurs de terrains ne semblent pas vouloir de la VSA. À Valenciennes, après l'une de ses trop rares enquêtes sur le terrain (et à notre connaissance l'unique réalisée sur un système de VSA), la CNIL a constaté[39] que la solution fournie gracieusement par l'industriel chinois Huawei n'avait servi qu'une seule fois, pour repérer un flagrant délit de dépôt d'ordure. Le procès verbal de la CNIL indique que le compte utilisateur créé pour accéder à l'interface du logiciel n'était plus connecté à aucun flux vidéo depuis « l'expiration des mots de passe due à l'absence d'utilisation du dispositif par les agents ». À Nice, il arrive que près d'une alerte sur deux générée par le système de VSA corresponde à une fausse alerte. Et même lorsque la performance technique semble être au rendez-vous et qu'une alerte est confirmée par l'opérateur, ce dernier ne dispose pas toujours d'une patrouille disponible pour intervenir sur les lieux.

Enfin, rappelons que ce réflexe de voir en la technologie une solution évidente à un problème donné - par association à un imaginaire de progrès et de rationalité - n'a rien d'une nouveauté et a démontré toute ses limites avec l'exemple récent de l'épidémie de covid-19. Le postulat de voir en la surveillance des déplacements de la population une possibilité de résoudre les causes d'une pandémie était non seulement critiquée depuis le début mais également illusoire sur la nature des problèmes en question. Il est assez clair, avec trois années de recul qu'en tant que problématique sanitaire, cette épidémie ne pouvait se voir maîtrisée que par une politique sanitaire (qui a d'ailleurs fait l'objet de nombreuses lois et initiatives). **L'application de surveillance TousAnticovid a été non seulement un échec politique**, celle-ci étant évaluée comme avoir eu une « utilité marginale »[40] mais également **un gouffre économique** puisqu'elle aurait coûté environ 15 millions d'euros[41] pour cette absence de résultat.

De façon similaire, les problématiques de sécurité des Jeux olympiques ont des causes et imbrications complexes et tomber dans **le piège technosolutionniste** plutôt que de prendre du recul pour trouver des solutions réfléchies et adaptées ne permettra pas de les résoudre et au contraire, de façon similaire à TousAnticovid, n'auraient pour effet que d'habituer la population à des outils de surveillance de masse et déséquilibre grandement la démocratie.

39 Compléments d'information de la Région à propos de l'expérimentation de portiques de reconnaissance faciale, 2018, consultable sur https://data.technopolice.fr/fr/entity/hi661p1k6s9

40 Rapport accessible à https://bonjour.tousanticovid.gouv.fr/cms/f0744e36-4b6c-4faf-9e17-483dc4b35671_Bilan_TousAntiCovid_2021.pdf

41 La Tribune, « *TousAntiCovid : une utilité "marginale" d'après l'étude d'impact, faut-il l'arrêter ?* », publié le 24 février et accessible à https://www.latribune.fr/technos-medias/tousanticovid-une-utilite-marginale-d-apres-l-etude-d-impact-faut-il-l-arreter-904705.html

5. L'échec de l'encadrement du déploiement de la vidéosurveillance

Suite au déploiement massif de la vidéosurveillance, plusieurs comités d'éthique de la vidéoprotection se sont constitués afin de répondre à une demande d'encadrement de ces dispositifs de surveillance. Ils sont créés à l'initiative de la municipalité et leur composition dépend de la volonté des pouvoirs publics. Or, les années passant, ils ont largement été décriés, qualifiés[42] de « **comités fantômes** », sans aucun moyen ni pouvoir et parfois, sans qu'ils se réunissent pendant plusieurs années. La Ligue des droits de l'Homme, dont la participation est souvent sollicitée, **a refusé de devenir un faire-valoir** : elle « *considère que les comités d'éthique ne sont qu'un leurre destiné à donner une illusion de fonctionnement démocratique à l'installation des systèmes de vidéosurveillance et réaffirme son opposition à toute participation* »[43].

Plus largement, c'est l'ensemble des règles censées contenir le déploiement de la vidéosurveillance au nom de la protection des droits fondamentaux qui sont presque systématiquement ignorées. Ainsi, que ce soit au niveau des collectivités qui les déploient, des préfets qui les autorisent ou des comités d'éthiques qui sont amenés à se prononcer sur tel ou tel déploiement, la démonstration de l'utilité des caméras au regard de la finalité choisie — un critère de légalité découlant pourtant de l'article 251-2 du code de la sécurité intérieure — est presque systématiquement omise. Cela rend illégal des centaines de milliers de caméras déployées sans que les autorités n'aient pris la peine de justifier leur déploiement.

C'est ce que rappelle l'une des rares affaires où des citoyens déterminés de la commune de Ploërmel sont parvenus à s'organiser pour contester la vidéosurveillance. La Cour administrative d'appel de Nantes leur donnant raison dans on arrêt du 9 novembre 2018, notant que certaines caméras avaient été installées « *aux abords des écoles ou à proximité des commerces, bars ou autres établissements recevant du public, sans qu'il soit établi, par les statistiques relatives à la délinquance dans la commune, que ces lieux seraient particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants* », jugeant donc qu'un tel déploiement « *apparaît disproportionné au regard des nécessités de l'ordre public* »[44]. Des conclusions qui, en creux, peuvent s'appliquer à l'immense majorité des déploiements de caméras.

---

42 Le Monde, « *Vidéosurveillance : des « comités d'éthique » sans pouvoirs, sans budget et, parfois, sans activité* », publié le 27 juillet 2018 et accessible à https://www.lemonde.fr/pixels/article/2018/07/27/videosurveillance-des-comites-d-ethique-sans-pouvoirs-sans-budget-et-parfois-sans-activite_5336791_4408996.html

43 Guide juridique de la LDH sur la vidéosurveillance accessible à https://www.ldh-france.org/wp-content/uploads/2018/07/Guide-Juridique-la-vid%C3%A9osurveillance-DEF.pdf

44 CAA Nantes, 9 novembre 2018, Commune de Ploërmel, n° 17NT02743 disponible sur https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000037829899

On retrouve ce même phénomène de manque d'effectivité des garanties prévues par la loi en matière de fichiers de police. Si ces traitements de données sont encadrés en théorie par des principes de proportionnalité et de limitation d'accès, en pratique ils constituent des bases de données gigantesques et consultées de façon quotidienne et banale par les agents de polices. L'exemple le plus symptomatique de cette dérive est le fichier de traitement des antécédents judiciaires (TAJ) qui comporte actuellement près de **vingt millions de fiches et plus de huit millions de photographies**. Nous avons d'ailleurs dénoncées cette disproportion et l'absence de contrôle de la collecte et de l'intégrité des données du TAJ dans notre plainte collective déposée devant la CNIL.[45]

S'agissant des **études d'impact** préalables, elles s'avèrent également inefficaces. Alors que la VSA est déployée dans de nombreuses villes françaises, notre travail de documentation ne nous a jamais permis de mettre la main sur une étude d'impact en bonne et due forme, alors même que celles-ci sont requises par la législation française et européenne en matière de données personnelles. À Marseille, suite à un recours en référé que nous avions déposé devant le tribunal administratif, nous avons appris que la ville avait entrepris de légitimer son expérimentation de la VSA, alors déjà en cours, via une étude d'impact. Celle-ci fut communiquée à la CNIL pour avis à l'été 2020. Les services de la CNIL répondirent qu'« une première analyse du document [avait] permis de relever un certain nombre de points de fond et de méthode pour lesquels des précisions et compléments [devaient] être apportés ». Manière d'indiquer que ce travail n'était ni fait ni à faire. Quoique la CNIL ait exigé des compléments d'information sur des points précis[46], la ville de Marseille n'a à notre connaissance jamais finalisé ce document, ce qui ne l'a pas empêchée de[47].

À la lumière de ces tristes précédents, il apparaît clairement que le dispositif d'encadrement de la VSA esquissé par le projet de loi qui vous est soumis est non seulement particulièrement complexe mais surtout incapable d'assurer une protection efficace des droits fondamentaux, comme nous l'explicitions dans la première partie.

B. Surveillance de masse

En plus de son absence d'évaluation, son coût faramineux et son inutilité, la vidéosurveillance algorithmique est un outil de surveillance de masse, c'est-à-dire qu'il s'attaque à scruter et analyser les corps de toute personne qui se déplace dans l'espace public. **La VSA change le rapport de la police**

45 Pour plus de détails, le résumé et l'accès à la plainte sont disponibles sur https://www.laquadrature.net/2022/09/26/15-248-personnes-portent-plainte-contre-la-technopolice/

46 Le document est accessible ici :https://data.technopolice.fr/fr/entity/p05u7e4k8ie

47 Marsactu, « *La Ville de Marseille développe la vidéosurveillance intelligente malgré son moratoire* » publié le 14 février 2022 et accessible à https://marsactu.fr/la-ville-de-marseille-developpe-la-videosurveillance-intelligente-malgre-son-moratoire/

vis-à-vis de la population, témoignant d'un rapport déshumanisé et distant. Celle-ci est désormais mise en données et passe au statut de **cobaye**, utilisée pour améliorer les algorithmes d'entreprises privées. Enfin, l'automatisation des caméras constitue un **changement d'échelle** dans les potentialités de surveillance et d'abus policiers qui devrait nous alarmer.

1. Stigmatisation d'une catégorie de population

Comme tout système de surveillance de l'espace public, la vidéosurveillance automatisée **surveille en priorité les personnes qui passent le plus de temps à l'extérieur** et détecte des comportements d'autant plus efficacement qu'elle a pu s'entraîner à partir d'une grande quantité de séquences d'images représentant une même action. En pratique ce seront donc les comportements typiques de ces populations qui passent du temps dans la rue, peu importe que ces activités soient licites ou illicites. Ce sont précisément ces comportements que les fournisseurs de ces outils mettent en avant comme comportements dit « anormaux » : maraudage, mendicité, réunions statiques. Par exemple, la RATP a expérimenté[48] dans la salle d'échange du RER des Halles un système pour repérer les personnes statiques pendant plus de 300 secondes.

Si ce comportement alerte les forces de l'ordre, on peut craindre pour les personnes qui ne peuvent pas voir la rue comme un « simple endroit de passage », car elles y vivent ou en font un repère social nécessaire.
La vidéosurveillance automatisée amplifiera donc les pratiques discriminatoires **en automatisant les contrôles fondés sur des critères sociaux**, permettant de multiplier les alarmes sonores ou les contrôles humains et d'exclure une partie de la population de l'espace public.

La focalisation de la VSA sur les populations les plus pauvres n'est pas le simple « effet de bord » d'une technologie immature qui aurait encore quelques « biais ». Au contraire, les constructeurs de ces dispositifs d'analyse et détection affirment clairement lutter contre des comportements définis comme « anormaux » qui, bien qu'étant parfaitement communs et « normaux » pour une large partie de la population, permettent de dénigrer les populations qui adoptent ces comportements. In fine, ces technologies décupleront la capacité à normaliser l'espace public et pousseront les personnes à autocensurer leurs propres comportements. Si l'on sait qu'il y a un algorithme mis en œuvre, est-ce qu'on pourra faire trois fois le tour d'un quartier pour le plaisir d'une balade, si cela peut potentiellement être repéré comme « suspect » ?

2. Changement du rapport de la police à la société

48 « *La sécurité à l'heure de l'intelligence artificielle* », Iinstitut Paris Région, février 2020, accessible à https://www.institutparisregion.fr/fileadmin/NewEtudes/000pack2/Etude_2310/NR_833_web.pdf

En outre, **la vidéosurveillance automatisée renforce la distance qui sépare la police de la population**. Cette distance est d'abord physique : l'interaction passe par des écrans et ne se réalise que dans une seule direction. La distance est aussi intellectuelle : les agents n'ont plus à comprendre, à évaluer ou à anticiper l'action des autres humains quand une machine le fait à leur place. Peu importe que formellement la décision d'intervenir soit prise par un agent de sécurité ou de police (pour rappel, c'est déjà obligatoire sur le fondement de l'article 22 du RGPD), faire reposer ces choix sur une analyse automatique effectuée par un algorithme dont le fonctionnement repose sur des choix politiques, n'est pas neutre.

Cet écart entre la police et la population a pu être observé lors du confinement et peu après, avec des dérives dans l'utilisation de la vidéosurveillance et des pouvoirs entre les mains des forces de l'ordre, qui présagent d'une croissance exponentielle des possibilités de dérives si la vidéosurveillance algorithmique venait à être autorisée. Ainsi « **les amendes sans contact** » distribuées par la police grâce à l'utilisation de caméras de vidéosurveillance, à Millau ou en Île-de-France, témoignent des abus rendus possibles par le déploiement des technologies de surveillance.

- À Millau[49], des personnes s'étant rendues à un rassemblement post-confinement ont reçu des amendes, sans qu'aucun contrôle d'identité n'ait été réalisé ni de contravention notifiée. Ces amendes ont été envoyées aux personnes fichées par les services de renseignements aveyronnais grâce au visionnage des caméras de vidéosurveillance. Après une bataille juridique longue de deux ans, le tribunal de Millau a abandonné les charges contre la trentaine de personnes concernées par ces amendes.
- En île-de-France[50], certaines familles ont reçu jusqu'à plusieurs dizaines de milliers d'euros d'amendes pour non port du masque, non-respect du confinement, sans qu'à aucun moment les personnes se soient fait contrôler leur attestation. Encore une fois, ce harcèlement des jeunes de quartiers populaires est rendu possible par les caméras de vidéosurveillance. Le Défenseur des Droits a été saisi.

Ces exemples montrent bien les abus dont sont capables les agents des forces de l'ordre. Les caméras de vidéosurveillance, d'autant plus dotées d'un algorithme et associées au pouvoir contraventionnel[51] qui ne cesse de croître, permettent de s'acharner sur certaines populations et rendent plus compliquée toute contestation ou négociation. Les deux exemples cités sont extrêmement choquants et ne doivent pas constituer la norme. La vidéosurveillance algorithmique banalisera ces abus.

49 Lire notre analyse ici https://technopolice.fr/blog/les-amendes-sans-contact-une-strategie-de-harcelement-policier/
50 Une enquête du Bondyblog en date du 26 juillet 2021 https://www.bondyblog.fr/societe/police-justice/des-jeunes-surendettes-a-cause-des-amendes-du-couvre-feu-dans-les-quartiers/
51 Renforcé par la LOPMI avec les amendes forfaitaires délictuelles, plus d'infos ici https://www.laquadrature.net/2022/10/28/examen-de-la-lopmi-refusons-les-policiers-programmes/

De façon plus diffuse, cette mise à distance technologique accompagne une **politique générale d'austérité**. La collectivité assèche ses dépenses d'accompagnement et d'aide aux individus pour ne plus financer que leur gestion disciplinaire. Dans un courrier à la CNIL, la région PACA défendait l'expérimentation[52] de la reconnaissance faciale aux abords de deux lycées en affirmant que ce projet constituait « une réponse au différentiel croissant constaté entre les exigences de sécurisation des entrées dans les établissements et les moyens humains disponibles dans les lycées, dans le cadre des plans successifs de réduction des effectifs dans la fonction publique ».

Le personnel encadrant, soucieux et à l'écoute, est remplacé par des machines dont le seul rôle est d'ouvrir et de fermer des accès. Autre exemple à Nîmes, où la métropole a ponctionné[53] presque 10 millions d'euros sur le budget d'investissement « eau » pour les dépenser à la place dans l'achat d'un logiciel de Détection Automatique d'Anomalieponctionné en temps réel.

3. Humains cobayes

Un autre aspect de la VSA est la tendance croissante à être mis en données. Au-delà de la surveillance de l'espace public et de la normalisation des comportements qu'accentue la VSA, c'est tout un marché économique de la data qui en tire un avantage. Dans le cadre des expérimentations prévues par le projet de loi, dès lors qu'un acteur tiers est en charge du développement du système de surveillance, cela permet aux entreprises privées concernées d'utiliser les espaces publics et les personnes qui les traversent ou y vivent comme des « données sur pattes ». C'est exactement ce que prévoit le VIII de l'article 7 puisque les données captées par les caméras dans l'espace public peuvent servir de données d'apprentissage.

Les industries de la sécurité peuvent donc faire du profit sur les vies et les comportements des habitants d'une ville, améliorer leurs algorithmes de répression et ensuite les vendre sur le marché international. C'est ce que fait la multinationale française Idémia, qui affine ses dispositifs de reconnaissance faciale dans les aéroports français avec les dispositifs PARAFE ou MONA, pour ensuite vendre des équipements de reconnaissance faciale à la Chine et participer à la surveillance de masse (et au génocide des Ouïghours), ou encore pour remporter les appels d'offres de l'Union Européenne en vue de réaliser de la surveillance biométrique aux frontières de l'UE. Tel a également été le cas à Suresnes[54] où l'entreprise XXII a direc-

52 Courrier disponible sur notre article accessible à https://www.laquadrature.net/2019/10/28/lycees-nice-marseille-premiere-victoire-contre-la-reconnaissance-faciale/

53 Sciences critiques, « *A Nimes, la reconnaissance faciale dévoile son vrai visage* », publié le 20 février 2022 et accessible à https://sciences-critiques.fr/a-nimes-la-reconnaissance-faciale-de-voile-son-vrai-visage/

54 Lire notre analyse «*Les Suresnois·es : nouveaux cobayes de la technopolice* », publiée le 21 avril 2021 et accessible à https://technopolice.fr/blog/les-suresnois%C2%B7es-nouveaux-co-

tement utilisé les caméras de la ville pour entraîner ses algorithmes, les habitantes et habitants de la ville étant transformé·es en cobayes pour le développement commercial d'un produit de surveillance.

À titre d'exemple, **l'un des plus importants marchés de la surveillance aujourd'hui porte sur le contrôle des frontières[55] à l'intérieur et à l'extérieur des pays membres de l'Union européenne**. L'usage d'algorithmes de détection de comportements est ainsi utilisé sur des drones en Grèce afin de repérer et suivre des personnes aux zones de frontières. Dans ce cas précis, il est impossible de réduire la technologie fournie (et donc conçue et entraînée au préalable) à une seule assistance technique. Au contraire, elle est au service d'une politique policière répressive et d'une pratique dénoncée comme brutale dans ce pays.[56]

Non seulement ces technologies développées en France sont mises au service de politiques pouvant être violentes mais, comme toute source d'information, elles peuvent également **être détournées de leur usage premier** à partir du moment où elles existent. Prenons à nouveau l'exemple des outils de surveillance mises en place pour le contrôle du covid-19 qui ont été utilisées à des fins politiques dans plusieurs pays tels que l'Inde, Israël ou la Chine, comme l'a récemment révélé Associated Press[57].

4. Changement d'échelle

Enfin, la vidéosurveillance automatisée fait changer d'échelle les pouvoirs répressifs de l'État. Aujourd'hui, le nombre limité d'agents de police contraint celle-ci à concentrer une large part de ses ressources sur ses missions les plus importantes et les plus légitimes (crimes, violences aux personnes). Elle ne dispose ainsi que d'un temps et de ressources limitées pour poursuivre des activités moins prioritaires, des actions et interpellations qui ne conduisent à aucune poursuite concrète ou légitime. Demain, la VSA promet d'effacer cette limite matérielle en décuplant les capacités opérationnelles de la police pour poursuivre les missions de son choix, que ces missions soient peu légitimes ou qu'elles constituent aussi des abus.

Par exemple, le suivi visuel d'opposants politiques ou d'un groupe prédéterminé implique aujourd'hui des moyens humains si importants que ces opérations ne peuvent rester qu'exceptionnelles. La VSA rend la chose triviale

---

bayes-de-la-technopolice/

55 Lire notre analyse « *La technopolice aux frontières* », publiée le 18 février 2021 et accessible à https://technopolice.fr/blog/la-technopolice-aux-frontieres/

56 Ceci est typiquement illustré par l'aveu même d'une personne faisant parti d'un consortium de recherche ayant développé cet outil : « *For me, the one thing is, I don't know exactly what the police will do to the migrants after we alert them." He grimaced. "But what can I do," he said.*» A lire dans cet article d'Algorithm Watch https://algorithmwatch.org/en/greece-plans-automated-drones/

57 Associated Press, « *Police seize on Covid-19 tech to expand global surveillance* » publié le 21 décembre 2022 et consultable à https://apnews.com/article/technology-police-government-surveillance-covid-19-3f3f348d176bc7152a8cb2dbab2e4cc4

en permettant de suivre, à coût quasi-nul, une personne sur l'ensemble des caméras d'une ou plusieurs villes, ou avec des drones. Ce changement d'échelle transforme considérablement la manière dont les pouvoirs de police sont exercés. D'une action précise répondant à des « besoins » pouvant être débattus démocratiquement, **nous assistons à l'apparition d'une police omnisciente disposant de la capacité de surveiller et d'agir sur l'ensemble de la population**.

Ce changement d'échelle sans précédent ne devrait pas être l'objet de mesure d'urgence sous les prétextes de Jeux olympiques. À ce jour, les rares tentatives de recueillir les avis de la population à propos de la vidéosurveillance algorithmique ont montré un intérêt vif pour le sujet, et des inquiétudes. D'abord **la consultation de la CNIL sur la VSA en mars 2022 a vu plus de 200 contributions de la société civile**[58] s'inquiétant du déploiement de tels dispositifs. Également, le **Défenseur des Droits a réalisé** une enquête[59] sur la vision des technologies biométriques par les Français, qui s'estiment trop peu informés et souligne les risques considérables pour les droits fondamentaux si des technologies biométriques comme la VSA venaient à être généralisées. Enfin, avec ses modestes moyens en tant qu'association, **La Quadrature du Net a réuni plus de 15 000 signatures pour une plainte collective envoyée à la CNIL en septembre 2022**[60].

Ce changement d'échelle dans la surveillance, la déshumanisation de la population, qui devient un cobaye pour les industries sécuritaires et dont les franges les plus précaires sont particulièrement ciblées par ces technologies, ne permet pas d'autoriser la vidéosurveillance algorithmique dans ces conditions d'urgence.

58 Voir le communiqué de presse de la CNIL du 19 juillet 2022 accessible à https://www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position
59 Enquête publiée le 6 octobre 2022 et accessible à https://www.defenseurdesdroits.fr/fr/actualites/2022/10/les-technologies-biometriques-vues-par-les-francais-trop-peu-informes-face-a-des
60 Plus d'informations sont disponibles sur notre site internet : https://technopolice.fr/blog/15-248-personnes-portent-plainte-contre-la-technopolice/

III. Le cadre juridique de la VSA

La vidéosurveillance automatisée est aujourd'hui interdite par le cadre de protection des données personnelles prévu par le RGPD et la loi Informatique et Libertés.

Afin de s'affranchir de cette interdiction, le projet de loi introduit une affirmation erronée selon laquelle ces dispositifs ne mettraient pas en œuvre des traitements de données biométriques, méconnaissant totalement la définition de ces traitements (A). En parallèle, est proposé un cadre d'expérimentation confus et large qui va à l'encontre des principes fondateurs de proportionnalité et de nécessité prévus par les mécanismes du droit à la vie privée et du droit à la protection des données personnelles (B). Surtout, avec ce projet de loi, le gouvernement s'inscrit à rebours du mouvement actuel de refus de la surveillance biométrique au sein des institutions de l'Union européenne et dans les États membres, qui réclament une interdiction de ces dispositifs. (C).

A. Les données biométriques doivent être rigoureusement protégées

1. Une définition large

Le droit des données personnelles prévoit une protection particulière pour les données dites « sensibles » au vu des informations particulièrement intimes qu'elles révèlent (telles que les orientations politiques ou sexuelles). Parmi ces données sensibles, on trouve la catégorie des données dites « biométriques », qui sont « les données à caractère personnel résultant d'un **traitement technique spécifique**, relatives aux **caractéristiques physiques, physiologiques ou comportementales** d'une personne physique, qui permettent ou confirment son **identification unique** »[61].

Le traitement de ces données sensibles est encadré strictement par les articles 9 du RGPD et 10 de la directive « police-justice ».

La définition mentionnée ci-dessus, prévue pour protéger le traitement de données rattachables au corps humain, peut être dissociée en trois éléments qui permettent de qualifier des données de «biométriques». **Or on retrouve systématiquement ces trois éléments dans le cas des dispositifs de vidéosurveillance automatisée.**

61 Voir article 4§14 du RGPD et article 3§13 de la directive 2016/680 dite « police-justice »

a. Tout d'abord, il faut que les données fassent l'objet d'un traitement technique spécifique.

Les dispositifs objet du projet de loi sont concernés puisqu'ils interviennent en addition du traitement général de captation d'images dans l'espace public par caméras fixes ou drones. De plus, le traitement technique est spécifique en ce qu'il consiste en la mise en œuvre d'un **algorithme ou programme informatique appliqué aux flux vidéos** afin d'isoler, caractériser, segmenter ou rendre apparente une information relative à une personne physique filmée ou encore à extraire du flux vidéo, même a posteriori, des données concernant cette personne.

b. Ensuite, les données doivent se rapporter aux caractéristiques physiques, physiologiques ou comportementales d'une personne.

Toutes ces données sont bien celles que la vidéosurveillance automatisée capte pour détecter une situation ou un évènement :

- les données comportementales visent **toute information relative à l'action du corps dans l'environnement et l'espace**. Pourront être qualifiés de biométriques une direction de déplacement, une position dans l'espace et le temps (assis, debout, statique, allure de la marche, appartenance à un groupe, geste spécifique de la main…), un vêtement ou un accessoire porté par la personne à un instant T, un geste, une expression d'émotion.

- les informations physiques ou physiologiques peuvent se rapporter au **corps d'une personne filmée au sens large**, tels que des visages, des silhouettes ou toute caractéristique isolée du corps, telle que la couleur des cheveux, la couleur de peau, la couleur des yeux, la forme du visage, la taille, le poids, l'âge.

c. Enfin, le traitement doit avoir pour but l'identification unique de la personne.

Ce critère doit être compris en ce que le traitement permet de **reconnaître et isoler une personne en particulier**, sans forcément que soit recherchée ou associée son identité civile.

En effet, dans ses lignes directrices relatives au traitement des données personnelles par appareils vidéo, le Comité européen pour la protection des données (CEPD) indique que cette notion n'implique pas nécessairement de révéler l'état civil d'une personne mais, plus largement, de pouvoir individualiser une personne au sein d'un groupe ou de l'environnement. Pour le Comité *« si un responsable du traitement souhaite détecter une personne concernée qui pénètre à nouveau dans l'espace surveillé ou dans une autre zone (par exemple, pour projeter une publicité personnalisée continue), la*

*finalité serait alors **d'identifier de manière unique une personne physique**, ce qui signifie que l'opération relèverait d'emblée de l'article. »*.

Le CEPD donne ainsi l'exemple suivant :

*« Dès lors que le système se fonde sur l'analyse de caractéristiques physiques pour **détecter des personnes spécifiques qui entrent dans le champ de la caméra** (comme les visiteurs d'un centre commercial) et les suivre, il constitue une méthode d'identification biométrique, car il vise la **reconnaissance** par l'utilisation d'un traitement technique spécifique. »*
(Lignes directrices sur les vidéos contenant des données personnelles 3/201, version 2.0, point 82 p. 19).

Lorsqu'une empreinte numérique est associée à une personne pour la reconnaître sur un écran, il s'agit d'une identification unique.

Ainsi, **la fonction d'identification unique concerne également la classification de comportements sur la base d'une analyse des corps**. Une telle interprétation de la définition de « traitement biométrique » est partagée par le Défenseur des droits dans son rapport « Technologies biométriques : l'impératif respect des droits fondamentaux » de 2021, mais surtout dans sa récente enquête « Perception du développement des technologies biométriques en France » publiée le 6 octobre 2022.

En introduction, le Défenseur des droits rappelle que les technologies biométriques sont définies comme « *des technologies dont le fonctionnement consiste **à collecter des caractéristiques corporelles spécifiques à chaque personne dans le but d'authentifier, d'identifier ou d'évaluer les individus**. Au sens du droit des données personnelles, ces caractéristiques constituent des données biométriques lorsqu'elles font l'objet de traitements spécifiques permettant d'établir l'identification des individus de manière unique. À l'heure où les traitements de données issues du corps humain se multiplient, la présente étude d'opinion **aborde ces technologies au sens large**, en en dégageant trois finalités principales : l'authentification, l'identification et l'**évaluation**.* »

Le Défenseur des droits estime que les données biométriques doivent, au sens du droit européen des données personnelles, également s'entendre comme l'évaluation des personnes à partir du moment où les données traitées pour cette évaluation sont « *des données corporelles et/ou issues de systèmes biométriques* » et visent à « *identifier ou déduire des émotions, des traits de personnalité ou des intentions (on parle alors de systèmes de "reconnaissance des émotions") » ou bien à « **inscrire la ou les personnes visées dans des catégories spécifiques**, par exemple de sexe, d'âge, de couleur de cheveux, de couleur des yeux, d'origine ethnique ou d'orientation sexuelle ou politique en vue de prendre des mesures spécifiques (on parle alors de systèmes de "catégorisation").* » (page 3).

Le Défenseur des droits donne comme exemple de catégorisation « ***la détection de comportements dits anormaux*** *afin de lutter contre les vols dans les supermarchés, ou encore l'analyse des réactions de consommateurs à la présentation de biens ou de services afin notamment de leur proposer de la publicité ciblée.* »

De manière plus générale, il explique que « les technologies d'évaluation dites également d'analyse (on parle également de vidéo "*intelligente*" ou "*augmentée*") » sont des dispositifs d'évaluation et sont donc, à ce titre, des traitements de données biométriques.

Ainsi, les systèmes prévus par le projet de loi, en ce qu'ils ont pour fonction de détecter des évènements ou de reconnaître des individus, sur la base des comportements des personnes filmées, **doivent être qualifiés de traitements de données biométriques**.

Dès lors, le III de l'article 7 du projet de loi, qui dispose que les traitements « *ne traitent aucune donnée biométrique* », ne constitue qu'une affirmation vide d'effet juridique puisqu'elle rentre en contradiction avec des règles applicables de droit de l'Union européenne.

Il convient de véritablement questionner ce choix d'introduire de telles définitions, qui laisse penser qu'il relève plus d'une manœuvre politique tendant à rassurer et minimiser la dangerosité de cette technologie, que d'une seule ignorance de l'état du droit (qui serait tout autant critiquable). En effet, présenter une telle garantie vide de substance est une tactique généralement utilisée par les promoteurs[62] de ces technologies pour s'affranchir des questions de libertés publiques et mieux faire accepter leur implantation.

En ce sens, lorsque le projet de loi prévoit au même III de l'article que 7 que le traitements « *procèdent exclusivement à un signalement d'attention, strictement limité à l'indication du ou des événements prédéterminés qu'ils ont été programmés pour détecter* » et ne « *produisent aucun autre résultat et ne peuvent fonder, par eux-mêmes, aucune décision individuelle ou acte de poursuite* », il s'agit à nouveau de minimiser la finalité globale de ces dispositifs au travers d'allégations vides de portée légale.

D'une part, il convient de rappeler que dans tous les cas l'article 22 du RGPD interdit qu'une décision soit fondée exclusivement sur un traitement automatisé, donc le projet de loi ne fait que réaffirmer ce principe.

62 Voir par exemple la politique de vie privée de l'entreprise XXII disponible sur https://www.xxii.fr/rgpd/

D'autre part, il convient de souligner que **toute utilisation de ces systèmes a nécessairement pour but de permettre aux agents de sécurité d'effectuer une action ciblée sur la personne dont le comportement ou le corps est analysé** pour déclencher un « évènement ». En d'autre termes, la finalité globale des systèmes de vidéosurveillance automatisée est bien de permettre à des agents humains de réaliser certaines actions spécifiques en réaction aux alertes (contrôle, interpellation, intervention..), sur la base d'une première individualisation ou identification unique telle que décrite ci-dessus.

Dans tous les cas, le traitement aura comme fonction de « permettre » (pour reprendre les termes de la définition) l'identification unique de la personne, de façon différée. Les agents ayant accédé à l'information issue des traitements s'en serviront vu qu'ils cherchent à agir sur la personne et donc à l'identifier, que ce soi par une reconnaissance ou le relevé de son identité civile in fine.

Cet aspect du projet de loi est le plus choquant, à la fois sur le plan juridique et politique, en ce que le gouvernement tente de se soustraire à une définition et un régime bien ancrés dans le droit de l'Union européenne. Il est impératif que le débat soit replacé vu pour ce qu'il est et que le Parlement discute de la réalité juridique que recouvrent les dispositifs prévus par l'article 7, en l'occurrence la mise en œuvre de traitement de données biométriques des personnes filmées.

2. Une protection élevée

La question de la protection des données biométriques dans les dispositifs de vidéosurveillance automatisée est d'ailleurs actuellement porté au niveau judiciaire par des actions en cours contre les dispositifs de Marseille [63] (devant le tribunal administratif de Marseille), Moirans[64] (devant le tribunal administratif de Grenoble) et Vannes[65] (devant le tribunal administratif de Rennes) afin de faire affirmer durablement cette interprétation dans la jurisprudence. L'ensemble de ces affaires contentieuses devraient donner lieu à des décisions au cours de l'année 2023.

63 Voir le résumé de la procédure dans cet article en date du 11 octobre 2022 et accessible à https://www.laquadrature.net/2022/10/11/face-a-la-justice-la-mairie-de-marseille-defend-la-video-surveillance-algorithmique/

64 Mediapart, « *Vidéosurveillance : Moirans, cité de la démesur*e » publié le 8 mai 2022 et accessible à https://www.mediapart.fr/journal/france/080522/videosurveillance-moirans-cite-de-la-demesure

65 Lire cet article du 4 janvier 2023 Télégramme en date du et accessible à https://www.letelegramme.fr/morbihan/vannes/un-avocat-attaque-en-justice-la-politique-de-videosurveillance-de-vannes-et-ses-cameras-augmentees-04-01-2023-13252854.php

Enfin, au niveau politique, les débats en cours autour du projet de règlement européen relatif à l'intelligence artificielle intègrent l'ensemble de ces considérations afin d'évacuer les possibles barrières d'interprétation de la définition actuelle du RGPD.

D'une part, le projet de règlement consacre les nouvelles définitions de « catégorisation biométrique » et « reconnaissance des émotions ». De plus, des amendements actuellement discutés ont pour but d'intégrer une nouvelle notion de « biometrics-based data » (données fondées sur la biométrie) afin d'inclure les données corporelles ou comportementales qui n'ont pas pour but de permettre ou confirmer l'identification unique.

Ces ajouts, proposés notamment par les rapporteurs du texte, ont pour but d'écarter tout débat stérile sur l'étendue du périmètre des traitements biométriques et consacrer la protection claire et ferme du droit européen sur les données du corps humain. Pour saisir la complexité et l'étendue des réflexions sur la notion de données biométriques, nous vous invitons à vous reporter aux travaux de la Professeure Gloria Gonzalez Fuster, qui a notamment écrit un rapport] complet sur le sujet pour le Parlement européen[66].

D'autre part, l'approche générale du Conseil, publiée en décembre 2022, intègre une définition des données biométriques beaucoup plus large, **qui n'est pas conditionnée à une finalité de permission ou confirmation de l'identification unique**[67].

B. Une « proportionnalité » et une « nécessité absolue » indémontrables pour les JO

La vidéosurveillance automatisée que le projet de loi veut autoriser est, ainsi, contraire au droit de l'UE, notamment en ce que ces dispositifs biométriques ne respectent pas l'exigence de « nécessité absolue » et qu'ils consistent en des décisions automatisées. Nous attirons ainsi particulièrement votre attention sur le fait que la France se mettrait directement en situation d'infraction au droit de l'Union européenne si elle venait à adopter l'article 7 de ce projet de loi.

1. Le contrôle de proportionnalité, un cadre impératif à ne pas abandonner

Le droit des données personnelles pose une exigence de proportionnalité (article 5, 1., c du RGPD ; article 4, 1, c de la directive « police-justice » et

66 « *Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence* » publié le 16 décembre 2021 et accessible à https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)697191

67 Voir article 3, §33 de la position, accessible à https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf

article 4, 3° de la loi Informatique et Libertés) : tout traitement de données personnelles doit être proportionné à l'objectif poursuivi, c'est-à-dire que les données traitées doivent être adéquates (permettre effectivement de poursuivre la finalité), nécessaires (il ne doit pas être possible de traiter d'autres données) et non-excessives. Ce principe est parfois appelé celui de « minimisation des données »[68].

Cette exigence de nécessité est renforcée pour les traitements de données biométriques, compte tenus de leur gravité et dangers intrinsèques, qui doivent respecter une exigence de « nécessité absolue » selon les dispositions de la directive « police-justice », transposée à l'article 88 de la loi Informatique et Libertés. Il s'agit donc d'un contrôle de proportionnalité volontairement rigoureux.

En pratique, cette exigence signifie que le traitement ne peut être considéré comme licite que s'il n'existe **aucun autre moyen moins attentatoire aux libertés qui permettrait d'atteindre l'objectif poursuivi**. Cette exigence de nécessité absolue n'est pas une nouveauté juridique et a déjà permis de limiter ou interdire les technologies les plus intrusives.

Par exemple, lorsque la région PACA avait tenté de mettre en place une expérimentation de reconnaissance faciale à l'entrée de deux lycées, la CNIL avait jugé que la finalité de sécurisation et de fluidification des entrées au sein des lycées « *peut incontestablement être raisonnablement atteinte par d'autres moyens* », concluant que le dispositif était disproportionné.

De la même manière, dans un avertissement à la ville de Valenciennes révélé par Mediapart, la CNIL avait jugé que le dispositif de vidéosurveillance automatisée mis en place par la ville était disproportionné, notamment car la nécessité n'avait pas été prouvée et l'absence d'alternative n'avait pas été documentée[69].

Le Conseil d'État avait fait le même raisonnement lorsque il s'est penché sur l'utilisation des drones par la police lors des manifestations. Pour les juges, le ministre de l'intérieur n'apportait « *pas d'élément de nature à établir que l'objectif de garantie de la sécurité publique lors de rassemblements de personnes sur la voie publique* ***ne pourrait être atteint pleinement, dans les circonstances actuelles, en l'absence de recours à des drones*** »[70].

68 Courrier révélé par Mediapart, «*La Cnil juge illégale la reconnaissance faciale à l'entrée des lycées* », 28 octobre 2019, accessible à https://www.mediapart.fr/journal/france/281019/la-cnil-juge-illegale-la-reconnaissance-faciale-l-entree-des-lycees

69 Avertissement publié par Mediapart, «Vidéosurveillance : Valenciennes et son modèle de « safe city » hors la loi », 1er aout 2021, accessible à https://www.mediapart.fr/journal/france/010821/videosurveillance-valenciennes-et-son-modele-de-safe-city-hors-la-loi

70 CE, 22 décembre 2020, La Quadrature du Net, n° 446155, Rec. T. p. 750, pt. 11, disponible sur https://www.legifrance.gouv.fr/ceta/id/CETATEXT000042729524

Enfin, ce critère de nécessité a aussi été efficacement mobilisé contre la vidéosurveillance dite « classique », c'est-à-dire non biométrique. Dans un arrêt du 9 novembre 2018 déjà cité, la cour administrative d'appel de Nantes a ainsi rappelé que « *la mise en œuvre de tels systèmes de surveillance doit être assortie de garanties de nature à sauvegarder l'exercice des libertés individuelles. Dès lors leur autorisation suppose qu'une* ***telle mesure soit nécessaire et proportionnée à la préservation de l'ordre public.*** »

Cet arrêt exigeait que la proportionnalité soit prouvée au moyen notamment de statistiques de délinquance de la commune pour déterminer si la zone était exposée à des risques d'agression ou de vol (le passage de la décision est précité dans la partie **II**).

La structure d'expérimentation proposée ici par le gouvernement tente de s'affranchir de cet examen de proportionnalité, en posant un principe de légalité de certains usages et circonstances préétablies ?

Or, il est certain que pour une utilisation par des services de sécurité ou de police, il y aura toujours d'autres moyens d'assurer la sécurité autrement que par une technologie automatisée analysant le comportement des individus dans l'espace public, extrêmement intrusive et attentatoire à la vie privée. Et ce, aussi bien pour les caméras fixes que pour les drones. Jamais le gouvernement ne démontre dans son étude d'impact que la prévention des risques ne pourrait pas être assurée par des méthodes « classiques » de sécurité qui ne nécessitent pas de mettre en œuvre une technologie de surveillance et d'analyse de comportements à grande échelle.

Si l'on appliquait la mise en balance exigée par le contrôle de proportionnalité, le résultat de l'équation entre, d'une part, l'atteinte aux libertés et, d'autre part, la nécessité de l'objectif, exclurait tout dispositif de vidéosurveillance abusif puisque l'atteinte à la vie privée engendrée par le traitement de données biométriques ne pourra que très rarement, voire jamais, être évaluée comme absolument nécessaire pour atteindre l'objectif poursuivi.

Ce critère de nécessité absolue est donc aujourd'hui un mécanisme juridique documenté et efficace pour interdire une utilisation non propice et abusive de ces technologies de surveillance de l'espace public. Accepter de légaliser en amont ces expérimentations, alors qu'aucune preuve de l'effectivité de ces technologies ne permet de satisfaire un contrôle de proportionnalité classique, reviendrait à abandonner le socle fort de protection des données personnelles qui repose sur cet examen de la nécessité absolue.

2. L'impasse de la légalisation par usage

L'approche du projet de loi, qui vise à autoriser des dispositifs de vidéosurveillance automatisée selon des risques pré-identifiés et des usages déterminés par décret, ne répond qu'à des intérêts industriels et économiques, et non à une logique de protection des libertés publiques, qui elle repose toujours sur le principe de proportionnalité. Cette approche doit donc être fermement rejetée.

Cela avait d'ailleurs été le cas au moment de l'adoption du RGPD, au regard des faiblesses qu'elle entraînerait pour le droit des personnes. Le G29 était clair : « *les droits accordés à la personne concernée par le droit européen doivent être respectés quel que soit le niveau des risques que ces dernières encourent du fait du traitement des données concerné* »[71] (Traduction libre, §2). « *Les principes fondamentaux applicables aux responsables du traitement doivent rester les mêmes, quels que soient le traitement et les risques pour les personnes concernées* » (Traduction libre, §4).

Mettre de coté la notion de « nécessité absolue » en adoptant une approche par les usages ferait reposer la charge de la preuve sur les personnes concernées par la surveillance, qui devront démontrer a posteriori que leur est causé un dommage par ces expérimentations, au lieu de la faire reposer sur le législateur et le pouvoir exécutif. Or, il ne suffit pas qu'une technologie soit « peu risquée » pour que celle-ci devienne « nécessaire », ni même souhaitable.

Afin de défendre cette logique, le gouvernement tente de présenter des garanties pour limiter ces risques. Comme nous l'avons exposé ci-avant, les garanties techniques sont inadaptées au regard des processus de fabrication et de fonctionnement de ces systèmes. Mais, surtout, sur le plan juridique, nous voyons depuis plusieurs années que l**es garanties ne suffisent jamais à limiter des technologies** la plupart du temps déjà déployées, parfois à grande échelle, alors mêmes qu'elles ne sont pas légales. Quand bien même elles seraient contestées, elles auront déjà commencé à produire leurs effets illicites et nocifs.

Les analyses d'impact, les pouvoirs de contrôle de la CNIL, les soi-disant contre-pouvoirs locaux, les droits d'information du public, aucune de ces garanties n'empêche les autorités de violer la loi. À notre échelle, les actions contentieuses que nous portons concernent toujours des projets déjà autorisés ou mis en place, et qu'aucun garde-fou prévu par la loi n'a permis d'empêcher. L'exemple le plus significatif étant l'intervention tardive de la CNIL contre l'installation de portiques de reconnaissance faciale dans des lycées mentionnée ci-dessus, ou l'absence de sanction contre le déploie-

71 Voir Opinion 14/EN WP 218, 30 mai 2014 accessible à https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

ment actuel de dispositifs de surveillance sonore de la ville d'Orléans plus d'un an après la plainte devant la CNIL (en plus de notre recours devant le TA d'Orléans)[72].

S'il fallait une démonstration de l'absence, en pratique, de barrière au développement de technologies de surveillance illégales, notons l'aveu du ministre de l'intérieur le 25 octobre 2022. Au cours d'une audition[73] au Sénat, celui-ci a concédé que les dispositifs de vidéosurveillance automatisée actuellement mis en œuvre par les villes étaient illégaux, sans pour autant appeler à les arrêter malgré les incidences graves sur les droits des personnes filmées, et ce malgré l'obligation que le ministre a, en application du deuxième alinéa de l'article 40 du code de procédure pénale, de signaler au procureur de la République ces délits.

En outre, le projet de loi ne donne à la CNIL que des prérogatives de contrôle extrêmement faibles, qui ne sont pas à la hauteur des dangers de ces technologies. La Commission est pourtant la seule autorité à pouvoir correctement appréhender le fonctionnement de ces dispositifs ainsi que faire appliquer les règles de protection des données personnelles. Or, elle ne dispose d'aucun pouvoir contraignant dans l'ensemble du processus d'expérimentation, qu'il s'agisse du décret d'autorisation de l'expérimentation (au IV, il s'agit d'un avis uniquement consultatif), dans la décision du représentant de l'État ou du préfet de police de mettre en œuvre le système (au VI, cette décision lui est simplement adressée) ou dans le suivi de expérimentation (au VII, le préfet tient la Commission au courant « au tant que besoin », c'est-à-dire d'une manière pleinement discrétionnaire).

Cette critique n'a pas pour objet de réclamer l'attribution de davantage de pouvoirs à la CNIL puisque nous souhaitons le retrait de l'ensemble du cadre d'expérimentation. Mais nous souhaitons démontrer par là l'absence de volonté politique de prévoir de réels garde-fous au déploiement de ces technologies. Le gouvernement préfère au contraire accompagner leur développement de façon opaque et centralisée autour du pouvoir exécutif, plutôt que de protéger les droits des citoyens en multipliant les garanties.

72 69. Voir notre article « Surveillance sonore : LQDN attaque l'expérimentation d'Orléans », publié le 14 décembre 2021 et accessible à https://www.laquadrature.net/2021/12/14/surveillance-sonore-lqdn-attaque-lexperimentation-dorleans/

73 Extrait précité de l'audition de M. Gérald Darmanin sur la sécurité des jeux Olympiques et Paralympiques de 2024 accessible ici : https://video.lqdn.fr/w/m7tt1cpdvc8nKA4eMumfoZ

C. La nécessité d'une interdiction

Demain comme aujourd'hui, **seules les mesures d'interdiction, fondées notamment l'absence de nécessité, pourront protéger les libertés publiques et ne pas risquer de basculer dans un État de surveillance**. C'est d'ailleurs l'avis[74] de autorités européennes de protection des données (Comité européen pour la protection des données et Contrôleur européen pour la protection des données) sur le projet de règlement sur l'intelligence artificielle, qui appellent toutes deux à interdire complètement deux choses :

- D'une part, *« **toute utilisation de l'IA en vue d'une reconnaissance automatisée des caractéristiques humaines dans des espaces accessibles au public**, tels que les visages, mais aussi la démarche, les empreintes digitales, l'ADN, la voix, la pression sur des touches et d'autres signaux biométriques ou comportementaux, dans tous les contextes. »* (§32).

- D'autre part, la **catégorisation biométrique** « tant pour les autorités publiques que pour les entités privées » c'est-à-dire « *des **systèmes d'IA classant les individus à partir de données biométriques** (par exemple, à partir de la reconnaissance faciale) dans des groupes en fonction de l'origine ethnique, du sexe, ainsi que de l'orientation politique ou sexuelle, ou d'autres motifs de discrimination* » (§33).

Nous vous interpellons également sur le fait qu'actuellement, ces interdictions sont soutenues et poussées par un grand nombre de parlementaires européens dans les discussions en cours sur le règlement relatif à l'intelligence artificielle. Par cette loi, la France s'inscrirait donc encore plus à contre courant des volontés protectrices des institutions européennes[75].

Ce mouvement au niveau européen repose sur la prise en compte du rapport de force entre les citoyens et l'État et du pouvoir que ces technologies confèrent en terme de volume d'information et de pouvoir de décision sur la population. Dans le même avis, le Comité européen pour la protection des données et Contrôleur européen pour la protection des données affirment de façon forte et puissante que :

« *Le fait d'être déterminé ou classé par un ordinateur quant à son comportement futur, indépendamment de sa propre volonté, porte également **atteinte à la dignité humaine**. Les systèmes d'IÀ destinés à être employés*

74 Avis 05/2021 du 18 juin 2021 accessible à https://edps.europa.eu/system/files/2021-10/2021-06-18-edpb-edps_joint_opinion_ai_regulation_fr.pdf

75 Voir Silicon Republic, « *EU lawmakers are calling for a full ban on biometric surveillance* » publié le 10 novembre 2022 et accessible à https://www.siliconrepublic.com/enterprise/eu-biometric-surveillance-ban-ai-act ainsi que cet article de l'association EDRi, « *European Parliament calls loud and clear for a ban on biometric mass surveillance in AI Act* » publié le 14 septembre 2022 et accessible à https://edri.org/our-work/european-parliament-calls-loud-and-clear-for-a-ban-on-biometric-mass-surveillance-in-ai-act/.

*par les services répressifs pour effectuer des évaluations individuelles des risques sur des personnes physiques afin d'évaluer le risque qu'une personne physique se rende coupable d'une infraction pénale ou de récidive ou pour prédire la survenance ou la répétition d'une infraction pénale réelle ou potentielle sur la base du profilage d'une personne physique ou de l'évaluation des traits et caractéristiques de la personnalité ou du comportement infractionnel passé utilisés en fonction de leur destination, conduiront à une sujétion majeure de la prise des décisions policières et judiciaires, r**éduisant ainsi l'être humain concerné à l'état d'objet**. » (§ 34 de l'avis joint précité).* »

C'est ici tout l'enjeu du débat qu'il vous revient de trancher avec ce projet de loi : **accepter ou non un changement de dimension de la surveillance** en autorisant l'État à analyser, classer, évaluer les mouvements et comportements de chaque individu dans l'espace public. En lui donnant des pouvoirs de décision décuplés par l'automatisation de la prise d'information, ce projet change également la perception que l'État a de ces citoyens, qui deviennent uniquement des facteurs mathématiques de dangerosité à placer sur une échelle de risques.

Conclusion

En conclusion, la vidéosurveillance algorithmique constitue une technologie dangereuse pour les libertés et ne devrait pas être adoptée dans la précipitation. Comme le dit la CNIL dans son avis sur le projet de loi « *Le déploiement, même expérimental, de ces dispositifs constitue un tournant* » et « *regrette d'avoir à se prononcer en urgence* ». En dépit de ce constat, que nous partageons, la CNIL préfère réguler par les usages en se confinant à un rôle d'accompagnement des entreprises. Cette position ne fait qu'accentuer son désengagement des sujets de surveillance étatique, qu'elle se doit de réinvestir pour conserver sa fonction de gardienne des libertés publiques.

Ce projet de surveillance place la France dans une position isolée au sein de l'Union européenne et **confirme la distance qu'elle prend vis à vis des règles protectrices de l'Union européenne** (comme elle l'a fait pour l'encadrement de la surveillance des métadonnées). En outre, les fondements et motivations du projet de loi confirment le rapprochement avec d'autres États plus enclins à recourir à des technologies de surveillance, tels que la Chine que l'on met artificiellement à distance avec un imaginaire lointain et repoussant. Certes, la réalité du régime et les pratiques étatiques diffèrent, l'étendue de la vidéosurveillance (avec 372 caméras pour 1 000 habitants en moyenne) sans commune mesure avec l'Europe. Pourtant, on retrouve dans les politiques techno-sécuritaires adoptées par la France ces dernières années une logique similaire.
Pour chaque problème de sécurité, la solution immédiatement proposée repose dans la surveillance numérique de la population et l'augmentation des pouvoirs de contrôle. À coté, la croyance dans l'innovation et le progrès ne souffre d'aucune critique et on observe un refus permanent de remise en question de l'objectif et de l'efficacité des dispositifs. Enfin, les enjeux des libertés et du modèle de société que l'on construit avec ces technologies sont inaudibles et systématiquement mis en second plan.

De notre côté, nous demandons la suppression pure et simple de l'article 7 de la proposition de loi sur les Jeux olympiques. Depuis de nombreuses années, ces technologies sont déployées illégalement sur le territoire et les industries de la sécurité font pression pour que leurs technologies puissent être légalisées et donc commercialisables. Un tel changement de société ne devrait pas être justifié par l'urgence supposée d'un évènement sportif, masquant en fait des enjeux économiques.

En ce que les dispositifs de VSA touchent directement au corps humain et portent atteinte à la dignité humaine, ils ne peuvent pas être autorisés au prétexte d'un évènement sportif, surtout lorsque aucune démonstration de leur utilité pour prévenir des atteintes à la sécurité n'est fournie. S'il

devait y avoir un quelconque débat pour encadrer ce dispositif de surveillance, il devrait être à la mesure des bouleversements qu'il engendrerait dans la société. À titre de comparaison, **les lois de bioéthique** – qui constituent d'ailleurs une spécificité procédurale française – sont un exemple d'**outil législatif prenant la mesure des changements philosophiques et politiques induits par l'apparition de nouvelles technologies**. Même si on peut là encore en critiquer la faible portée pratique, au moins ces lois sont-elles prises selon un échéancier spécifique permettant un temps long de réflexion, la tenue d'états généraux ainsi que le suivi par une autorité spécifique, le Comité consultatif national d'éthique, avec (et bien qu'elle soit là encore insuffisante) une volonté de prise en compte de la société civile dans ce processus. À l'inverse, en faisant passer son texte à toute vitesse et en utilisant un prétexte de circonstance (les JO) pour rendre la violation des libertés plus acceptable, **le gouvernement s'inscrit à rebours de cette logique d'inclusion démocratique des citoyens** (alors que comme nous l'avons exposé, ceux-ci ont démontré toute leur opposition à la VSA, notamment au travers de la plainte collective que nous avons déposée devant la CNIL) **et du rôle du Parlement** dans la discussion des changements de sociétés. **La fuite en avant techno-sécuritaire ne peut-elle donc souffrir d'aucun réel débat démocratique ?**

Au-delà même de la qualité du débat, nous restons convaincu qu'il est de notre responsabilité collective de refuser le déploiement de technologies telles que la vidéosurveillance automatisée. Il existe des moments dans l'histoire où nous devons décider que certaines technologies sont trop dangereuses. Et c'est alors le rôle du législateur que de les interdire. L'exemple du clonage, pour lequel les débats ont abouti à choisir son interdiction au regard de ses dangers intrinsèques constitue ici un parallèle intéressant.

Plutôt que de discuter des modalités d'un « encadrement approprié », nous exprimons donc notre refus vis-à-vis de ces technologies. Nous pensons à nos grand-mères et à nos grand-pères qui, s'ils avaient du vivre au début des années 1940 dans un monde saturé de vidéosurveillance automatisée, n'auraient pas survécu plus de trois semaines dans la clandestinité, et n'auraient donc pas pu organiser des réseaux de solidarité dissidents pour résister au régime nazi. **Il est des technologies qui sont par essence incompatibles avec la défense de formes de vie démocratique. La VSA en fait partie.**

Nous défendons donc le maintien du cadre juridique actuel, qui permet l'interdiction de la vidéosurveillance automatisée et est à même de protéger la population contre les abus des autorités en matière de surveillance et appelons à rejeter l'article 7.