Refuser la vidéo-surveillance algorithmique (VSA)

Le projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 contient un article 7 qui vise à légaliser – via un cadre dit « d'expérimentation » - le déploiement et la mise en oeuvre des dispositifs de vidéosurveillance algorithmique (VSA). La Quadrature du net a écrit une lettre pour alerter les députés sur les dangers de cette loi pour nos libertés.

Le choix des Jeux n'est sans doute pas anodin. Les politiques ont souvent profité de moments extraordinaires pour expérimenter des technologies de surveillance, avec des « mesures d'urgence temporaires », mais systématiquement inscrites par la suite dans le droit commun.

Table des matières

1. Aspects techniques

La VSA est une automatisation du travail d'analyse des images de vidéosurveillance (autrefois fait par des agents), grâce à un logiciel qui produit des notifications lorsque qu'il détecte un événement qu'on l'a entraîné à reconnaître. La reconnaissance faciale ne fait pas partie de la VSA, qui reconnait des corps, des mouvements et non des visages. Ce logiciel (IA) est basé sur une technologie d'apprentissage qui permet d'isoler des informations signifiantes à partir d'images (photos ou vidéos).

L'apprentissage consiste à entraîner les algorithmes à détecter automatiquement, à partir de milliers d'enregistrement de caméras de vidéosurveillance, certaines catégories *d'objets* (une valise, des ordures, …), de *personnes* (allongées sur le sol, statiques trop longtemps, non masquées, correspondant à une certaine silhouette recherchée ou portant certains habits, …) ou *d'événements* (franchissement d'une ligne, bagarre, rassemblement, cambriolage, …).

Les deux fonctionnalités les plus mises en avant sont *la production d'alertes en temps réel* (situations suspectes) et *l'automatisation de recherches et de « résumés vidéo » a posteriori* dans les archives vidéo (p.ex. les hommes portant un t-shirt jaune et un pantalon noir dans une zone géographique donnée durant les dernières 24h ou alors tous ceux qui ressemblent à une certaine photo).

1.1 Comment fonctionnent ces algorithmes VSA ?

Dans cette partie, nous allons détailler la construction et le fonctionnement des algorithmes de la VSA, en mettant en relief les choix politiques.
Pour pouvoir faire de la reconnaissance sur des vidéo, il convient de traduire ces informations (flux de pixels) en informations statistiques manipulables qu'on appelle **caractéristiques**. Exemple : imaginons qu'on veuille trouver les éléments les plus probables dans l'image d'un chat. L'humain va se limiter à quelques caractéristiques comme les moustaches et les oreilles pointues, mais la VSA va détecter d'autres caractéristiques invisibles à l'homme, comme un certain contraste produit par les pixels du pelage. Elle retiendra les plus probants.

Phases d'apprentissage de la VSA

Il y a différents niveaux de choix politiques dans l'apprentissage de la VSA qui portent sur:

a) le jeu de données et la labellisation
b) les corrections du logiciel et choix définitif des caractéristiques du modèle
c) l'usage de cet algorithme à des fins particulières

a) Choix du jeu de données et labellisation

Pour entraîner les VSA, ce sont des millions d'heures d'images de personnes et de traitements de données personnelles, aussi diversifiées que celles auxquelles les algorithmes seront effectivement exposés (espaces publics et privés), qui doivent être collectées, rassemblées et traitées.

Le choix du jeu de données influence fortement les décisions finales de l'algorithme. Deux jeux différents produiront des résultats différents. Par exemple, si vous alimentez une VSA avec des vidéos de rixes avec des Noirs, le programme déduira qu'une caractéristique des rixes est la couleur de peau. Or ce choix est du ressort des politiques.

Le fait de graver des décisions politiques dans la configuration du logiciel en choisissant un jeu de données représente un choix comparable à l'action du législateur. Ceci donne un pouvoir énorme à la police.

Pour caractériser certains évènements ou personnes, la méthode de labellisation est utilisée, c'est-à-dire que des images sont associées à un label, comme « violence de rue », « taggage », « manifestation » etc.

La labellisation donne aussi un pouvoir arbitraire aux politiques.

b) Correction du logiciel et choix définitif des caractéristiques du modèle

Les jeux de données ont fourni un ensemble de caractéristiques des objets recherchés.

La suite de l'apprentissage de la VSA consiste à la mettre en situation réelle pour qu'une fonction d'optimisation décrive et localise les erreurs logicielles, puis les corrige automatiquement, jusqu'à ce que le résultat soit satisfaisant.

Les caractéristiques des objets (la plupart définies par l'algorithme lui-même) sont ensuite affinées par un humain pour arriver au résultat le plus précis. Par exemple, la base de données peut contenir beaucoup de personnes en survêtement en train de commettre un acte délictueux et la VSA infèrera que porter ce vêtement est un facteur de risques, ce qui devrait être corrigé.

c) Choix d'usage de l'algorithme

Une fois que l'algorithme est prêt, il **faut le lier à une application (interface homme-machine) pour les agents**. Par exemple, générer une alerte sur un choix d'évènements ou de combinaisons d'évènements, signaler une zone en couleur sur une carte, appeler une brigade etc. Il peut s'agir de quelqu'un qui court, un rassemblement, une personne allongée, une personne qui écrit sur un mur, etc. **Le choix politique de demander à l'algorithme de repérer ces types de comportements à un sens et des conséquences sur l'action policière**.

Le résultat de toutes ces opérations a), b) et c), coûteuses en temps de travail, a énormément de valeur et a vocation à être ensuite vendu à un ensemble de clients.

On comprend, d'après ce qui précède, qu'il importe peu que les données d'entraînement soient supprimées ou anonymisées, le résultat auquel elles ont abouti sera conservé (configuration + logiciel) et pourra servir à une multitude d'applications chez divers clients.

Certains programmes mémorisent les données de leur apprentissage, ce qui représente une atteinte potentiellement grave à la vie privée .

1.2 Les « garanties » de l'Etat pour les données sensibles

L'expérimentation proposée par le gouvernement tente de s'affranchir de certains examens de proportionnalité, en posant un principe de légalité de certains usages, càd que la VSA ne serait appliquée que dans certains cas menaçant l'ordre public mais pas pour la surveillance des citoyens, en y apportant certaines « garanties ».

Impossibilité technique de protéger les données sensibles

L'article 7 prévoit comme garantie que les données d'apprentissage soient « pertinentes, adéquates et représentatives ». Ces garanties semblent en décalage avec la réalité du machine learning.

- 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.
- 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. L'algorithme peut utiliser des données sensibles comme caractéristique d'un évènement (exemple : être jeune pour un graffeur)

L'article 7 prévoit également comme garantie que le traitement de ces données doit être « loyal, objectif et de nature à identifier et prévenir l'occurrence de biais et d'erreurs. » Or c'est le politique qui introduit des biais dans l'apprentissage, puis dans le logiciel adapté pour les reconnaître.

Opacité due à la complexité des calculs

L'article 7 prévoit comme garantie que soient automatiquement enregistrés les « évènements permettant d'assurer la traçabilité du fonctionnement de l'algorithme ».

Pour effectuer tous les calculs que nécessite l'analyse des images vidéo, le « machine learning » et le « deep learning » sont structurés en nombreuses couches de réseaux neuronaux. **Cette immense complexité rend les algorithmes totalement opaques dans leur fonctionnement**, y compris pour les data scientists qui les manipulent, ce qui ne permet pas d'avoir une utilisation respectueuse des droits de la personne. Cette garantie légale est donc inopérante.

1.3 Les algorithmes sont développés par des entreprises privées

Des entreprises privées définissent la normalité dans l'espace public

Ce sont des entreprises privées qui vendent ces logiciels aux collectivités et définissent ce qu'il est possible de détecter avec la VSA. Il s'agit donc d'une forme de délégation au privé (donc aux intérêts marchands) de la définition l'ordre public et de nos libertés.

Le marché de la vidéosurveillance est en plein essor (10% de croissance par an de prévu). Il représentait 45 milliards d'euros en 2020 et pourrait représenter jusqu'à 75 milliards d'ici 2025.

La vidéosurveillance : un marché économique en plein boom

La vidéosurveillance algorithmique est investi par une panoplie d'acteurs : les grandes multinationales du Big Data comme IBM (30 caméras VSA à Toulouse); les industriels de la sécurité comme Thalès, largement soutenus par les subventions publiques (expérimentation Safe City à Nice et La Défense ou encore la SNEF à Marseille) ; enfin, les start-ups comme Aquilae (projet VSA JOP2024 sur Paris), ou Two-I (reconnaissance faciale au stade municipal de Metz).

1.4 L'opacité des expérimentations VSA entretenue par l'Etat

Il est très difficile d'avoir accès aux documents administratifs sur l'installation de ces technologies sur le territoire français, malgré les saisines de la CADA.

Par exemple, la municipalité de Dijon n'a jamais répondu aux demandes de la Quadrature du Net depuis plus de deux ans. De son côté, Marseille, ville pionnière dans le développement illégal de la VSA, refuse méticuleusement de fournir des informations sur ses expérimentations.

À cela s'ajoute le fait que les collectivités n'ont pas besoin de justifier leurs objectifs pour les déploiements.

1.5 La recherche publique finance les technologies VSA illégales

S'agissant des Jeux 2024, **l'Agence Nationale de la Recherche (l'ANR) a financé la vidéosurveillance algorithmique à hauteur de plusieurs millions d'euros.**

Dans un appel à projet « Flash » de 2020, nous apprenons que 6 projets ont été sélectionnés, qui visent à développer des algorithmes capables de détecter des comportements anormaux dans 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 critiques ou sécuriser l'accès via la reconnaissance faciale.

1.6 L'État subventionne le déploiement de la vidéosurveillance

L**e ministre de l'intérieur incite à installer des caméras de vidéosurveillance** dotées de ces technologies illégales en les finançant à travers le Fonds interministériel de prévention de la délinquance (FIPD). 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.

Également, la circulaire du 11 février 2022 relative aux orientations budgétaires des politiques de prévention de la délinquance et de la radicalisation pour 2022 incite clairement les collectivités locales à se doter de VSA via des subventions.

Le Livre blanc de la sécurité intérieure, qui dresse la feuille de route du ministère pour les prochaines années, est très clair dans son titre III « Porter le Ministère de l'Intérieur à la frontière technologique » avec les dispositions du rapport annexé à la LOPMI (casques et lunettes augmentés de policiers-robots, exploitation d'une multitude de données par intelligence artificielle, ou casques de « réalité augmentée » permettant d'interroger des fichiers en intervention).

Si la question de la légalisation de la vidéosurveillance 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.**

2. Aspects économiques de la surveillance de masse

Le dernier décompte du nombre de caméras de vidéosurveillance « classiques « (sans reconnaissance faciale ni VSA) par la CNIL date de **2012 et fait état de plus de 800 000 caméras sur le territoire national, dans des espaces publics ou privés. Ce chiffre a sans nul doute 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

2.1 Pas d'évaluation publique de la vidéosurveillance

Le projet de loi propose d'expérimenter la VSA 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 sa capacité d'analyse automatique d'images, alors que l'utilité des caméras de vidéosurveillance pour lutter contre la délinquance n'a jamais fait ses preuves.

2.2 De rares études pointent l'inutilité de la vidéosurveillance

Le rapport de la Cour des comptes de 2020 rappelle « qu'aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation ». Quant au laboratoire de recherche de la CNIL, le LINC, il affirme 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 du chercheur Guillaume Gormand, commandées par la gendarmerie, concluent, elles aussi à une absence d'effet sur le taux d'infractions 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).

2.3 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 l'achat de logiciels de gestion du parc de caméras, l'installation de nouvelles caméras, la transmission de flux, des capacités de stockage des données dans des serveurs assez puissants pour analyser des grandes quantités de données très rapidement.

- Sur le temps long, ces dispositifs 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.

Le ministère de l'Intérieur évoque pour les Jeux l'installation de 15 000 nouvelles caméras, pour 44 millions d'€ de financement du FIPD. **Une caméra de vidéosurveillance coûte 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 abonnement 4G/5G (autour de 9 000 € par an et par caméra).**

Avec l'ajout d'une nouvelle brique logicielle à ces systèmes, la VSA contribue à l'explosion des budgets de vidéosurveillance. À terme, outre l'achat de nouvelles licences logicielles aux startups et industriels du secteur, la VSA incitera les pouvoirs publics à se doter de nouvelles caméras haute définition.

S'agissant des enjeux budgétaires des Jeux, 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 433 à 481 millions € au lieu des 225 millions prévus.**

2.4 Le mythe de l'efficacité de la vidéosurveillance

La VSA 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 nécessaire pour faire face à la quantité de flux vidéo ainsi générée.

Le fiasco du Stade de France en mai 2022 est un bon exemple d'instrumentalisation d'un évènement à des fins de promotion de dispositifs de surveillance. La vidéosurveillance a été particulièrement inutile ce jour-là. Afin de masquer la désorganisation et la violence policière, le gouvernement pointe les solutions de reconnaissance faciale et de VSA, qui auraient évité les problèmes, alors que pour de nombreux observateurs, une gestion classique de la foule par des policiers habitués à aménager efficacement l'espace pour éviter les fortes concentrations, aurait sans doute été bien plus efficace.

Depuis des années, les industriels du secteur ne cessent de promettre que l'efficacité de la vidéosurveillance dépend d'un surcroît d'investissement. Mais ces promesses n'ont jamais été tenues.

Enfin, rappelons que la croyance dans la capacité des technologies à résoudre tous les problèmes n'a rien d'une nouveauté et a montré ses limites avec l'échec flagrant de l'application TousAntiCovid à 15 millions d'Euros.

2.5 L'échec de l'encadrement du déploiement de la vidéosurveillance

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 un 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 ». **Des conclusions qui, en creux, peuvent s'appliquer à l'immense majorité des déploiements de caméras**.

Il apparait clairement que le dispositif d'encadrement de la VSA esquissé par le projet de loi est incapable d'assurer une protection efficace des droits fondamentaux.

3. Aspects politiques de la 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.

3.1 Stigmatisation d'une catégorie de population

Comme tout système de surveillance de l'espace public, **la VSA surveille en priorité les personnes qui passent le plus de temps à l'extérieur.** Ce sont donc les populations les plus pauvres, qui ne voient pas la rue comme un « lieu de passage », mais un lieu où elles vivent, qui seront les plus repérées par les algorithmes, entraînés à détecter les comportements dits « anormaux » : maraudage, mendicité, réunions statiques… **Ce qui donnera lieu à une discrimination et une exclusion d'une partie de la population de l'espace public**.

La RATP a expérimenté dans les salles d'échange du RER des Halles un système pour repérer les personnes statiques pendant plus de 300 secondes.

3.2 Changement du rapport de la police à la société

La VSA accentue 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.
- Elle est aussi intellectuelle : les agents n'ont plus à comprendre ou à évaluer de leurs semblables. Peu importe que formellement la décision d'intervenir soit prise par un agent de police (obligatoire sur le fondement de l'article 22 du RGPD), les alertes de la VSA, qui reposent sur des choix politiques, ne sont pas neutres

En île-de-France, certaines familles ont reçu jusqu'à plusieurs dizaines de milliers d'euros d'amendes pour non port du masque, ou non-respect du confinement, sans qu'à aucun moment il y ait eu contrôle de leur attestation. Ce harcèlement des jeunes de quartiers populaires a été rendu possible par les caméras de vidéosurveillance. Le Défenseur des Droits a été saisi.

Cet exemple montre bien les abus qui peuvent arriver avec des caméras de vidéosurveillance au pouvoir contraventionnel. La VSA banalisera ces abus.

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 automatisée.

3.3 Tendance à la mise en data des humains

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.

Les industries de la sécurité privées font du profit sur les vies et les comportements des habitants d'une ville, afin d'améliorer leurs algorithmes de répression et ensuite les vendre sur le marché international. Les habitants sont transformés en cobaye pour le développement d'un produit de surveillance.

Ces technologies ainsi développées peuvent être mises au service de politiques violentes de certains pays ou détournées de leur usage premier.

3.4 Changement d'échelle dans la surveillance

La VSA 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 peu de ressource pour des activités moins prioritaires.
- Demain, la VSA promet d'effacer cette limite matérielle en décuplant les capacités opérationnelles de la police pour poursuivre toutes les missions de son choix, même celles peu légitimes ou constituant des abus. Par exemple le suivi visuel d'opposants politiques sur l'ensemble des caméras de la ville est rendu trivial par la VSA

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.

À ce jour, les rares tentatives de recueillir les avis de la population à propos de la vidéosurveillance algorithmique ont montré de vives inquiétudes. D'abord la consultation de la CNIL sur la VSA en mars 2022 a vu plus de 200 contributions de la société civile s'inquiétant du déploiement de tels dispositifs. Également, le défenseur des Droits a réalisé une enquête sur les Français et **souligne les risques considérables pour les droits fondamentaux si des technologies biométriques comme la VSA venaient à être généralisées.** Enfin, La Quadrature du Net a réuni plus de 15 000 signatures pour une plainte collective envoyée à la CNIL en septembre 2022.

4. Aspects législatifs

4.1 Les données biométriques uniques

Dans le Règlement Général de Protection des Données (RGPD) européen, le droit des données personnelles prévoit une protection particulière pour les données dites « sensibles » (telles que les orientations politiques ou sexuelles, les données médicales). Parmi ces données sensibles, on trouve la catégorie des données dites « biométriques », qui sont définies selon 3 critères, « 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 » (article 4§14 du RGPD et article 3§13 de la directive 2016/680 dite « police-justice»).

Or on retrouve bien ces 3 critères dans la VSA : il y a bien traitement technique des données par le caméra et l'algorithme, qui permet d'isoler, de caractériser une personne unique (physique, physiologique et comportementale). Il convient aussi de noter que la finalité de la VSA est de permettre à des agents humains de réaliser certaines actions spécifiques (contrôle, interpellation…) en réaction aux alertes du système, sur la base d'une première individualisation ou identification unique. **L'identification unique est donc inhérente au VSA et est soit immédiate, soit différée**.

Mais la partie III de l'article 7 du projet de loi affirme le contraire, que les 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 ». Or cette technologie, comme on l'a vu, permet tout à fait d'isoler une personne.

Même le **CEPD** (Comité Européen pour la Protection des Données, qui veille à l'application du RGPD sur le territoire de l'UE), dans ses Lignes directrices sur les vidéos contenant des données personnelles , précise que la notion d'identification unique 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 d'un environnement. **Ainsi, cette notion concerne également la classification de comportements sur la base d'une analyse des corps** (ce que fait la VSA). Une telle interprétation est partagée par le **Défenseur des droits** dans son rapport Technologies biométriques : l'impératif respect des droits fondamentaux de 2021, et dans l'enquête Perception du développement des technologies biométriques en France de 2022.

Dès lors, la partie III de l'article 7 du projet de loi, qui affirme que les algorithmes « ne traitent aucune donnée biométrique », rentre en contradiction avec des règles applicables de droit de l'Union européenne.

4.2 Actions judiciaires en cours

- Des actions judiciaires sur la question de la protection des données biométriques dans les dispositifs de VSA sont en cours à Marseille, Moirans et Vannes, afin de faire affirmer durablement cette interprétation d'identification unique biométrique. Ces affaires devraient donner lieu à des décisions au cours de l'année 2023.

- Une nouvelle proposition autour du projet européen de règlement relatif à l'intelligence artificielle est en cours de discussion, en y intégrant de façon claire les notions de « catégorisation biométrique », « reconnaissance des émotions » et d'inclure aussi les données corporelles ou comportementales qui n'ont pas pour but de permettre l'identification unique.

4.3 Les questions de « proportionnalité » et de « nécessité absolue »

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 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 ».

Cette exigence de proportionnalité est renforcée pour les traitements de données biométriques qui doivent respecter une exigence de « nécessité absolue » selon les dispositions de la directive « police-justice ». 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.

Ces exigences ont déjà permis de limiter ou interdire les technologies les plus intrusives.

- 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 le dispositif était disproportionné.
- La ville de Valenciennes avait tenté de mettre en place un dispositif de VSA, jugé à nouveau disproportionné par la CNIL.
- Le Conseil d'État avait fait le même raisonnement lorsqu' 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 de preuve de nécessité absolue de l'usage des drones.

Jamais le gouvernement ne démontre dans son étude que la prévention des risques ne pourrait pas être assurée par des méthodes « classiques » de sécurité, sans le déploiement d'une technologie de surveillance et d'analyse de comportements à grande échelle, extrêmement intrusive et attentatoire à la vie privée.

Ce critère de nécessité absolue est un mécanisme juridique documenté et efficace pour interdire une utilisation non propice et abusive de ces technologies de surveillance de l'espace public. 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.

4.4 La légalisation par « usage » tentée par le gouvernement

L'expérimentation proposée par le gouvernement tente de s'affranchir de cet examen de proportionnalité, en posant un principe de légalité de certains usages, càd que la VSA ne serait

appliquée que dans certains cas menaçant l'ordre public mais pas pour la surveillance des citoyens, en y apportant certaines « garanties » et du « peu de risques ».

Cela signifie que des personnes impactées par la surveillance devront elles-mêmes démontrer a posteriori le dommage causé, au lieu d'une règlementation en amont par le législateur. Et il ne suffit pas qu'une technologie soit « peu risquée » pour qu'elle devienne « nécessaire ».

Comme nous l'avons expliqué dans le 1er paragraphe (aspects techniques de la VSA), **il n'y a pas de garantie technique du fait des choix politiques arbitraires de l'apprentissage de la VSA et de l'obscurité des algorithmes.**

Sur le plan juridique, nous voyons depuis plusieurs années que **les 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. Ni le pouvoir de contrôle de la CNIL, ni les soi-disant contre-pouvoirs locaux, n'ont empêché les autorités de violer la loi. Un exemple significatif est l'absence de sanction de la CNIL contre le déploiement sauvage des caméras à reconnaissance faciale (à Nice notamment) interdites en France. Le Sénat lui-même, qui a reconnu l'illégalité du déploiement de la VSA dans certaines villes, n'a jamais appelé à les arrêter (Dijon, Toulouse, Vannes).

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, alors qu'elle est la seule autorité qui puisse faire appliquer les règles de protection des données personnelles. Elle ne peut donner qu'un avis consultatif et n'est mise au courant du suivi de l'expérimentation que de façon discrétionnaire (parties IV, V, VI et VII de l'article 7).

Le gouvernement préfère accompagner le développement de ces technologies de façon opaque et centralisée autour du pouvoir exécutif, plutôt que de protéger les droits des citoyens en multipliant les garanties verbales. Les intérêts économiques et industriels priment.

5. Conclusion : interdire la VSA

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 des autorités européennes de protection des données (CEPD) sur le projet de règlement sur l'intelligence artificielle, qui appelle 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).

Par cette loi, la France s'inscrirait donc encore à contre-courant des volontés protectrices des institutions européennes, soutenues par de nombreux parlementaires.

C'est ici tout l'enjeu du débat : 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.