

VSA



**VIDÉOSURVEILLANCE
ALGORITHMIQUE**

DANGERS ET CONTRE-ATTAQUE

Qu'on le veuille ou non, qu'on le sache ou non, les algorithmes dédiés à l'analyse automatique des flux de vidéosurveillance sont omniprésents dans notre quotidien. Sans qu'on n'ait notre mot à dire, cette « vidéosurveillance algorithmique », ou VSA, s'immisce subrepticement dans nos vies avec des conséquences dramatiques sur les libertés.

Le plus souvent, ces algorithmes sécuritaires brillent par leur invisibilité — leurs concepteurs s'appliquent consciencieusement à les faire disparaître dans le mobilier urbain, à dissimuler ces mécanismes d'automatisation, à les rendre les plus discrets possibles pour mieux banaliser leur présence et leurs effets en matière de contrôle social.

Cette technologie de VSA est un nouvel outil de contrôle donné à la police. Elle ajoute aux caméras parsemant les villes une couche logicielle pour analyser, classer, catégoriser nos corps et nos déplacements. Dans la droite ligne de l'imaginaire de la « Smart City », elle nourrit la fiction d'une ville parfaitement optimisée grâce à des capteurs vidéos et des algorithmes capables de tout mettre en données pour en tirer des prédictions et reconnaître des « signaux faibles ».

La VSA s'est développée ces dernières années et s'est installée dans les villes françaises en toute discrétion et en toute illégalité. Dans les réseaux d'acteurs faisant la promotion de la Technopolice (ministres, hauts fonctionnaires, industriels de la surveillance, ingénieurs en vision machine, etc.), on a redoublé d'ingéniosité pour élaborer des concepts de novlangue destinés à enrubanner les algorithmes des caméras, qui en un tour de passe passe deviennent des caméras « intelligentes et augmentées ». La vidéosurveillance se mue en « vidéo-protection », les algorithmes « optimisent » et « rationalisent » la répression policière. Au « pays des Lumières », on promet à longueur de temps d'« encadrer rigoureusement » ces technologies pour sauvegarder les « libertés individuelles ».

Sauf que derrière ces écrans de fumée, la VSA sert une idéologie : celle de la surveillance totale et de la répression systématisée.

Alors que, pour la première fois, s'amorcent à travers le pays des expérimentations « légales » de VSA permises par la loi relative aux Jeux Olympiques de Paris 2024, il apparaît crucial de déconstruire ces mythes et d'expliquer ce que recouvre politiquement et techniquement la surveillance algorithmique de nos corps par le truchement de la vidéosurveillance qui s'est démultipliée depuis vingt ans, et ce afin de mieux s'organiser pour résister et refuser ce projet sécuritaire.

Cette brochure propose d'ausculter la manière dont la vidéosurveillance algorithmique transforme notre rapport à la ville et dont elle impacte nos libertés. Elle est le fruit de plusieurs années de luttes de terrain, d'enquêtes, d'analyses et de contentieux juridiques, portées par La Quadrature du Net et les collectifs locaux Technoplice.

Son objectif consiste à redonner une matérialité aux algorithmes d'analyse des flux de vidéosurveillance tout en les resituant dans leur contexte historique, politique et économique. Parce que mieux nous pourrions comprendre ces dispositifs, mieux nous pourrions les débusquer, les contourner, les dénoncer, et ainsi tenir en échec le funeste projet de société dont ils relèvent. Pour ensuite imaginer ensemble un futur joyeux et lumineux, un horizon commun pour nos villes et nos villages, loin de la surveillance inhérente à la Smart City, et loin des pulsions morbides des cyber-flics de la Technoplice.

Table des matières

Préambule : la VSA, qu'est ce que c'est ?	8
I La VSA détruit nos villes et nos vies	11
A La VSA, produit d'un fantasme sécuritaire	13
B Mutation des pratiques policières	17
C Répression descorps, transformation du rapport à la ville	22
II L'empire de la VSA	29
A Une convergence d'intérêts	31
B Une avancée à visage masqué	36
C Fabrique de l'acceptabilité	43
III Le pire est à venir	49
A Un agenda politique ancien	51
B La loi « Jeux Olympiques », première brique légale hypocrite	56
C L'arbre qui cache la forêt	61
IV Riposter	69
Documenter	71
S'organiser	73
Agir	75
Reprendre la ville	76



Préambule :

la VSA, qu'est ce que c'est ?

La vidéosurveillance algorithmique (VSA) consiste en l'installation et l'utilisation par la police d'un logiciel qui analyse les images des caméras de vidéosurveillance afin de repérer, identifier ou classer des comportements, des situations, des objets ou des personnes en particulier.

Ces logiciels sont conçus par des **entreprises privées** et 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 spécifiques à partir d'images fixes ou animées. À travers des techniques d'« apprentissage machine » (l'une des méthodes associées à « l'intelligence artificielle »), les algorithmes **sont entraînés à détecter automatiquement** certains éléments.

Ces logiciels sont majoritairement utilisés **par la police** en lien avec les caméras de vidéosurveillance : soit pour de la détection

en temps réel de certains « événements », soit en différé dans le cadre d'enquêtes policières.

Les alertes « en temps réel », qui permettent à une plus petite équipe de repérer, dans une grande quantité de flux vidéos, des « événements » d'intérêt pour la police : le logiciel relève de manière automatique des situations perçues comme suspectes ou risquées et en notifie les agents présents dans le « centre de supervision urbain » (CSU), le local technique où sont acheminés les flux vidéos en vue de leur visionnage. En pratique, la VSA vise à détecter des **objets** (une valise, des ordures), des caractéristiques liées aux **personnes** (personnes allongées sur le sol, graffeurs, vêtements) ou encore des **événements** (franchissement d'une ligne, regroupement de personnes).

S'il est très facile d'effectuer une recherche dans un document texte, la tâche s'avère plus compliquée et chronophage lorsqu'il s'agit d'effectuer une recherche dans un flux vidéo. La VSA peut être utilisée en temps différé dans le cadre d'enquêtes pour **automatiser 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 détecter l'ensemble des hommes portant un t-shirt jaune et un pantalon noir repérés dans une zone géographique donnée durant les dernières 24h. La VSA peut également raccourcir le temps de visionnage en **condensant 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 une ellipse sur le reste du temps de vidéo.

Précisons que les deux utilisations de la VSA en direct et a posteriori **reposent sur le même procédé d'analyse automatisée** et qu'il n'y a donc **pas lieu de les distinguer d'un point de vue technique**.

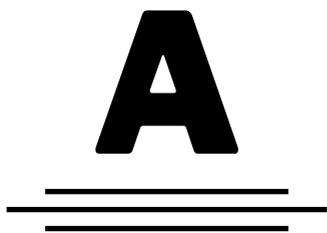
Ce travail d'analyse était jusque là effectué par des personnes, principalement des agents de la ville ou policiers municipaux dans les centres de supervision urbains (CSU) dans le cas des caméras de vidéosurveillance publiques.



**La VSA
détruit nos
villes et nos vies**

La vidéosurveillance algorithmique transforme profondément notre rapport à la ville. En cela, elle s'inscrit dans une vision politique ancienne de l'espace public vu comme lieu de sécurité et de contrôle des corps. En pratique, **elle modifie la manière dont nous y faisons société en renforçant les normes sociales visant à exclure les plus précaires et en donnant à la police une capacité nouvelle et considérable de répression.**





La VSA, produit d'un fantasme sécuritaire

Si les algorithmes de détection des comportements peuvent aujourd'hui se faire une place dans l'arsenal de surveillance, c'est notamment dû à **l'héritage d'une vision sécuritaire de la ville et de la société**, ancrée depuis plusieurs décennies dans le paysage politique.

■ « L'insécurité » comme moteur idéologique

L'argument principal invoqué pour déployer la VSA est le même que celui qui a conduit à l'installation de caméras de surveillance dans l'espace public : **lutter contre l' « insécurité »**. Ce terme ne renvoie à aucun fait concret ni à une évaluation précise du niveau de la délinquance, mais désigne un **phénomène politique produit par les pouvoirs publics** à partir des années 1970.

L'insécurité est en réalité un **sentiment** variant selon des déterminants sociologiques, des perceptions ou des expériences. Pour les chercheurs Philippe Robert et Renée Zauberman, « l'insécurité » est une notion qui mêle deux concepts distincts. D'une part, **une peur concrète** des personnes pour elles ou leurs proches, une **émotion** issue d'une expérience personnelle, et d'autre part **une préoccupation plus abstraite** sur la manière de considérer une situation, d'appréhender la délinquance comme problématique sociétale¹. **L'insécurité procède donc de manières subjectives de percevoir des évènements, et non d'une réalité objective quantifiable.**

1 — Philippe Robert et Renée Zauberman, Du sentiment d'insécurité à l'État sécuritaire, Le Bord de l'eau, 2017.

C'est à partir de la fin des Trente Glorieuses – période marquée par une précarisation des relations de travail et l'apparition du chômage de masse – que ce sentiment a été pris en charge par l'État, rompant avec une politique pénale auparavant axée principalement sur l'identification des personnes délinquantes. Désormais, le **traitement politique de la criminalité allait faire de celle-ci un risque de masse** dont il faudrait contrôler les effets néfastes pour celles et ceux qui sont affecté-es. La manière dont cette criminalité est **vécue** par les citoyen·nes (et non pas uniquement par les victimes des infractions) devient alors centrale, ce qui s'accompagne d'une **inflation législative** et d'une multiplication de déclarations et d'effets d'annonce.

Petit à petit, **les dirigeants ont utilisé cette peur pour faire prospérer une vision autoritaire de la sécurité dans l'espace public**. Cette peur est sans cesse gonflée, tantôt par la mise en avant de faits divers dans les médias, tantôt par l'accroissement visible de dispositifs répressifs – créant la manifestation physique qu'il y aurait des raisons d'avoir peur –, tantôt par la mesure, à travers des sondages, de ce « sentiment d'insécurité ».

Déploiement de l'urbanisme sécuritaire et de la vidéosurveillance

Cela s'est également manifesté dans les choix stratégiques de politique publique de sécurité. Dans les années 1980, celles-ci intégraient des logiques de prévention spécialisée, de politique sociale et des volets au niveau local. Aujourd'hui, **elles se construisent sur une « politique de la ville » pilotée par le ministère de l'Intérieur, majoritairement répressive** et mettant en œuvre des stratégies de « prévention situationnelle ». Derrière ce terme verbeux se cache une vision particulière de la commission des infractions, selon laquelle celle-ci pourrait être empêchée ou diminuée si on modifie l'environnement dans lequel le passage à l'acte a généralement lieu. En pratique, la prévention situationnelle a pour but de modifier l'aménagement des espaces publics afin de diminuer ces conditions contextuelles et dissuader les auteurs. Il s'agit par exemple de rendre les rues moins sombres ou d'en diminuer le nombre de recoins.²

2 Pour approfondir sur la notion de « prévention situationnelle », lire l'ouvrage « Circulez, la ville sous surveillance » de Thomas Jusquiamé, Ed. Marchialy.

La prévention situationnelle a été l'un des moteurs du développement de la vidéosurveillance, dans un contexte marqué par le recul de l'action sociale. **Elle alimente la vision faussée selon laquelle l'insécurité se situerait principalement dans les espaces publics**, en jouant notamment sur les peurs décrites précédemment. Les caméras ont petit à petit remplacé les médiateur-ices sociaux dans les rues. Aussi, **toutes les autres formes d'insécurité**, qu'elles soient **sociales** (la précarité du logement, de l'emploi), **sociétales** (la pollution, le sexisme, le racisme) ou encore **sanitaires** (la malnutrition, les addictions) **sont négligées**.

À travers la vidéosurveillance et son pendant algorithmique, les « incivilités de rue » et leur traitement répressif sont ainsi mis-es en avant, invisibilisant les autres illégalismes et d'autres approches vis-à-vis des comportements violents ou simplement déviantes. Au prétexte d'un renforcement de la sécurité, c'est bien une **tentative de discipliner les classes populaires qui se fait jour. De fait, les premières victimes de la VSA sont les personnes qui vivent dans la rue**. Si leur sécurité avait été une réelle préoccupation, alors une des priorité aurait été de donner un toit aux plus de 600 personnes sans domicile mortes dans la rue en 2022. Et pendant que les policiers scrutent la rue et sur-criminalisent les populations en proie aux discriminations structurelles, les délinquants en col blanc sont de moins en moins inquiétés.



La sécurité des femmes en est un exemple typique :

Selon cet imaginaire répressif, le danger de la violence et du viol se situerait essentiellement dans la rue (sombre de préférence) et la solution serait de poser une caméra de surveillance pour protéger et rassurer les femmes.

Sauf que les études et chiffres disponibles sont sans équivoque : les femmes sont surtout en danger chez elles, au travail ou dans d'autres espaces privés. Dans 91 % des cas, les agressions sont perpétrées par une personne connue de la victime (le conjoint ou l'ex-conjoint dans 47 % des cas). Et les constats produits ces dernières années tendent à démontrer que la réponse politique ne se situe pas dans le tout répressif mais dans un changement en profondeur de la société à travers une transformation des institutions, la prévention, l'accompagnement ou encore la formation. Quant à la sécurité dans l'espace public, on pourrait en priorité chercher à changer les comportements quand on sait que plus de 88 % des témoins ne réagissent pas devant les incidents et agressions à caractère sexuel et que, caméra ou pas, la police sera dans la quasi-totalité des cas défailante pour prendre et traiter une plainte pour violence sexiste ou sexuelle.

Source : *The Conversation*, « La sécurité des femmes : une question surtout domestique », 24 novembre 2021, accessible à <https://theconversation.com/la-securite-des-femmes-une-question-surtout-domestique-170841>

Mais la réalité n'arrétant nullement les promoteurs de la VSA, ils n'hésitent pas à surfer sur la croyance que ces dispositifs, tout comme les caméras sur lesquels ils s'appuient, renforcent la « sécurité » des personnes dans l'espace public. C'est au nom de ce principe flou et abstrait que sont vendus les logiciels de VSA, dont **les usages pourront se démultiplier au gré des obsessions policières et des priorités du moment** : il y a déjà une demande politique en faveur d'une VSA dédiée à la détection des « rodéos urbains » ou des « vendeurs à la sauvette ».

B

Mutation des pratiques policières

Les algorithmes de VSA sont conçus pour être utilisés par la police, dont ils systématisent les logiques répressives et discriminatoires, tout en contribuant à déshumaniser encore davantage le rapport de l'institution à la police.

Une société de contrôle dopée aux algorithmes

De façon générale, **la VSA est typique du pouvoir sécuritaire** théorisé par Michel Foucault. La sécurité – ou ce que Gilles Deleuze appellera « société de contrôle » – fonctionne à la régulation et au pilotage en temps réel de flux circulant dans des milieux ouverts. Après les disciplines qui marquent l'essor de l'État-nation et du capitalisme industriel au XIXe siècle (et que Foucault résumait par la formule « faire vivre et laisser mourir »), **la société de contrôle cherche à réguler les flux en temps réel** (« laisser passer, laisser faire, passer et aller »)³.

Dans un contexte où l'État et les grandes organisations capitalistes voient leur puissance indexée à leur capacité à démultiplier les flux (de personnes, de marchandises, de capitaux, de données), **le contrôle social doit être « sans friction »**, capable de passer à l'échelle pour contrôler chacune de leurs composantes « à la volée ». Démultipliant les calculs, agrégeant des statistiques, identifiant et classant des individus et leurs

3 — Sur les régimes de pouvoir identifiés par Foucault, voir Olivier Razac, Avec Foucault, après Foucault : disséquer la société de contrôle, L'Harmattan, 2008 ; sur la notion de pouvoir sécuritaire dans l'œuvre de Foucault, voir en particulier Michel Foucault, Sécurité, territoire, population : Cours au Collège de France, 1977-1978, Seuil, 2004, pp. 62-64. Voir enfin Gilles Deleuze, « Post-scriptum sur les sociétés de contrôle », L'Autre journal n° 1, 1990.

comportements au travers de dispositifs largement invisibles, la VSA est l'une des plus parfaites incarnations de ces nouvelles modalités de contrôle policier, la clé du vieux **fantasme d'une « surveillance permanente, exhaustive, omniprésente, capable de tout rendre visible »**, ainsi que le décrivait Foucault dans *Surveiller et punir*⁴.

Pour autant, dans la société de contrôle, les logiques d'auto-discipline fonctionnent toujours à plein, chacun-e incorporant les normes dominantes lorsqu'il ou elle se sent scrutée par des dispositifs de vidéosurveillance. En ce qu'elle porte dans son code informatique la formalisation de la norme, la VSA **pousse le mécanisme de surveillance à son paroxysme et incarne un outil de normalisation par excellence**. Elle devient alors un vecteur puissant de transformation de la manière dont nous vivons la ville.

■ Démultiplication des forces policières

Aujourd'hui, la grande majorité de ce qui est filmé par les caméras n'est jamais regardé. Avec près d'une centaine de milliers de capteurs vidéos sur la voie publique, il ne serait ni réaliste politiquement ni soutenable sur le plan économique de placer un agent derrière chaque caméra pour scruter ce qu'il se passe en temps réel. Même Christian Estrosi, maire de la ville de Nice, le dit : « On a 4 500 caméras mais pas 4 500 opérateurs. Il faut un signal pour dire de regarder là où quelque chose est en train de se passer⁵ ».

À Marseille, dans les documents liés au marché public pour l'expérimentation de la vidéosurveillance automatisée, la mairie indiquait ainsi en 2018 que « *[s]es opérateurs ne peuvent pas visualiser l'ensemble des flux* » et qu'il « *est donc nécessaire que la solution logicielle permette d'effectuer de façon autonome cette visualisation*⁶ ».

4 — Michel Foucault, *Surveiller et punir, Naissance de la prison*, Gallimard, 1975, p. 215.

5 — « Caméras augmentées : en première ligne, Nice veut « aller beaucoup plus loin » », La Croix, avril 2024 : <https://www.la-croix.com/cameras-augmentees-en-premiere-ligne-nice-veut-aller-beaucoup-plus-loin-20240412>.

6 — Programme Fonctionnel Technique final - Acquisition d'un Dispositif de Vidéoprotection Intelligente, 2018 : <https://data.technopolice.fr/fr/entity/fs2gpylqvgs>.

*La VSA vient régler un **problème d'économie politique lié à la vidéosurveillance, faisant en sorte qu'aucune image n'échappe à une analyse policière désormais automatisée.** Prenons l'exemple du suivi visuel d'opposant-es politiques ou d'un groupe prédéterminé. Auparavant, elle impliquait des moyens humains importants, obligeant la police à prioriser les dossiers. Aujourd'hui, **la VSA lève ces contraintes humaines et matérielles.** À travers l'automatisation, tout agent peut suivre, à coût quasi nul, les activités d'une personne ou d'un groupe de personnes sur l'ensemble des caméras d'une ou plusieurs villes, ou avec des drones, le tout aussi bien en temps réel qu'en temps différé.*

Dans le cas d'une enquête policière, le visionnage en temps différé des enregistrements vidéos pour retrouver des indices ou des preuves prend un temps considérable, mobilisant pour chaque enquête plusieurs agents durant de longues heures de travail. Cela a par exemple été le cas pour l'enquête de l'affaire dite « Lafarge », suite à une action de militant-es écologistes dans des usines de la multinationale du ciment : les enquêteurs ont exploité une très grande quantité d'images de vidéosurveillance pour visionner les bandes et trouver des éléments matériels permettant de corroborer leur version⁷. Avec la VSA en temps différé, qui permet la recherche de certains éléments via des mots-clés ou offre la possibilité de condenser de longues heures d'enregistrement, **nombre d'images qui n'étaient jusque-là pas exploitées pourront d'un clic passer au crible d'une analyse automatisée.**

À terme, la VSA rend également possible la **constatation systématique des infractions**. À la suite des radars automatiques destinés à réprimer les excès de vitesse, la VSA permet en effet d'**automatiser la « vidéoverbalisation »**, générant une manne financière inexploitée pour les pouvoirs publics. Dans des villes, des alertes sont déjà produites par les systèmes de VSA pour réprimer certaines infractions au code de la route. Les opérateurs n'ont qu'à regarder passer les alertes pour rédiger un procès-verbal et infliger des amendes⁸. Si les fichiers de police étaient couplés à ces systèmes, il deviendrait relativement aisé

7 — « Affaire Lafarge. Les moyens d'enquête utilisés et quelques attentions à en tirer », article publié sur *Rebillyon* et disponible sur <https://rebillyon.info/Affaire-Lafarge-Les-moyens-d-enquete-25197>.

8 — Thomas Jusquiamé, « Les cuisines de la surveillance automatisée », *Le Monde diplomatique*, 1er février 2023.

d'identifier les personnes via la reconnaissance faciale et d'élargir le champ des infractions concernées.

Avec la VSA, les 250 000 policiers et gendarmes actuels voient leurs capacités atteindre celles qu'auraient des millions d'agents ne recourant pas à ces technologies. De quoi atteindre **un ratio police/population typique des États policiers**, sans qu'aucun contre-pouvoir efficace ne puisse être mis en place.

■ Déshumanisation et biais d'automatisation

La VSA codifie dans un dispositif technique une **vision stéréotypée de la « délinquance » et des personnes ou comportements « suspect-es »**. Le code de l'algorithme est fixe, sans nuance. En générant des alertes qui interpellent le policier et le poussent à agir, il s'impose face à toute appréciation humaine d'une situation donnée.

L'intervention de l'opérateur humain, qui décide des suites à donner aux alertes générées par les systèmes de VSA, est présenté par les promoteurs de la Technopolice comme une garantie. Selon cette logique, la présence en bout de chaîne du policier compenserait la rigidité algorithmique. C'est négliger le **« biais d'automatisation »**, qui conduit les humains à **faire démesurément confiance aux systèmes algorithmiques**. En pratique, le recours à un algorithme risque de déresponsabiliser davantage les policiers. Il leur confère une illusion de maîtrise et leur offre un alibi commode (« c'est la machine qui l'a dit ») pour justifier d'être intervenus à un endroit ou un moment en particulier.

En insérant ces technologies de VSA dans leur processus de décision, **la distance qui sépare la police de la population s'agrandit**. Cette distance est d'abord **physique** : la relation police-citoyen-nes est de plus en plus médiée par des dispositifs technologiques. C'est le paradigme des « agents connectés » et ou « augmentés », équipés de caméras-piétons, de tablettes et autres smartphones dotés de logiciels de lecture automatique de plaques d'immatriculation et d'applications d'accès aux fichiers de police. C'est aussi un effet de la « robocopisation » des équipements, de la culture de l'armement, de la systématisation des patrouilles véhiculées, qui contribuent à créer une forte distance entre la police et les habitant-es. La vidéosurveillance

et la surcouche algorithmique induite par la VSA aggravent ces tendances : au quotidien les agents ne sont plus dans la rue, mais derrière leurs écrans, le plus souvent dans un centre de contrôle, le CSU, depuis lequel ils observent, de loin, la population. Et quand ils en descendent, c'est pour l'arrêter et la violenter. La VSA contribue à aggraver ces logiques.

La distance est aussi **intellectuelle** : **ces policiers augmentés n'ont plus à comprendre, contextualiser, évaluer ou anticiper l'action des autres humains quand une machine le fait à leur place.** La VSA codifie dans un dispositif technique une vision stéréotypée de la « délinquance » et des personnes ou comportements « suspect·es ». En générant des alertes qui interpellent le policier et le poussent à agir, elle s'impose face à toute appréciation humaine d'une situation donnée.



C

Répression des corps, transformation du rapport à la ville

La VSA inscrit dans le code une vision particulière des normes comportementales et de la déviance, une vision policière qui passe à l'échelle du fait de sa mise en algorithmes. Ce faisant, elle risque de **renforcer l'exclusion et la stigmatisation de celles et ceux perçus comme suspect-es ou non légitimes à occuper l'espace public.**

Tous-es suspect-es : l'arbitraire policier mis en algorithmes

La vidéosurveillance algorithmique en temps réel a pour objectif d'automatiser le travail de visionnage de la vidéosurveillance. Il est donc demandé au logiciel de rechercher ce qui leur semble « anormal ». En pratique, il s'agira de repérer les individus « bizarres », les « comportements anormaux » grâce à des « signaux faibles ». **Ces « signaux faibles » permettraient d'identifier une personne « suspecte » d'avoir commis ou de pouvoir commettre une infraction,** systématisant en les automatisant les critères arbitraires déjà utilisés par la police. Des caractéristiques corporelles ou comportementales déjà perçues comme suspectes, souvent injustement discriminatoires, racistes, stigmatisantes se retrouveront ainsi « codées » dans les algorithmes de VSA. Au détour de ce processus, des situations très banales se retrouvent qualifiées de « suspectes » et dignes de l'attention policière. En réalité, **aucun comportement n'est suspect en soi,** il ne l'est que de manière relative à un imaginaire, à une vision de la société.

Comportements repérés par la VSA

Les exemples concrets de VSA en France montrent que les comportements faisant l'objet d'une alerte sont très anodins. Par exemple, le logiciel Jaguar commercialisé par la société Evitech propose de repérer comme situations suspectes les « arrêts fréquents », les « contre sens », les « groupes » ou encore une « vitesse insuffisante ou excessive ».

À Vannes, la société Cogitech a remporté le marché public de VSA. Dans le document technique associé à ce marché, il est prévu que l'analyse porte sur les données comportementales suivantes : « marchant, courant, debout, assis, baissé, accroupi, etc. ».

La ville nettoyée de ses « nuisibles⁹ »

La liste des situations détectées par les systèmes de VSA illustre bien les **usages de l'espace public perçus comme légitimes, et ceux qui sont au contraire diabolisés, traqués et réprimés** – les « nuisibles », pour reprendre l'expression utilisée par les syndicats policiers en réaction au meurtre de Nahel et aux soulèvements des quartiers populaires suscités par ce drame.

Ainsi, un usage documenté de la VSA consiste à détecter des activités de « maraudage », c'est à dire une personne qui resterait un peu trop longtemps statique, ou limiterait ses déplacements à une zone restreinte. La VSA recherche aussi les personnes au sol ou allongées. **Les personnes ouvertement stigmatisées par ces cas d'usage sont celles qui font la manche ou qui sont sans domicile.** À travers ces détectations, la VSA cible également les personnes qui travaillent dans la rue, par exemple les travailleuses du sexe. Un autre cas d'usage de la VSA est la détection des regroupements de personnes, notamment devant les halls d'immeuble. Les jeunes des quartiers populaires qui

9 Le terme « nuisibles » est utilisé dans un communiqué de presse des syndicats de police Alliance et UNSA Police publié le 30 juin 2023 suite aux révoltes urbaines en réaction au meurtre de Nahel.

se retrouvent dans la rue, en partie parce qu'ils ou elles n'ont pas toujours les moyens de se retrouver dans un espace privé – encore moins un espace privé de qualité où nouer des sociabilités –, sont ouvertement visé·es.

La VSA renforce donc la répression d'activités, de comportements, de modes de vie déjà exposés à une forte discrimination et répression policière. Elle codifie dans un dispositif technique une vision stéréotypée de la « délinquance » et des personnes ou comportements « suspect·es ». Elle acte une **vision de la rue comme simple lieu de passage**, un espace transitoire plutôt qu'un lieu de vie, un moyen de se rendre d'un espace privé – si possible commercial – à un autre. Les personnes repérées par les logiciels seraient celles qui ne font pas partie du flux des villes, des mouvements pendulaires domicile-travail-domicile, celles qui ne font pas uniquement que se déplacer d'un point A à un point B., alimentant une vision utilitariste de la vie en ville. En somme, on repère celles et ceux qui ne participent pas, pas assez, ou pas assez bien à la machine capitaliste. On ne dort pas dans la rue, on ne joue pas dans la rue, on ne se rassemble pas dans la rue. Dans la rue, on est en mouvement, on passe son chemin.

Une telle philosophie pouvait déjà être perçue dans l'analyse des restrictions mises en place lors des confinements durant la pandémie de COVID-19 en 2020 et 2021. L'attestation de déplacement dérogatoire autorisait la sortie de chez soi pour une liste définie d'usages jugés « légitimes ». Aller au travail, à l'école, faire des achats et se déplacer pour des raisons de santé. Derrière ces choix qui pourraient paraître indolores se révèle une vision du monde : celle du travail productif et de la consommation.

■ Nos corps mis en données

Quoique prétendent ses promoteurs, **la VSA repose sur l'exploitation de nos données personnelles et biométriques.** Les fabricants de cette technologie voient en nos corps une source d'informations à exploiter pour faire du profit en mettant au service des États une nouvelle capacité de surveillance de la population.

Les algorithmes de VSA ne sont pas des outils magiques. Ils ne font qu'appliquer une série d'instructions. Contrairement à ce que la notion « d'intelligence artificielle » voudrait nous faire croire, la machine ne « voit » pas. Elle ne fait pas de distinction consciente entre un·e humain·e, une benne à ordures ou une voiture. **Pour l'algorithme, il n'y a que des images composées d'un certain nombre de pixels** de couleurs différentes. Ses concepteurs doivent recourir à des méthodes capables de l'aider à détecter une empreinte – c'est-à-dire une combinaison mathématique entre des positions de pixels les uns par rapport aux autres et leur couleur – à une appellation précise (par exemple « voiture », « individu humain », « valise », « ordures »). **Le logiciel établit seulement une correspondance entre cette empreinte numérique et les mots « voiture » ou « humain »**, ou des catégories plus précises comme « humain avec un haut de couleur rouge et un pantalon de couleur bleue ».

Or, contrairement à la machine, le droit fait la différence entre les données qui constituent l'empreinte d'un objet et celles qui constituent l'empreinte d'un·e humain·e. Selon le Règlement européen général sur la protection des données (RGPD), les **données biométriques** sont toutes les **données physiques, physiologiques ou comportementales qui peuvent permettre d'identifier une personne de façon unique**. Ces données sont considérées comme sensibles et bénéficient d'une protection particulière.

Les promoteurs de la VSA s'efforcent de nier le caractère biométrique des données traitées par leurs systèmes afin d'échapper aux protections prévues par le droit. Or, même sans recourir aux empreintes faciales des individus (reconnaissance faciale), **plusieurs méthodes de VSA permettent de suivre une personne** – par exemple à travers la couleur de ses vêtements ou sa démarche – à mesure qu'elle évolue dans un espace urbain et passe dans le champ de vision de différentes caméras (cette capacité de suivi des personnes repose sur des algorithmes dits de « réidentification »). Dès lors que les algorithmes de VSA permettent de retrouver une personne au milieu d'autres à partir des données physiques ou comportementales, il s'agit **d'identification biométrique**.

L'identification biométrique

L'identification biométrique est une **technique** qui permet de retrouver **une personne** parmi un **échantillon de personnes** à partir de **caractéristiques physiques, physiologiques ou comportementales**.



Technique pour identifier une personne	Échantillon	Caractéristiques
algorithmes de reconnaissance faciale	ensemble de la population	distance entre certains points du visage (keypoints)
algorithmes de réidentification	personnes présentes dans un périmètre donné à un moment donné	sa taille, sa couleur de peau, sa couleur de cheveux, ses vêtements...

Comprendre les algorithmes de reconnaissance faciale et leurs usages

Les **algorithmes de reconnaissance faciale** ont été « légalisés » en 2012 via le décret à l'origine de la création du fichier de police de traitement des antécédents judiciaires (TAJ). Ce fichier concerne toutes les personnes mises en cause par la police. Le décret prévoit que ces fiches puissent contenir « *la photographie comportant les caractéristiques techniques permettant le recours à un dispositif de reconnaissance faciale* ».

Les algorithmes de reconnaissance faciale fonctionnent en **attribuant une empreinte à chaque visage**. Cette empreinte est construite à partir de la distance qui sépare certains points du visage, choisis stratégiquement pour garantir que la combinaison des distances permette d'identifier un visage sur une photo avec une marge d'erreur suffisamment faible.

Ainsi, quand la police questionne le logiciel de reconnaissance faciale, elle envoie la photo d'une personne non identifiée, trouvée par exemple sur des images de vidéosurveillance, et **le logiciel compare l'empreinte de son visage aux empreintes des 8 millions de personnes ayant une fiche avec photo dans le TAJ**.

Comprendre les algorithmes de réidentification et leurs usages

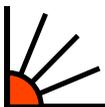
Les **algorithmes de réidentification** permettent de **retrouver une même personne sur plusieurs images à partir de ses attributs physiques et comportementaux**. Ils fonctionnent différemment des algorithmes de reconnaissance faciale, car l'identification de la personne ne se fait pas sur la base d'une comparaison entre une base de données et une image externe, mais par comparaison entre deux images de vidéosurveillance (deux caméras différentes ou deux moments différents sur une même caméra) afin de pouvoir les relier et ainsi retracer le chemin de la personne. **Pour ce faire, le logiciel dresse là aussi une empreinte de la personne, basée sur une multitude de caractéristiques** qu'il est en mesure de repérer chez une personne, comme le type et la couleur de ses vêtements, sa silhouette, sa taille, la couleur de sa peau, ses accessoires et bien d'autres.

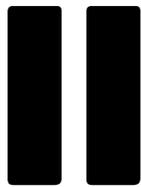
Ces algorithmes sont totalement illégaux mais sont déjà largement en usage. On les retrouve notamment dans un projet européen dénommé « Prevent PCP », déployé à Paris et Marseille pour suivre les bagages dans les gares d'une caméra à l'autre. Afin de s'assurer qu'il s'agit bien du même bagage, les informations sur la personne qui le porte sont utilisées. Un bagage ressemble trop à un autre, en revanche la personne qui le porte, par exemple une femme avec un t-shirt rouge, a des caractéristiques suffisamment rares pour identifier le bagage de manière unique. Pour suivre un bagage, l'humain-e qui l'accompagne et l'ensemble de ses données biométriques sont utilisées. L'appellation « suivi de bagage » fait oublier que c'est avant tout l'humain qui est suivi.

■ Une perte de libertés pour tous·tes

La ville, et l'espace public de manière générale, constitue un lieu précieux. Un lieu dense, protéiforme, en mouvement permanent, où s'exercent de nombreuses libertés, où l'on peut s'affranchir de certaines assignations imposées.

L'anonymat et le respect de la vie privée y sont fondamentaux. Car c'est à travers eux que peuvent s'exercer toutes les autres libertés : **liberté de manifester, liberté d'aller et venir, liberté d'expression.** Or, en renforçant les dispositifs de surveillance et en augmentant le nombre de caméras pour y ajouter des algorithmes d'analyse, **l'État fait de l'atteinte à la vie privée un principe et non l'exception.** Il part du postulat que tout·e citoyen·ne est suspect·e en puissance, que ce serait à elles et eux de justifier tout comportement déviant ou leur simple présence dans certains lieux. **La VSA est fondamentalement contraire à la défense des formes de vie démocratique.**

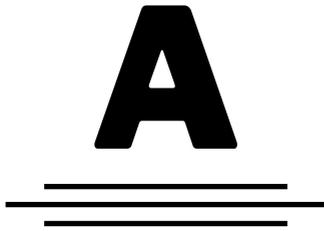




L'empire de la VSA

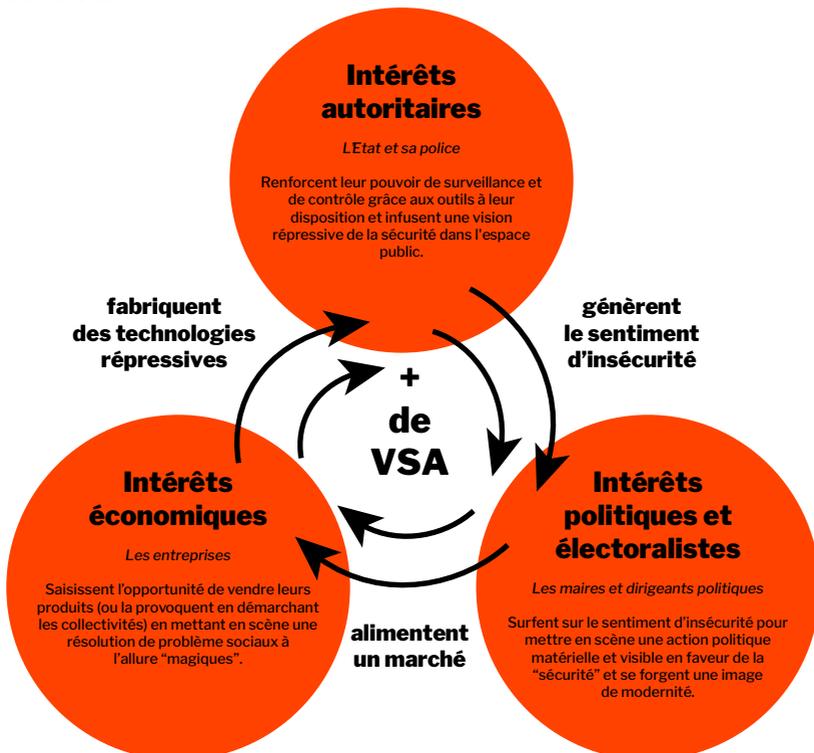
En quelques années, **la VSA s'est fait une place dans le débat public et dans la pratique policière**, au point d'avoir fait l'objet d'une législation dédiée avec le cadre « expérimental » de la loi relative aux Jeux Olympiques adoptée en 2023. Pour comprendre cette percée fulgurante, il faut se pencher sur la composition des réseaux d'acteurs dédiés à sa promotion mais également sur les **mécanismes d'opacité et les stratégies d'acceptabilité** que ces derniers ont déployées dans le but de l'imposer.





Une convergence d'intérêts

Le déploiement de la VSA ne répond à aucun besoin sociétal réellement documenté mais résulte d'une convergence d'intérêts : **économiques** pour les entreprises qui la développent, **politiques et électoralistes** pour les décideurs publics, **autoritaires** pour la police qui accroît toujours plus son pouvoir de contrôle.



I Des intérêts économiques d'abord

Ce sont des entreprises privées qui vendent ces logiciels aux villes, aux collectivités ou à d'autres acteurs privés (notamment les commerces). Cette nouvelle « offre » commerciale centrée sur l'automatisation des analyses de la vidéosurveillance s'inscrit dans un phénomène plus global : celui du **marché de la sécurité**. Il s'agit d'un secteur très lucratif et en pleine expansion. En France, il est estimé à **34 milliards d'euros (soit 1,6 % du PIB¹⁰)**. Au sein de ce secteur florissant, le **business de la vidéosurveillance** se porte particulièrement bien, puisque la CNIL estimait que le chiffre d'affaire du secteur atteignait **1,7 milliards d'euros en 2022¹¹**.

Au niveau mondial, le marché de la sécurité privée est estimé à 660 milliards d'euros et celui de la vidéosurveillance à 45 milliards en 2020 (avec des projections à 76 milliards pour 2025). Toujours à l'échelle mondiale, la vidéosurveillance algorithmique représentait en 2020 plus de 11 milliards de dollars, avec une croissance de 7% par an¹².

Comme le montre la sociologue Myrtille Picaud dans ses recherches¹³, le marché numérique de la sécurité urbaine est investi par **une panoplie hétérogène d'acteurs** :

- Il y a d'abord les grandes **multinationales provenant du domaine de la tech**, à l'image d'IBM à Toulouse, qui a équipé une trentaine de caméras de vidéosurveillance de la métropole avec un logiciel de vidéosurveillance automatisée.

10 — Myrtille Picaud, « Peur sur la ville. La sécurité numérique pour l'espace urbain en France », Rapport de recherche, École urbaine de Sciences-Po, 2021 : <https://hal.science/halshs-03138381/>.

11 — Philippe Gosselin et Philippe Latombe, « Rapport d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité », Assemblée Nationale, avril 2023 : https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/16b1089_rapport-information.

12 — « Ce que pèse le marché mondial de la surveillance », TelQuel, juillet 2021 : https://telquel.ma/2021/07/02/ce-que-pese-le-marche-mondial-de-la-videosurveillance_1727755.

13 — Myrtille Picaud, « Peur sur la ville. La sécurité numérique pour l'espace urbain en France », Rapport de recherche, École urbaine de Sciences-Po, 2021 : <https://hal.science/halshs-03138381/>.

- Ensuite, il y a les **industriels de la sécurité**, largement soutenus par les subventions publiques, qui se sont intéressés à la numérisation de ce marché. C'est le cas par exemple de Thales, avec l'expérimentation Safe City à Nice et à La Défense, ou encore de la SNEF à Marseille.
- Plus modestes et plus récentes, **des startups** ont été lancées dans le but de se positionner sur ce marché prometteur. Certaines investissent explicitement le marché de la police urbaine, comme Videtics, startup implantée dans le technopôle de Sophia Antipolis, près de Nice. D'autres tentent de se dessiner une image plus vertueuse et « éthique », à l'image de l'entreprise XXII qui, après avoir perdu plusieurs marchés sécuritaires, met surtout en avant des usages d'apparence plus inoffensifs (par exemple en repérant automatiquement l'arrivée d'un piéton afin de faire passer le feu au rouge pour les voitures¹⁴).
- Enfin, les **entreprises étrangères**, grandes ou petites, ne sont pas en reste. Une des solutions de vidéosurveillance algorithmique les plus répandues en France est proposée par Briefcam, une entreprise israélienne rachetée par le groupe japonais Canon¹⁵ : pas moins de 200 villes françaises seraient dotées de sa technologie de VSA¹⁶.

L'argent attirant l'argent, les grands groupes et les startups du secteur enchaînent les levées de fonds, aussi bien auprès des acteurs publics (notamment la BPI France) que privés. L'État subventionne également ces entreprises au titre des **financement de recherche**. En 2019, l'Agence nationale de la recherche (ANR) accordait par exemple plus d'un million d'euros à Idemia, Thales et Deveryware (depuis rachetée par la holding spécialiste de surveillance ChapsVision) afin de développer des applications de VSA en lien avec la préfecture de police de Paris¹⁷.

14 — Rappelons que cette même startup avait conclu en 2021 un partenariat avec la ville de Suresnes et directement utilisé les caméras de la ville pour entraîner ses algorithmes, les habitant-es de la ville étant transformé-es en cobayes pour le développement commercial d'un produit de surveillance. Lire l'analyse ici : <https://technopolice.fr/blog/les-suresnois%C2%B7es-nouveaux-cobayes-de-la-technopolice/>.

15 — Plus d'informations sur cette entreprise ici : <https://technopolice.fr/briefcam/>.

16 — Thomas Jusquiamé, « Les cuisines de la surveillance automatisée », Le Monde diplomatique, 1er Février 2023 : <https://www.monde-diplomatique.fr/2023/02/JUSQUIAME/65535>.

17 — Voir la présentation du projet S²UCRE (Safety and Security of Urban Crowded Environments) ici : <https://data.technopolice.fr/fr/entity/dd33j6ttis?page=2>.

En faisant tourner leurs algorithmes sur les flux de vidéosurveillance, **ces entreprises agrègent quantité de données personnelles et biométriques** aux fins de les analyser, de les exploiter, de les recouper pour entraîner et **développer des logiciels qui seront ensuite vendus sur un marché international**. En outre, pour la VSA en temps réel, ce sont ces sociétés qui définissent ce qui est « normal » ou « anormal » au sein de l'espace public.

Zoom sur une des entreprises retenues pour les JO

Parmi les sociétés retenues pour assurer les expérimentations de VSA pour les JO, on trouve la startup parisienne Wintics, créée en 2017. Elle se place parmi les principaux acteurs du marché avec son logiciel « Cityvision » qui fait notamment de l'analyse de foules mais également de la détection de « présences suspectes » et de « comportements violents » ou « dangereux sur les quais ». Sa solution a notamment été utilisée dans les gares et stations de la RATP, lors du tour de France pour compter les vélos et aurait été récemment installée à l'aéroport de Rome pour « gérer les flux ». Ses fondateurs s'affichent régulièrement avec le gouvernement et représentent la France dans les salons internationaux. Wintics fait partie des entreprises sélectionnées pour mettre en œuvre l'expérimentation de la VSA dans les transports, dans le cadre de la loi JO (voir partie III).

Des intérêts électoralistes ensuite

La VSA s'inscrit totalement dans le mécanisme d'activation du sentiment d'insécurité. Comme la vidéosurveillance avant elle, la VSA se présente comme **une solution technologique à disposition des maires qui voudraient donner l'illusion d'avoir une action concrète sur la délinquance ou les troubles à l'ordre public**.

L'attrait politique de la VSA tient également au prétendu caractère « innovant » et « smart » colporté par la technologie numérique. Les algorithmes de détection incarnent l'innovation et un futur soi-disant « inéluctable ». De nombreux responsables politiques, y compris de très petites communes, veulent les adopter **pour se donner une image de progrès et de modernité**.

Ainsi, comme les caméras, la VSA joue sur le **solutionnisme technologique**. Elle permet de prétendre résoudre un problème politique à moindre coût, tout en justifiant l'existence du parc de caméras existant.

■ Des intérêts autoritaires, enfin

Enfin, comme on l'a déjà évoqué, la VSA accroît considérablement les pouvoirs de contrôle et de surveillance de la police. En ne se contentant pas d'observer passivement mais **en ajoutant aux caméras une analyse automatisée et permanente des flux de vidéosurveillance, les forces de l'ordre ont la capacité de démultiplier leurs activités de surveillance, leurs interventions, la vidéo-verbalisation, et les arrestations.** Le tout en compilant constamment des informations liées à notre présence dans l'espace public : comportements, déplacements, habitudes... Toutes ces données tirées des traitements automatisés donnent à la police un pouvoir de s'immiscer toujours plus dans nos vies, et participent pleinement de la **dérive autoritaire** qui se donne à voir chaque jour un peu plus.

À la vue de cette convergence d'intérêts économiques, politiques et policiers, on comprend alors comment la VSA a pu se développer aussi rapidement et facilement, **chacun de ces intérêts s'auto-alimentant et les trois se perpétuant les uns les autres.** En effet, les entreprises de VSA ont pu trouver leur raison d'être en s'ancrant dans le discours réactionnaire de la peur du crime alimenté depuis des années. Leurs technologies sont apparues comme une façon innovante de répondre aux problématiques « d'insécurité ». Que ce soit au niveau national ou local, les politiciens s'en sont saisis à des fins électorales. Enfin, la police s'en est trouvée confortée dans son rôle central dans la régulation et le contrôle social.

L'ensemble de cette **logique techno-sécuritaire** contribue en réalité à activer le sentiment de peur d'une partie de la population, entretenant à son tour la demande sociale en vidéosurveillance. Et ce d'autant que tous les gardes-fous institutionnels censés préserver les droits humains sont mis en échec par un jeu d'opacités multiples.

B

Une avancée à visage masqué

Si les dangers de la reconnaissance faciale sont très présents dans l’imaginaire collectif, les autres applications de la VSA sont inconnues de la majorité de la population. Même en s’intéressant particulièrement au sujet, **il est difficile de savoir comment celle-ci est développée**, ou quel spectre d’usages elle recouvre. Il est encore plus **difficile de savoir, parmi ces usages, lesquels sont déjà en cours d’utilisation par la police**. C’est en entretenant cette opacité que les promoteurs de la VSA – responsables politiques et entreprises – tentent de la déployer. Une fois celle-ci installée, il est en général trop tard pour renverser la machine. **L’opacité entretenue autour de la VSA devient donc un frein à l’exercice des mécanismes démocratiques et d’opposition politique.**

■ Opacité politique et administrative

Si la police judiciaire y recourt déjà en temps différé pour ses enquêtes, **le déploiement de la VSA se joue principalement à l’échelle locale**, car ce sont le plus souvent les collectivités (communes, régions, etc..) qui administrent les parcs de vidéosurveillance et sont donc compétentes pour mettre en place un logiciel de VSA. Alors que cette technologie est totalement illégale – et ce quels que soient ses cas d’usage –, elle a ainsi pu se déployer partout en France sur la base de décisions éparses et éclatées géographiquement, prises le plus souvent par des villes à la fois peu soucieuses de la licéité de ces dispositifs, sensibles aux discours commerciaux des entreprises et aux demandes des services de police municipale.

De plus en plus étendu, ce réseau de collectivités recourant à la VSA a ainsi participé à **imposer un état de fait au niveau national, faisant émerger et exister une technologie de surveillance en dépit de sa totale illégalité.**

Les décisions d'investir dans des logiciels de surveillance algorithmique sont le plus souvent prises lors des conseils municipaux, départementaux ou régionaux et sont inscrites dans les procès verbaux de ces réunions. En général, la collectivité émet un appel d'offres pour acquérir et installer une solution logicielle, auquel les entreprises de VSA répondent. L'ensemble de ces documents – procès verbaux et appels d'offres – sont des documents administratifs. Ils ne sont généralement pas rendus public mais il existe des dispositions législatives permettant à quiconque en faisant la demande d'y accéder. C'est grâce à cette procédure, dite « demande CADA » (pour Commission d'accès aux documents administratifs) que **chacun-e peut demander à avoir accès à un document public**, via un e-mail ou un courrier papier et tant qu'elle respecte un certain formalisme¹⁸.

Si l'administration ne répond pas sous deux mois, il est possible de saisir la Commission d'accès aux documents administratifs afin qu'elle fasse respecter la demande. Si la demande CADA est une méthode très incertaine (les documents communiqués sont souvent caviardés ou incomplets) et chronophage, **elle reste la méthode la plus efficace pour lever l'opacité qui règne autour du déploiement des logiciels de VSA.**

18 — Voir notre guide pour faire des demandes CADA : <https://technopolice.fr/blog/guide-se-renseigner-sur-la-surveillance-dans-sa-ville/>.

Briefcam à Moirans

La ville de Moirans, en Isère, a décidé de se doter du logiciel de VSA Briefcam. La Quadrature du Net a fait une demande CADA auprès de la commune pour obtenir le manuel d'utilisation. Celle-ci a refusé, prétextant ne pas y être autorisée en raison du secret des affaires. Il a alors fallu saisir la Commission d'accès aux documents administratifs qui a rendu un avis affirmant que ce manuel était bel et bien communicable en vertu de la loi française. Malgré cela, la ville a maintenu son refus, obligeant La Quadrature à introduire un recours. Une fois devant le tribunal administratif, la commune de Moirans a toutefois abandonné l'affaire et a communiqué ce document sans attendre une décision de justice qui aurait très certainement été en sa défaveur.

Avis de la CADA disponible ici : <https://cada.data.gouv.fr/20212725/>.

Non seulement **le choix de recourir à la VSA n'est généralement pas rendu public**, mais il est aussi imposé aux habitant·es des villes. Jamais leur consentement n'est demandé, alors même que cette technologie est extrêmement intrusive et conditionne l'exercice de leurs libertés et la manière dont elles et ils vivent la ville. Il n'y a en général ni débat ni vote auprès de la population d'une commune afin de décider collectivement de mettre en place ou non une telle technologie de surveillance. Même les élu·es d'opposition se heurtent souvent à un **manque de transparence**. De plus, une fois les logiciels installés, **aucune information n'est donnée aux personnes soumises à ces analyses algorithmiques** : on passe alors sous une caméra de vidéosurveillance sans savoir que l'on fait l'objet d'une analyse algorithmique.

Dès lors que la connaissance de ces projets est entravée, les mécanismes démocratiques de contestation de ces projets, de même que les garde-fous juridiques normalement applicables, ne peuvent être mobilisés pour s'opposer à la VSA.

■ Opacité technique

Les algorithmes utilisés par la VSA sont développés par des entreprises qui sont les seules à avoir la main sur les choix qui se retrouvent gravés dans le code. **Parmi ces choix se cachent de nombreuses décisions politiques.** Intégrer de la transparence tout au long de la fabrication de ces algorithmes permettrait au minimum de comprendre comment ces choix sont opérés.

Les algorithmes de VSA rassemblent divers algorithmes de vision assistée par ordinateurs, parmi lesquels on trouve :

- les algorithmes de **détection**, qui permettent d'isoler différents éléments d'une image ;
- les algorithmes **d'identification**, qui qualifient ces éléments ;
- les algorithmes de **suit**, qui permettent de suivre ces éléments ;
- les algorithmes de **reconnaissance faciale** ;
- les algorithmes de **franchissement de ligne**, qui repèrent quand un élément se trouve dans une certaine zone de l'image ;
- et une quantité d'autres algorithmes qui, une fois assemblés, couvrent un spectre d'analyse très large.

L'étendue des fonctionnalités d'un logiciel est décidée par l'entreprise – souvent en fonction de la demande des collectivités ou de la police – en combinant ces différents algorithmes. **Le code du logiciel n'est jamais publié, le choix des algorithmes utilisés et de leur paramétrage non plus, pas plus que les jeux de données utilisés pour l'entraînement des algorithmes d'identification. Toute la chaîne de production est opaque.** Il n'est donc pas possible de savoir quelles données de nos corps la VSA traite effectivement.

Parmi ces algorithmes, certains reposent sur une sous-catégorie du *machine learning* appelée le *deep learning*. La particularité du *deep learning* est que les variables qui sont utilisées dans les corrélations sont cachées sous des couches de calculs les rendant imperceptibles. Par exemple, pour catégoriser une image de chat, le concepteur ne spécifie pas à l'algorithme de repérer des oreilles pointues ou des moustaches. À la place, l'algorithme

se sert de toute information à sa portée, issue des positions de pixels associées et de leur couleur. Les variables utilisées en pratique peuvent donc ne même pas être compréhensibles par un humain. Il existe ainsi une forme de « boîte noire » dans le raisonnement de l'algorithme, que personne ne peut comprendre. **Le *deep learning* a donc aussi cette particularité d'être opaque dans les variables utilisées, y compris pour la personne qui le conçoit et le met en place.**

Les logiciels de VSA sont utilisés par l'État et pour autant il n'existe aucune information publique précise sur leur fonctionnement. Lors des débats sur la loi JO, **le gouvernement a refusé d'accorder un droit de transparence sur ces algorithmes**, invoquant un objectif de « sécurité ». Le seul moyen disponible pour obtenir des éléments de compréhension est d'étudier la promotion qu'en font les entreprises dans leur communication commerciale. Or, celle-ci est souvent très repeinte d'un vernis marketing, et ne suffit pas à établir clairement ce que sont les opérations de classement produites par le logiciel.

■ Opacité pratique

Les logiciels de VSA sont des biens marchands répondant à une logique d'offre et de demande. Lorsqu'elles s'adressent à leurs potentielles clientes que sont les collectivités, les entreprises souhaitent que celles-ci achètent leur licence. En bonnes commerciales, elles vont mettre en avant le plus de « besoins » possible que pourraient avoir les villes et qui correspondraient aux usages du logiciel.

Ainsi, une ville qui décide de mettre en place une surveillance de dépôt d'ordures sauvages se verra proposer tout le « package » du logiciel de VSA, qui peut comprendre d'autres utilisations de surveillance. La police qui l'utilisera, en pratique peu scrupuleuse, aura ainsi ensuite entre ses mains de multiples outils, sans que l'on sache exactement lequel est utilisé. S'ajoute donc une **opacité pratique sur ce qui se passe concrètement dans les commissariats et les centres de supervision urbains.**

L'exemple de Marseille

A Marseille, le marché public prévoit une « tranche ferme » et une « tranche conditionnelle », c'est à dire un logiciel de base et une couche supplémentaire à installer ultérieurement, cette dernière contenant les usages les plus problématiques. Il est cependant impossible de savoir si celle-ci a été un jour implémentée. De la même manière, le logiciel Briefcam prévoit une simple case pour activer la reconnaissance faciale, qui d'après des retours du terrain est cochée par défaut. Les commerciaux de l'entreprise n'hésitent d'ailleurs pas à expliquer patiemment à leurs clients comment désactiver l'option en cas de contrôle inopiné de la CNIL.

La prétention de poser des garde-fous techniques, c'est-à-dire d'établir une frontière nette entre une VSA acceptable et une qui ne le serait pas est un mirage. « Détecter un objet au milieu de la route » et « détecter une personne qui dort dans la rue » sont deux actions qui utilisent les mêmes algorithmes, on ne peut pas établir de frontière technique entre les deux. L'opacité pratique et le manque de scrupules de la police nous assure d'une chose : **le seul garde-fou possible est l'interdiction totale de la VSA.**

À la fin, **quasiment personne ne sait ce qu'est la VSA.** Si une personne sait que la VSA existe, elle ne peut pas savoir pour autant où cette dernière est déployée. Si la personne est arrêtée par la police, elle ne saura pas si la VSA a joué un rôle dans son arrestation. Si elle a fait une demande CADA et sait que la VSA est présente dans sa ville, elle ne sera pas pour autant en mesure de savoir à quelles fins elle est vraiment utilisée et ne pourra donc pas s'y opposer.



Mise en place de la VSA : Où se situent les décisions et qui les prend ? Quel accès à ces décisions ?

Décisionnaires

Décisions

Accès aux décisions

LES COLLECTIVITÉS TERRITORIALES

influencent ou commandent des fonctionnalités

installer de la VSA sur un territoire

choisir l'entreprise de VSA

LES ENTREPRISES DE VSA

influencent ou commandent des fonctionnalités

choisir les détections permises par le logiciel

choisir de quelle manière se font les détections

?	?
choix des algorithmes utilisés pour une détection	choix des paramètres de ces algorithmes ?
?	?
choix des jeux de données utilisés ?	données utilisées par l'algorithme pour opérer la détection ?

LA POLICE

choisir quelles fonctionnalités du logiciel utiliser

Incomplet

Méthodes :

- Les demandes CADA permettent d'accéder aux procès-verbaux des conseils régionaux, départementaux et municipaux actant la décision d'installation, aux appels d'offres et au résultat de l'appel d'offre. (souvent sans réponses, réponses souvent parcellaires)
- Consulter le bulletin des annonces des marchés publics peut donner accès à des appels d'offre et à leurs résultats. (non systématique)

Incomplet et faussé

Méthode :

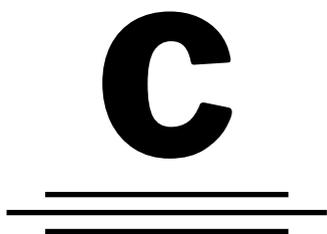
- Une fois le nom de l'entreprise fournissant le logiciel de VSA obtenu, il est parfois possible d'analyser son descriptif directement sur son site Internet. (attention, il s'agit souvent d'un descriptif commercial imprécis voire faux dans le but de convaincre les clients)

Impossible

Sauf fuite ou investigation journalistique

Impossible

Sauf fuite ou investigation journalistique



Fabrique de l'accep- tabilité

En parallèle de cette implantation commerciale dans les villes, **l'industrie de la VSA a fait en sorte de se construire une image vertueuse dans le débat public.** Afin d'emporter l'adhésion de la population et des institutions, le secteur a déployé tout un panel de stratégies pour rendre cette technologie de surveillance acceptable et être associé à une forme de respectabilité.

■ Affirmer la neutralité de la technique

C'est un grand classique. Les technologies de surveillance sont généralement présentées comme de simples outils techniques, qui auraient comme unique but d'aider de façon neutre et impartiale la personne qui l'utilise. **Mais rien n'est neutre dans la VSA.** Toute technique est formatée par ses conditions de production et par l'intention de ses auteurs. À chaque étape, **la VSA reproduit et met dans le code des décisions humaines, des visions subjectives de la société,** qui ont des conséquences politiques importantes.

Pour convaincre que la VSA est un logiciel sans conséquence, **le choix des mots utilisés pour nommer et décrire cette technologie représentait donc un enjeu stratégique majeur.** L'industrie a ainsi développé tout un discours marketing mélioratif et dédramatisant, visant à **éclipser la nature réelle de ce qui était filmé et analysé par les algorithmes.**

Nous avons expliqué que les logiciels de VSA analysent et classent ce qui est représenté sur les images de vidéosurveillance, c'est à dire le plus souvent des humain-es. Pour opérer des corrélations, les algorithmes vont donc utiliser les données présentes sur ces images, c'est à dire des informations

et caractéristiques relatives aux corps et aux comportements, les « données biométriques ». Mais cette qualification de « biométrie » fait tout de suite appel à l’imaginaire de l’intime et revêt une symbolique forte ainsi qu’une connotation intrusive.

Dans leurs discours, les entreprises se sont ainsi efforcées de masquer cette réalité en ayant recours à des jeux sémantiques et des périphrases. Les logiciels de VSA sont généralement présentés comme analysant et classifiant des « objets », bien que cette catégorisation inclue des personnes.

Les entreprises de VSA sont pour cela aidées par le milieu académique. Des chercheur·ses ont récemment démontré comment le milieu scientifique du *computer vision* faisait dominer **une perception neutre et purement intellectuelle des technologies d’analyse automatisée d’images d’humain·es**. En **séparant leurs recherches et les applications et usages** qui en seront fait en aval, tout en minimisant le fait qu’elles traitent des données d’humain·es, les chercheur·ses contribuent à **dissimuler le lien consubstantiel entre la technologie et ses applications pratiques, qui en font alors une couche fondatrice d’un paradigme de surveillance**¹⁹.

En ne distinguant pas les humain·es des objets, les entreprises visent à homogénéiser et mettre au même niveau les données traitées pour ces deux catégories, alors qu’elles sont politiquement et juridiquement très différentes dans leurs conséquences. Utiliser la couleur d’une voiture pour établir des corrélations n’a pas les mêmes incidences qu’utiliser la couleur de peau d’une personne. En mettant tout dans le même sac, **les promoteurs de la VSA écartent toute discussion politique sur la surveillance** dont leurs logiciels sont l’instrument.

19 — Pratyusha Ria Kalluri, William Agnew, Myra Cheng, Kentrell Owens, Luca Soldaini, Abeba Birhane, « The Surveillance AI Pipeline », septembre 2023 : <https://arxiv.org/abs/2309.15084?ref=404media.co>.

Le tableau ci-dessous fournit une brève description de chacune des dimensions disponibles :

Nom de la dimension	Description	Exemples de valeurs
Classe	Classe d'objet G	arçon, Fille, Voiture, Camion
Classe (Personnes)	Seules les classes d'objets "Personne", c'est-à-dire : Garçon, Fille, Homme, Femme	Garçon, Fille, Homme, Femme
Classe (Véhicules routiers)	Seules les classes d'objets "Véhicules routiers", c'est-à-dire : Moto, Voiture, Pickup, Fourgonnette, Camion, Bus	Moto, Voiture, Pickup, Fourgonnette, Camion, Bus
Catégorie de classe	Contient les catégories de classe suivantes : <input checked="" type="checkbox"/> Personnes : Garçon, Fille, Homme, Femme <input checked="" type="checkbox"/> Vélos : Vélo <input checked="" type="checkbox"/> Véhicules routiers : Moto, Voiture, Pickup, Fourgonnette, Camion, Bus <input checked="" type="checkbox"/> Autres véhicules : Train, Avion, Bateau	Personnes, Vélos, Véhicules routiers, Autres véhicules
Couleur	Couleur principale de l'objet	Noir, Vert, Orange
Heure de fin de l'objet	Heure de fin de l'objet dans le cadre 1	9/03/2018 13:04:11
Heure de début de l'objet	Heure de début de l'objet dans le cadre 1	9/03/2018 13:00:02
Date	Date de l'objet 1	9/03/2018
Date et Heure	Date et Heure de l'objet 1	9/03/2018 13:03
Jour	Jour de l'objet L	un, Mar, Mer
Jour (numéro)	Numéro du jour de l'objet (par exemple 19 si la date est 19/03/2018)	1,2,15,17,19
Heure	Heure de l'objet dans le format de plage horaire	04:00-05:00, 21:00-22:00
Heure (hh)	Heure de l'objet dans le format heure 0	6:00

De la même manière, les logiciels ne viseraient pas des « comportements » mais des « situations ». Concernant l'**audiosurveillance algorithmique** implantée dans ses rues par la société Sensivic, la ville d'Orléans a par exemple tenté de la faire passer **pour un simple « détecteur de vibration de l'air »**²⁰. Cette technologie, en réalité basée sur la pose de microphones couplés à un logiciel d'analyse algorithmique, fonctionne comme la VSA et la reconnaissance faciale sur de l'analyse de l'activité humaine afin de **repérer des cris ou divers bruits**.

Enfin, en mettant en avant que toute erreur du logiciel serait uniquement due à des « biais » et des « corrélations surreprésentées », les entreprises sous-entendent de nouveau qu'il serait possible d'avoir un algorithme neutre, fournissant une analyse objective de la réalité. Cela tend à alimenter l'illusion que toute erreur du logiciel serait uniquement liée à un dysfonctionnement technique réparable. Pourtant, nous l'avons vu, **toutes les décisions prises par le logiciel sont politiques** et ne sont que le **reflet de décisions et visions humaines antérieures et gravées dans le code de l'algorithme**. En insistant sur le fait que **la véritable décision serait, elle, prise par l'humain** au bout de la chaîne, les discours de promotion de la VSA (que l'on retrouve dans la bouche des institutions) masquent, délibérément ou par incompréhension de la technique, tous les choix opérés par les fabricants qui influencent et orientent cette décision.

■ Minimiser l'impact sur les libertés

Une autre stratégie consiste à **rapprocher la surveillance opérée par la VSA d'autres usages technologiques qui semblent beaucoup moins problématiques**. Sont ainsi mises en avant les situations où l'activité humaine est la moins perceptible : compter des voitures, repérer des ordures déposées sur des trottoirs ou des bagages abandonnés par exemple. Mais c'est oublier que pour cela l'algorithme sonde continuellement les flux vidéo de la rue ou de l'espace public où se situe l'objet concerné. Par ce détour rhétorique, les entreprises se gardent bien de faire comprendre que, même **pour repérer un objet, les humain-es sont analysé-es en permanence**.

20 — Voir l'analyse ici : <https://www.laquadrature.net/2023/01/12/surveillance-sonore-orleans-baratine-la-justice/>.

Dans cette **logique de minimisation**, est souvent mise en **concurrence la capacité d'atteinte aux libertés des différents outils de surveillance biométrique, pour en présenter certaines comme inoffensives**. Tout l'enjeu de cette stratégie est de hiérarchiser ces technologies afin de jeter l'opprobre sur certaines et ainsi maintenir les autres dans l'opacité pour en cacher la gravité. Les entreprises de l'industrie de la surveillance biométrique entendent par cette rhétorique contribuer à dessiner la ligne d'un soi-disant « garde-fou » tout en se donnant l'image de se préoccuper des libertés alors qu'elles sont en réalité en train de les piétiner.

La reconnaissance faciale est alors un outil stratégique très utile. Bien connue, et ce depuis longtemps, car très représentée dans la fiction dystopique, elle évoque instantanément la surveillance de masse : elle est dans l'imaginaire collectif la « ligne rouge » à ne pas franchir. Conscientes de cela, les entreprises tentent de **créer une différenciation entre la reconnaissance faciale, dangereuse, et les autres technologies de surveillance biométrique**, qui seraient beaucoup moins graves en comparaison et donc finalement acceptables. On retrouve ainsi dans des textes de lois une interdiction de recourir à la reconnaissance faciale qui est alors présentée comme une garantie, alors que bien d'autres cas d'usage de la VSA ne recourant pas à l'empreinte faciale fonctionnent de la même manière, et présentent les mêmes dangers pour la société.

■ Saisir toutes les opportunités

Toutes les occasions sont bonnes pour introduire une mesure de surveillance dans le débat public. Pour cela, **activer le sentiment d'insécurité et jouer sur la peur** lors d'évènements sortant du quotidien est un **opportunisme facile**. La technologie est de cette façon présentée comme un **outil magique** permettant de résoudre un problème inédit. L'épidémie de Covid-19 a par exemple été prétexte à l'usage de drones, à la mise en œuvre du suivi de nos déplacements et à une accélération de la collecte des données de santé.

Pour la VSA, **ce sont les Jeux Olympiques qui ont été instrumentalisés pour accélérer l'agenda politique de légalisation de cette technologie**.

De façon générale, les méga-événements sportifs, par leur dimension exceptionnelle et « hors du temps », permettent la mise en œuvre et l'accélération de politiques tout aussi exceptionnelles. Le chercheur Jules Boykoff compare²¹ ce phénomène d'accélération législative à la « théorie du choc » dégagée par Naomi Klein, qui décrit la façon dont les gouvernements 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. Il 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 « extraordinaire », où les règles politiques peuvent être temporairement suspendues, pour faire progresser des politiques qui auraient été impossible à mettre en place en temps normal.

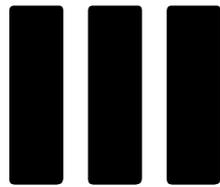
Par exemple, pour les JO de Tokyo en 2021, le gouvernement japonais a fait passer une loi « anti-conspiration »²² voulue de longue date pour mater les groupes militants et syndicaux, et fortement critiquée, notamment par les Nations Unies, au regard des atteintes aux libertés qu'elle créait et aux pouvoirs de surveillance qu'elle conférait à l'État. Plus récemment, le Qatar a mis en place un grand système de surveillance²³ des personnes assistant à la Coupe du monde de football en 2022.

En France, le gouvernement a utilisé les JO de Paris 2024 pour favoriser l'acceptation de la VSA. Gérald Darmanin l'a dit explicitement : « *À situation exceptionnelle, moyens exceptionnels* ». Pourtant, cette technologie ne changera en rien le déroulement de cet événement qui nécessite d'avantage de soutiens logistiques et humains qu'autre chose. Non, **cette échéance sportive a juste permis d'accélérer un agenda politique beaucoup plus large et prévu de longue date : l'enracinement de l'empire de la surveillance généralisée dans l'espace public.**

21 — Jules Boykoff, « Les Jeux Olympiques, le capitalisme de fête et la réponse des activistes », 2019 : <https://saccage2024.noblogs.org/files/2021/07/boykoff-v5.pdf>.

22 — Yann Rousseau, « Le Japon adopte une loi sécuritaire controversée », Les Échos, 16 juin 2017 : <https://www.lesechos.fr/2017/06/le-japon-adopte-une-loi-securitaire-controversee-172489>.

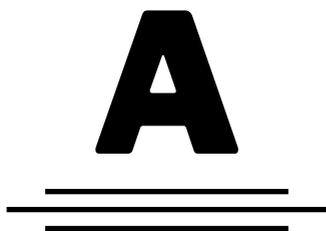
23 — Clément Le Foll et Clément Pouré, « Mondial : le Qatar met les supporters et le pays sous étroite surveillance », Mediapart, 19 novembre 2022 : <https://www.mediapart.fr/journal/international/191122/mondial-le-qatar-met-les-supporters-et-le-pays-sous-etroite-surveillance>.



**Le pire
est à venir**

Le contrôle de la rue a débuté il y a plus de trente ans avec les premières installations de caméras. Il s'accélère drastiquement avec le développement des algorithmes de surveillance biométrique. La légalisation de la VSA dans la loi relative aux Jeux Olympiques adoptée en 2023 amorce un pivot dans cette refonte sécuritaire de l'espace public. **Derrière la légalisation inédite de certains usages de VSA, ce sont d'autres dispositifs techno-sécuritaires, déjà parfois illégalement expérimentés, qui pourraient à leur tour être légalisés.** Catégorisation biométrique, reconnaissance faciale, capteurs en tout genre... Les demandes politiques pour la légalisation de nouveaux outils de surveillance sont nombreuses, et leur implémentation risque d'arriver bien plus vite qu'on ne pourrait le croire.





Un agenda politique ancien

Pour comprendre la place accordée à la VSA aujourd'hui, il faut revenir sur l'histoire de son **infrastructure de base : la vidéosurveillance**. Apparue dans les années 1990, elle a rapidement été présentée comme une réponse technosolutionniste à exploiter pour lutter contre le sentiment d'insécurité.

■ Gabegie financière

Après la création d'un cadre juridique en 1995²⁴ et suite à plusieurs déploiements locaux controversés, c'est sous le quinquennat de Nicolas Sarkozy **dans les années 2000 que l'État s'en est saisi pour en faire un instrument de politique nationale**. En 2007 est créé le Fonds interministériel de prévention de la délinquance et de la radicalisation (FIPDR). Ce fonds finance notamment des plans de prévention et très vite, les subventions du FIPDR accordées aux communes ont été orientées vers l'installation de caméras de surveillance. Deux tiers des crédits y étaient affectés entre 2010 et 2012²⁵. Et en 2023, 30 millions d'euros ont été versés pour des projets relatifs à la vidéosurveillance, soit un doublement par rapport aux sommes mobilisées pour ce type de projets entre 2007 et 2009.

24 — Loi n° 95-73 du 21 janvier 1995 : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000369046>.

25 — Philippe Robert et Renée Zauberman, Du sentiment d'insécurité à l'État sécuritaire, Le Bord de l'eau, 2017, p. 91.

Ce financement a porté ses fruits puisque **le nombre de caméras a explosé**. Pour les seules caméras de vidéosurveillance déployées par la police et les collectivités locales sur la voie publique, on en comptait au minimum 90 000 début 2023, auxquelles s'ajoutent environ 50 000 caméras-piétons et 800 drones de la police et de la gendarmerie nationales²⁶.

Comme pour toute politique publique aussi dispendieuse, il devrait exister des évaluations fiables de l'efficacité ou de l'utilité de la vidéosurveillance classique. **Pour les sociologues Philippe Robert et Renée Zauberman**, « *cette montée en puissance a été facilitée par le refus systématique de toute évaluation véritable, camouflé derrière une pseudo-évaluation administrative qui ne respecte aucune des règles du genre* ». En effet, l'État se refuse à produire toute forme d'évaluation et les rares études indépendantes menées sur le sujet pointent toutes vers **l'inefficacité et le caractère dérisoire du rapport coût/bénéfice de la vidéosurveillance**.

Parmi les quelques études qui existent tout de même, le rapport de la Cour des comptes de 2020 rappelle²⁷ 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* ». La vidéosurveillance est donc inefficace et inutile. Et pourtant, les autorités refusent de l'admettre et continuent de citer quantité d'anecdotes ou de témoignages de policiers indiquant qu'elle serait en réalité cruciale à la résolution des affaires ou à la prévention de la délinquance.

Les industriels ont réussi à surfer sur ce « bluff technologique » pour proposer de nouveaux produits et alimenter leur business : si les caméras ne sont pas efficaces, c'est qu'elles ne sont pas encore assez nombreuses. Il faudrait ainsi plus de caméras disséminées sur le territoire, que celles-ci soient dotées d'une meilleure définition, qu'elles offrent une champ de vision plus large (d'où l'arrivée de caméras 360, à pivot, etc.). **Le constat d'échec devient un prétexte pour persévérer dans cette voie technosolutionniste.**

26 — Philippe Gosselin et Philippe Latombe, « Rapport d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité », Assemblée Nationale, 12 avril 2023 : https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information.

27 — Cour des Comptes, Rapport « Les polices municipales », octobre 2020, p. 70 : <https://www.ccomptes.fr/fr/publications/les-polices-municipales>.

La loi « Sécurité Globale », adoptée en 2020, a constitué un catalyseur de cette logique visant à augmenter le nombre et le type de caméras (drones, caméras-piéton, caméras embarquées, caméras dans les hall de HLM ou les salles de garde à vue) et le nombre de personnes pouvant avoir accès à ces flux (SNCF, RATP, sécurité privée) au nom du sacro-saint « continuum de sécurité ». **Désormais, c'est l'automatisation de l'analyse des flux qui est brandie comme la panacée.**

La VSA s'inscrit donc dans cette **fuite en avant sécuritaire**. Mais elle résulte d'une autre dynamique, plus discrète et pourtant bien plus dangereuse : **celle de la biométrie et de l'analyse automatisée des corps dans l'espace public urbain.**

■ La mise sous pression biométrique

La volonté d'ajouter à la vidéosurveillance des logiciels d'analyse biométrique n'est pas apparue avec les Jeux Olympiques. Diverses prises de positions d'acteurs institutionnels démontrent **l'existence d'un agenda politique assumé.**

Les premières velléités de légaliser le couplage de la vidéosurveillance à la reconnaissance faciale apparaissent ainsi dès 2019 dans une note rédigée par le député macroniste Didier Baichère. Il prenait déjà comme prétexte les Jeux Olympiques, pour tenter de légaliser le recours à la reconnaissance faciale en temps réel²⁸. Cette proposition a été relayée par le secrétaire d'État au numérique Cédric O, qui, en octobre 2019 appelle à « *expérimenter la reconnaissance faciale pour que nos industriels progressent*²⁹ ».

28 — Didier Baichère, « La reconnaissance faciale », Note scientifique de l' Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST), juillet 2019 : <https://www2.assemblee-nationale.fr/content/download/82754/922439/version/1/file/Note+Scientifique+-+Reconnaissance+Faciale+-+VF+19072019.pdf>.

29 — Cédric O, « Expérimenter la reconnaissance faciale est nécessaire pour que nos industriels progressent », Le Monde, 14 octobre 2019 : https://www.lemonde.fr/economie/article/2019/10/14/cedric-o-experimenter-la-reconnaissance-faciale-est-necessaire-pour-que-nos-industriels-progressent_6015395_3234.html.

Au même moment, un colonel de gendarmerie expliquait dans une note dédiée à la reconnaissance faciale que, une fois couplée aux dizaines de milliers de caméras de vidéosurveillance installées sur la voie publique, cette technologie permettrait d'instaurer « *un autocontrôle limitant les incivilités (respect du code de la route, déjections animales, dépôts d'ordures) sur le modèle du crédit social chinois*³⁰ ».

Publié un an plus tard, le **Livre Blanc de la sécurité intérieure** venait acter ce projet, proposant d'augmenter les budgets de la police, notamment pour permettre le **déploiement de « l'identification biométrique à distance («visage, voix, odeur») et autres « technologies de reconnaissance du visage » ou de « lecture automatisée des plaques d'immatriculation »**. Ce même livre blanc « *estimait hautement souhaitable d'expérimenter la reconnaissance faciale dans les espaces publics*³¹ ».

Une telle proposition n'est pas restée lettre morte et a été reprise d'abord par le député Jean-Michel Mis dans son rapport sur les technologies de sécurité en 2021, puis par trois sénateurs en 2022 dans un rapport sur la « reconnaissance biométrique ». Marc-Philippe Daubresse (LR), Arnaud de Belenet (Union centriste) et Jérôme Durain (PS) proposaient à la fois d'expérimenter la reconnaissance faciale en temps réel et de recourir à ces technologies pour détecter certains événements. Ils imaginaient aussi comment pourrait être utilisée la VSA pour « *détecter certaines caractéristiques des personnes, comme par exemple le port de dispositifs occultant le visage d'un individu ou d'un groupe d'individus au sein d'une foule, pour permettre le suivi des personnes considérées comme de potentielles menaces - comme des blackblocs par exemple*³² ».

30 — Dominique Schoener, « Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité », Note du Centre de recherche de l'école des officiers de la gendarmerie nationale (CREOGN), septembre 2019 : <https://www.gendarmerie.interieur.gouv.fr/cragn/Publications/Notes-du-CREOGN/Reconnaissance-faciale-et-controles-preventifs-sur-la-voie-publique-l-enjeu-de-l-acceptabilite>.

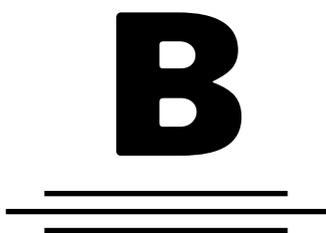
31 — Ministère de l'Intérieur, Livre blanc de la sécurité intérieure, 2020, p. 9 et p. 263 : <https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Livre-blanc-de-la-securite-interieure>.

32 — Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, « La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », Rapport d'information de la Commission des lois, mai 2022 : <https://www.senat.fr/notice-rapport/2021/r21-627-notice.html>.

Mais face à la contestation de la société civile, les cas d'usage de la VSA les plus sensibles au plan politique, et en particulier la reconnaissance faciale, ont été momentanément délaissés au profit d'applications en apparence moins sensibles pour les libertés publiques. Une **stratégie des petits pas** parfaitement résumée par le député Philippe Latombe lors d'une allocution en juin 2023 devant l'AN2V, le lobby de la vidéosurveillance :

« Avec la reconnaissance faciale, on touche à un tabou absolu, on touche au truc qui fait que ça fait hurler tout le monde. Ce que nous avons proposé (...), et je pense que c'est la vraie bonne façon de faire les choses : si on y va d'un coup d'un seul (...), ça va tellement crisper que ça passera pas. Il faut y aller en touchant les choses du bout du doigt et en y allant dans des cas très particuliers et très bien protégés, très bien balisés³³. »

33 — Félix Tréguer, « En visite aux « nuits de l'AN2V », le lobby de la vidéosurveillance », lundimatin, juillet 2023 : <https://lundi.am/En-visite-aux-nuits-de-l-AN2V-le-lobby-de-la-videosurveillance>.



La loi « Jeux Olympiques », première brique légale hypocrite

Cette stratégie des petits pas s'incarne donc dans la loi n° 2023-380 du 19 mai 2023 relative aux Jeux Olympiques et Paralympiques de 2024, dont **l'article 10 prévoit un cadre expérimental dédié à la VSA**. Elle constitue la **première brique légalisant un usage policier de ces technologies**.

■ Explication de texte

Que prévoit exactement ce texte ? Jusqu'en mars 2025, des solutions de VSA pourront être utilisées pour tout type « *d'événement récréatif, sportif et culturel* » *accueillant du public* et « *particulièrement exposé à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes* ». Contrairement à ce que laisserait penser l'intitulé de la loi, il ne s'agit donc pas seulement des Jeux Olympiques, loin s'en faut : **les festivals de musique, les matchs de foot sont autant d'événements qui rentrent dans le champ de l'expérimentation**. À titre d'exemple, la première utilisation de la VSA par la préfecture de police de Paris a eu lieu en avril 2024 lors d'un concert des Black Eyed Peas ainsi que pour un match entre le PSG et l'OL.

Les algorithmes de VSA, branchés aux caméras de vidéosurveillance, sont déployés sur et aux abords de ces événements publics, ainsi que dans les réseaux de transports avoisinants (gares et stations). Ils sont censés détecter en temps réel **huit catégories d'évènements** :

- présence d'objets abandonnés,
- présence ou utilisation d'armes,
- non-respect par une personne ou un véhicule du sens de circulation commun,
- franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible,
- présence d'une personne au sol à la suite d'une chute,
- mouvement de foule,
- densité trop importante de personnes,
- départs de feux³⁴.

On le voit, le gouvernement et le Parlement ont fait le choix de retenir des cas d'usages en apparence peu sensibles du point de vue des libertés publiques.

Sur le terrain, c'est toute **une ribambelle d'acteurs qui pourra utiliser ces logiciels : agents de polices municipales, de police nationale, de gendarmerie nationale, des force de sécurité des sociétés de transport** présentes sur les lieux en question (RATP, SNCF). Enfin, chaque déploiement sur un lieu donné et pour une période déterminée est autorisé par arrêté préfectoral, ces derniers indiquant également les événements devant être détectés parmi la liste prévue dans le décret.

34 — Décret n° 2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048007135>.

■ Une opportunité pour le secteur privé

Les systèmes de VSA utilisés sont, sans surprise, développés par des entreprises du secteur. **Le ministère de l'Intérieur a acquis les solutions techniques auprès de prestataires privés** après avoir lancé un marché public.

Un marché divisé en **quatre lots géographiques, tous remportés par des entreprises françaises**. La startup **Wintics** installe donc ses logiciels en Île-de-France quand **Videtics** se charge de l'Outre-Mer et d'un ensemble de régions du Sud (Provence Alpes Cote d'Azur, Rhône-Alpes et Corse). Pour les autres régions de France, c'est **ChapsVision** qui a été désignée. Cette entreprise, omniprésente dans les services de l'État et qui se veut le nouveau Palantir français, a récemment racheté la startup de VSA belge **ACIC** afin d'entrer sur le marché de la VSA. Enfin, **Wintics** s'est également vu attribuer la surveillance des transports (gares et stations). Quant à **Orange Business Service** – en partenariat avec **IpsoTek**, filiale d'**Atos** (nouvellement Eviden), elle est également attributaire du lot des transports et mobilisable en cas de défaillance de **Wintics**.

Au sein du ministère de l'intérieur, un **comité de pilotage** créé pour l'occasion chapeautera ce déploiement³⁵. Il est dirigé par **Julie Mercier**, cheffe de la direction des entreprises et partenariats de sécurité et des armes (DEPSA) au sein du Ministère, ce qui en dit long sur les intérêts en jeu. **Favoriser l'innovation « à la française » est un véritable objectif politique** qui pousse l'État à s'associer de plus en plus avec les acteurs privés.

La CNIL a d'ailleurs opéré un virage assumé dans cette direction ces dernières années. Originellement créée dans les années 1970 pour constituer un contre-pouvoir vis-à-vis des capacités de surveillance de l'État sur la population, l'autorité française de protection des données assume aujourd'hui de privilégier l'aide aux entreprises. Elle a ainsi lancé en 2023 une « offre d'accompagnement renforcé » pour aider les sociétés « présentant un fort potentiel de développement économique ou d'innovation » à se conformer à la législation.

35 — Décret n° 2023-939 du 11 octobre 2023 relatif aux modalités de pilotage et d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048197679>.

La CNIL se vante ainsi d'avoir accompagné les entreprises de VSA alors qu'elle aurait pu envoyer un signal politique fort en sanctionnant leurs pratiques.

Pour l'industrie de la vidéosurveillance, le marché public lié à l'expérimentation permise par la loi JO est apparu comme hautement stratégique. En effet, ce marché constitue une occasion unique pour les entreprises de VSA de faire la preuve de la supériorité de leurs produits, tout en affinant leurs modèles grâce à l'accès aux masses de données de vidéosurveillance qui s'ouvrent pour elles dans ce cadre.

■ Une « évaluation » jouée d'avance

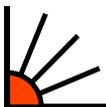
La loi relative aux Jeux Olympiques prévoit de façon assez originale une « évaluation » de l'expérimentation. Mais derrière ce terme, il faut déceler une supercherie censée elle aussi garantir « l'acceptabilité sociale » d'une technologie controversée – en l'occurrence la VSA. En évoquant un dispositif au caractère temporaire et réversible et qui sera évalué en fin de course, **il s'agit surtout de rassurer la population.**

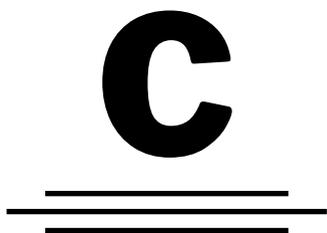
Un **comité d'évaluation** a été créé pour rendre compte de ces « tests »³⁶. On est toutefois en droit de s'interroger sur la capacité de ce comité d'évaluation à battre en brèche le technosolutionnisme à l'œuvre dans cette opération de légitimation de la VSA. Ce type d'approche expérimentale surnommée « bac à sable réglementaire » permet à l'État et aux industriels d'édicter un cadre juridique temporaire afin de favoriser l'innovation, en abaissant les garanties apportées à certaines réglementation d'intérêt général, notamment en matière environnementale ou pour la protection des droits humains. C'est ce qu'il risque de se passer ici : **l'évaluation ne sera pas faite sur les critères juridiques classiques de nécessité ou de proportionnalité de la mesure de surveillance mais sera plutôt guidée par une approche pragmatique** (évaluation de l'impact et des effets, performance technique des algorithmes) **et chiffrée** (nombre d'alertes pertinentes générées, nombre d'interpellations...).

36 — Décret n° 2023-939 du 11 octobre 2023 : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048197679>.

Surtout, on peine à voir comment, à l'issue de l'expérimentation, l'État abandonnerait soudainement le projet de déploiement massif d'une technologie dans laquelle il a tant investi et à laquelle il a déjà cédé énormément de place dans les pratiques policières. Les exemples passés nous montrent que **les projets sécuritaires censés être temporaires sont systématiquement prolongés**, telles que les boîtes noires de la loi Renseignement ou les dispositions dérogatoires de l'état d'urgence.

C'est pourquoi **l'issue du comité d'évaluation risque donc d'être surdéterminée par les enjeux politiques et économiques** : si l'efficacité policière de la VSA est jugée satisfaisante, on appellera à la pérenniser ; dans le cas contraire, on évoquera la nécessité de poursuivre les processus de développement afin que ces technologies parviennent à un stade de maturation plus avancé, ce qui justifiera de proroger le cadre expérimental jusqu'à ce que, *in fine*, elles aient fait leurs preuves. Dans un cas comme dans l'autre, au bout du compte, c'est toujours la police et les industriels qui gagnent.





L'arbre qui cache la forêt

Derrière la légitimation légale de quelques usages de la VSA à travers la loi sur les Jeux Olympiques, il y a en réalité tout un tas **d'autres technologies biométriques existantes**. Qu'elles soient déjà utilisées illégalement ou encore en développement, **elles dessinent le projet sécuritaire de contrôle de l'espace public voulu par les promoteurs de la surveillance**.

■ Les entreprises savent faire bien plus

VSA en temps réel ou sur des images archivées, **suivi de personnes et réidentification** à partir d'attributs physiques ou comportementaux (par exemple suivre et retrouver quelqu'un en fonction de la couleur de ses habits), **reconnaissance des émotions, reconnaissance faciale, comptage et catégorisation des profils ou des modes d'occupation de l'espace public** : toutes ces **applications de surveillance biométrique sont déjà proposées par les entreprises de surveillance**. Elles reposent toutes sur la même technologie de *machine learning* et sont développées par les mêmes ingénieurs, suivant des logiques techniques identiques. Chacune de ces applications ne constitue qu'un cas d'usage dans le panel de possibilités techniques offertes par la vidéosurveillance algorithmique.

Étendue des usages de la

VSA légale

Selon la loi sur les Jeux Olympiques et Paralympiques : il s'agit d'expérimentations dans le cadre d'un événement sportif ou culturel, limité dans le temps et dans l'espace possibles jusqu'en mars 2025

Détection de :

départ de feu

franchissement de ligne

déplacement à contre-sens

personne au sol

port ou usage d'armes

densité importante de personnes

bagage abandonné

mouvement de foule

Détection hors personnes :

animaux

véhicules

Lecture de :

plaques d'immatriculation

VSA illégale mais déjà en usage

Détection et suivi de personne :

par reconnaissance faciale

par ensemble de caractéristiques physiques

statique
(sert à retrouver les personnes sans domicile, les personnes qui mentient, les travailleuses du sexe, les "guetteurs", les "zonards"...)

se regroupant à plus d'un certain nombre

se déplaçant "trop" ou "pas assez vite"

exprimant une certaine émotion

en train de taguer

en train de voler

en train de dégrader

dans une certaine position
(accroupie, à genoux etc.)

portant ou non un masque

déposant des ordures

ayant un comportement "anormal" (c'est-à-dire peu fréquent ou inexistant dans les flux vidéo d'entraînement)

VSA en 2024

Liste non-exhaustive des usages recensés par les différents groupes Technopolice.

Recherche de personne et reconstitution de son trajet :

par reconnaissance faciale

d'une certaine couleur de peau

selon ses vêtements et leur couleurs

selon sa coupe de cheveux et leurs couleurs

selon ses accessoires

selon son genre

selon son âge

Recherche et reconstitution de déplacement de véhicules :

selon son modèle et sa couleur

selon sa plaque d'immatriculation (même partielle)

Autres fonctionnalités

condensé selectif de vidéos (suppression des moments d'inactivité dans de gros volumes d'image)

Usages potentiels de la VSA

Non retrouvés dans le recensement effectués par les groupes Technopolice mais techniquement réalisables

Détection et suivi de personnes :

jouant au ballon

collant des affiches

distribuant des tracts

portant un voile

mineurs sans adultes (par exemple lors d'un couvre-feu)

consommant une boisson alcoolisée

titubant (pour retrouver une personne en état d'ébriété)

Plusieurs entreprises françaises de VSA proposent déjà des applications de reconnaissance faciale : c'est le cas par exemple d'Idemia, Thales, Axis, Avigilon ou encore de Two-I. Pour l'heure, celles-ci ne sont proposées que dans les États les moins regardants sur la protection des libertés. Parmi les entreprises retenues dans le cadre du marché public lié à la loi « Jeux Olympiques », **Ipsotek**, filiale d'Atos-Eviden assume ainsi de faire de la **reconnaissance faciale en temps réel** et a notamment équipé l'aéroport d'Abu Dhabi, aux Émirats arabes unis. L'entreprise se vante sur son site Internet que son produit VIFace ait été « *déployé sur plus de 300 caméras à tous les principaux points d'arrêt de l'aéroport afin de détecter [des personnes] inscrites sur la liste de surveillance et d'aider les opérateurs en mode judiciaire à trouver et à suivre les individus*³⁷ ».

Comme nous l'avons illustré précédemment (voir p. 41), la **reconnaissance faciale** fait déjà partie des fonctionnalités activées par défaut dans les **logiciels de Briefcam vendus aux forces de police françaises**³⁸. Quant à **Two-I**, startup spécialisée dans la VSA, elle s'est d'abord lancée dans la **détection d'émotions**, qu'elle a expérimenté dans des gendarmeries et tenté d'utiliser dans les tramways niçois, avant de tester la reconnaissance faciale sur des supporters de football à Metz, puis de se concentrer sur des applications moins sensibles comme du comptage statistique sous couvert d'édifier des « villes intelligentes ». On le comprend, **les huit usages encadrés par la loi de 2023 sont quasiment anecdotiques par rapport à l'étendue des pratiques actuelles**.

■ Un plan de légalisation déjà amorcé

Les technologies sont donc déjà prêtes. Il leur manque seulement un cadre légal et une acceptabilité sociale pour s'imposer dans les pratiques policières. C'est ce à quoi travaillent déjà les institutions et les personnalités politiques.

37 — Voir le site d'ATOS : <https://archive.ph/YKhJF>. Voir aussi le site web d'Ipsotek, qui met en avant des « consumer stories » relatives au déploiement de la reconnaissance faciale : <https://archive.ph/wip/gaNO6>.

38 — D'après Disclose, « la fonction de reconnaissance faciale est activée par défaut » sur Briefcam depuis la mise en place de la version 5.2 du logiciel, qui date de 2018. Voir Clément Le Foll, « Reconnaissance faciale : Gérald Darmanin veut enterrer "l'affaire Briefcam" », Disclose, 9 avril 2024 : <https://disclose.ngo/fr/article/reconnaissance-faciale-gerald-darmanin-veut-enterrer-laffaire-briefcam>.

Alors que l'expérimentation du cadre de la loi JO vient à peine de commencer, **les propositions de législation pour multiplier les cas d'usage de la VSA fleurissent déjà.**

En avril 2023, alors que les débats sur la loi JO s'achevaient tout juste, les députés Philippe Gosselin (LR) et Philippe Latombe (Modem) rendaient un rapport sur les « enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité³⁹ ». Ils y rappelaient les « bénéfiques » que comporteraient la VSA en temps différé et « se félicitaient » des évolutions législatives relatives à la VSA en temps réel dans la loi sur les JO. Comme leurs camarades, ils y allaient également de leurs petites propositions d'évolution législative pour expérimenter la reconnaissance faciale.

En juin 2023, soit moins de trois mois après l'adoption de la loi relative aux Jeux Olympiques, **le Sénat**, à l'initiative du sénateur Marc-Philippe Daubresse, auteur d'un rapport sur le sujet, adoptait une **proposition de loi prévoyant une expérimentation de trois ans pour la reconnaissance faciale.** « Trop tôt », avait en substance répondu le gouvernement⁴⁰. Plus récemment, c'est une proposition de loi relative à la sécurité dans les transports qui propose d'accélérer la légalisation de la VSA, pour des utilisations en temps différé cette fois. Les agents de la RATP et la SNCF pourraient donc mettre en œuvre des filtres de recherche via les attributs biométriques sur les flux de vidéosurveillance, sur la base d'une expérimentation similaire à celle de la loi JO⁴¹.

Dans le même temps, des **élus locaux** sont en embuscade. Alors même qu'ils recourent déjà à des applications de VSA en toute illégalité, **ils font publiquement pression sur le gouvernement pour accélérer le processus de légalisation.** Parmi eux, on retrouve les « *usual suspects* », VRP de l'industrie de la surveillance : ainsi de Christian Estrosi, à Nice, ou de Laurent Wauquiez, président de la région Auvergne-Rhône-Alpes,

39 — Philippe Gosselin et Philippe Latombe, « Sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité », Rapport d'information de la Commission des lois, avril 2023 : https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information#.

40 — Marie Desrumaux. « Le Sénat adopte une proposition de loi sur la reconnaissance biométrique... », AEF info, 13 juin 2023 : <https://www.aefinfo.fr/depeche/693729-le-senat-adopte-une-proposition-de-loi-sur-la-reconnaissance-biometrique-jugee-inopportune-par-le-gouvernement>.

41 — Voir l'article 9 de la proposition de loi relative à la sûreté dans les transports, déposé par Philippe Tabarot et ses collègues : <https://www.senat.fr/leg/pp123-235.html>.

qui en mars 2024 a fait voter une résolution visant à faire appliquer l'expérimentation de la VSA prévue par la loi JO dans les gares et les lycées de sa région⁴².

Et comme souvent, les choses se jouent aussi beaucoup au niveau européen. Soucieux de ne pas injurier l'avenir, **le gouvernement français a ainsi multiplié les manœuvres à Bruxelles pour sécuriser sur le plan juridique le recours à la VSA et anticiper le futur avec la reconnaissance faciale.** Ainsi, un règlement relatif à l'intelligence artificielle a été adopté début 2024, pour lequel la France a réussi à faire obstacle aux demandes du Parlement européen visant à faire interdire le recours à la surveillance biométrique de l'espace public. **Ces pressions auront abouti à ce que le texte final autorise le recours à la VSA, y compris la reconnaissance faciale, à la fois en temps réel et a posteriori.** Même la reconnaissance des émotions, qui ne repose pourtant sur aucune base scientifique, est autorisée dans de nombreux cas, y compris à des fins de détection de mensonges.

■ Des garde-fous factices

Les promoteurs de ce projet de société expliqueront qu'il est impossible de se passer de ces outils, que cela doit se faire de façon encadrée, et qu'il est possible d'inscrire dans la loi des garde-fous capables de protéger les droits et libertés. **Mais l'histoire des technologies de surveillance démontre que les garanties juridiques sont systématiquement inappliquées,** laissées de côté, ouvertement méprisées, sans que les contre-pouvoirs institutionnels, qu'il s'agisse des juges ou de la CNIL, soient capables de les faire valoir.

Le déploiement de la VSA en est l'illustration même. **Elle s'est installée au fil des années en toute illégalité** et il est clair que ni les analyses d'impact, ni les pouvoirs de contrôle de la CNIL, ni les soi-disant contre-pouvoirs locaux comme les comités d'éthique de la vidéoprotection, ni le droit d'information du public, n'ont été d'aucun secours.

42 — Maurane Kerinec, « Wauquiez veut surveiller les trains et lycées régionaux avec l'intelligence artificielle », Reporterre, 22 mars 2024 : <https://reporterre.net/Wauquiez-veut-surveiller-les-trains-et-lycees-regionaux-avec-l-intelligence-artificielle>. «

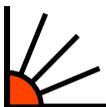
Ce qui domine, c'est plutôt le sentiment d'**impunité totale de la part des responsables**, ce qu'illustre parfaitement **l'affaire Briefcam** au ministère de l'Intérieur, révélée par Disclose en 2020. Car en l'espèce, les cadres de la Direction Générale de la Police Nationale, de même que les ministres successifs, ont sciemment organisé le secret s'agissant du **recours à ce logiciel de VSA par la police, se sachant hors du droit**⁴³. Le ministre Darmanin avait alors annoncé une enquête indépendante dont les conclusions seraient rendues publiques. Or le rapport préparé par l'Inspection générale de l'administration, de même que ses préconisations, ont été vite enterrés⁴⁴. Ici comme dans tant d'autres affaires, ces règles de droit resteront inappliquées.

Résumons donc. Un **gouvernement hypocrite** qui met en avant le caractère « très encadré » du dispositif expérimental prévu par la loi Jeux Olympiques, alors qu'il cautionne l'utilisation illégale du logiciel de VSA de Briefcam par la police nationale, **œuvre à la promotion d'autres technologies de surveillance** et prépare déjà l'avenir. Des **collectivités qui ont utilisé pendant des années un logiciel illégal** et font profil bas en attendant les évolutions législatives. Incompétence et mauvaise foi des **parlementaires** ne faisant aucun effort de compréhension des technologies qu'ils légalisent tant ils **adhèrent au discours sensationnaliste de la « peur de l'insécurité »**. Lâcheté de la part de la CNIL qui, plutôt que mettre un sérieux coup d'arrêt à cette dynamique de surveillance, **conçoit à poser un vernis « éthique » sur ces technologies** en créant l'illusion d'être un garde-fou suffisant. Enfin, mauvaise foi – ou plutôt mensonge – du **complexe industriel de surveillance** qui place ses pions pour **faire de la rue un terrain de jeu commercial** et contribue ainsi à saper la possibilité de formes de vie démocratiques, **contribuant à l'avènement de sociétés autoritaires et répressives**.

43 — Mathias Destal, Clément Le Foll et Geoffrey Livolsi, « La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale », Disclose, 14 novembre 2023 : <https://disclose.ngo/fr/article/la-police-nationale-utilise-illegalement-un-logiciel-israelien-de-reconnaissance-faciale/>.

44 — Clément Le Foll, « Reconnaissance faciale : Gérald Darmanin veut enterrer "l'affaire Briefcam" », Disclose, 9 avril 2024 : <https://disclose.ngo/fr/article/reconnaissance-faciale-gerald-darmanin-veut-enterrer-laffaire-briefcam>.

On le comprend : la seule voie pour que les espaces publics restent des lieux libres, pour ne pas accroître la discrimination des personnes précaires et marginalisées, pour ne pas renforcer le pouvoir de surveillance de la police en légitimant sa violence, la seule voie pour mettre un stop à cette pente glissante dont l'expérimentation légalisée par la VSA n'est que le premier pas, **c'est l'interdiction totale de l'usage d'algorithmes pour analyser les activités humaines à des fins policières.** Autant dire que, à défaut d'une mobilisation déterminée pour y faire obstacle, la banalisation de la vidéosurveillance algorithmique de l'espace public relève du fait accompli, et que sa pérennisation et sa légalisation apparaissent comme de simples formalités.



IV

Riposter

Derrière les expérimentations, **le monde de la surveillance bâtit son empire**. Après avoir balisé le terrain politique, après avoir structuré le milieu économique, la légalisation de la VSA dans la loi relative aux Jeux Olympiques est la première pierre institutionnelle d'une rupture historique : la surveillance permanente et automatisée de nos comportements dans l'espace public urbain.

Partout, nous devons continuer à **matérialiser le refus de ce projet autoritaire** et rappeler que la ville est à nous et qu'elle est un espace de libertés. Cela passera par de multiples voies d'actions⁴⁵ : faire connaître sans détour **qui sont les entreprises et acteurs politiques** promouvant la VSA, **visibiliser les caméras, exiger des comptes** de la part de nos maires et des parlementaires, **s'organiser** localement, **être créatives et créatifs tous-tes ensemble pour se réapproprier l'espace public et faire valoir notre droit à la ville libre**.

Nous pouvons agir pour empêcher l'extension de la surveillance totale de nos rues.

45 — Nous avons déjà esquissé quelques voies d'action contre la vidéosurveillance dans ce guide publié en 2022 : <https://technopolice.fr/guide-videosurveillance.pdf>.

A

Documenter

Un des principaux moteurs de la Technopolice est de se construire et de se développer dans une opacité complète. Pour **battre en brèche les projets de VSA**, il faut donc les rendre visibles, en **comprendre les contours et révéler leur fonctionnement**. En matérialisant leur existence, on parvient à mettre la lumière sur les décisions politiques qui les ont portés et on identifie bien plus clairement la technologie que l'on cherche à combattre.

Visibiliser les technologies et l'infrastructure du numérique est donc un premier jalon essentiel pour une prise de conscience collective et constitue une façon utile de se mobiliser.

Les demandes d'accès aux documents administratifs sont un outil efficace à la portée de toutes et tous pour obtenir des éléments sur les dispositifs de sa ville. Malgré leurs limites pratiques et juridiques, les demandes CADA demeurent un levier efficace pour sortir les projets de surveillance des salles de conseil municipaux où ils sont actés. Depuis le début du projet Technopolice, ce droit aux documents administratif nous a permis de récupérer des marchés publics, des manuels d'utilisation, des cartes d'emplacements des caméras, etc. Pour réaliser une demande CADA, vous pouvez suivre le guide dédié⁴⁶. Nous vous invitons également à utiliser la plateforme MaDada pour centraliser, suivre et partager les différentes demandes que vous avez réalisées⁴⁷.

46 – Voir ici : <https://technopolice.fr/blog/guide-se-reseigner-sur-la-surveillance-dans-sa-ville/>.

47 – Pour cela, créez vous un compte sur <https://madada.fr/>.

Il existe de nombreux autres moyens de documentation, certains déjà bien rodés et d'autres à inventer. Par exemple, la **recherche d'information en source ouverte** sur les sites internet des entreprises de surveillance ou des collectivités permet souvent de trouver des descriptions détaillées de technologies ou de cas d'usages déployés dans certaines villes. On peut également se plonger dans la lecture de compte-rendus de conseils municipaux ou assister à des réunions publiques. Interpeller son maire ou d'autres décideurs – notamment les parlementaires qui devront se prononcer sur la suite du processus de légalisation de la VSA – est également une manière de demander des comptes.

Enfin, si vous travaillez dans des administrations publiques ou des entreprises du secteur, ou si vous connaissez des gens dont c'est le cas, vous pouvez **faire fuiter des documents**⁴⁸ et permettre de lever le voile sur des informations souvent protégées par un « secret des affaires » bien largement interprété.

48 — Vous pouvez pour cela utiliser cette plateforme sécurisée : <https://technopolice.fr/leak/>.

B

S'organiser

Après l'étape de la documentation, **l'opposition à la vidéosurveillance algorithmique passe par des actions**. Il est possible d'agir au niveau national **auprès des institutions**. C'est ce que La Quadrature du Net s'efforce à faire avec d'autres associations comme la Ligue des droits de l'Homme ou Amnesty International, avec certes quelques victoires mais un succès bien trop limité tant les mécanismes démocratiques sont épuisés et le débat accaparé par des conceptions autoritaires.

Mais là où l'action apparaît la plus pertinente et la plus concrète **est à l'échelle des villes et des rues où nous vivons**. Lancée en 2019 par La Quadrature, l'initiative **Technopolice** a ainsi pour objectif d'engager une **dynamique décentralisée** afin de faire résonner sur le territoire les différentes voix qui s'élèvent contre les nouvelles technologies de surveillance policière. Puisque celle-ci change de forme de ville en village, il faut diversifier les fronts et les modes d'actions, s'adapter aux contextes et aux savoir-faire locaux.

Des collectifs se sont ainsi mis en place à Marseille, Montpellier ou encore Forcalquier, et même en Belgique ! Certains ont réussi à faire enlever des micros à Saint-Étienne, quand des plus petites bourgades se sont élevées contre l'arrivée de caméras de vidéosurveillance comme à Foix, Marcillac-Vallon ou Putanges-le-Lac. Des collectifs d'habitantes et d'habitants s'organisent ainsi un peu partout pour recenser, documenter et lutter contre ces technologies, tout en résistance aux politiques sécuritaires qu'on leur impose. **Ces luttes locales sont indispensables** au combat plus global contre la société de surveillance et permettent de remporter des victoires concrètes. Comme en PACA, où en lien avec des collectifs locaux, La Quadrature a réussi à faire interdire le recours à la reconnaissance faciale dans les lycées de la région.

Pour ces luttes ancrées, **les modes d'actions à explorer sont multiples**. Outre l'enquête, la veille et l'analyse, on peut organiser des « ballades cartographiques » pour repérer les emplacements et modèles des caméras et les répertorier sur une carte accessible en ligne ; on peut lancer des actions juridiques, écrire des lettres ouvertes pour politiser les élus locaux sur ces enjeux, organiser des événements d'information, des expositions ou des festivals documentaires autour de la surveillance pour sensibiliser les habitantes et habitants ; on peut **se réapproprier collectivement la notion de « sécurité » et imaginer ensemble des futurs émancipateurs**.

Enfin, il faut **nouer des alliances**. Il est en effet fondamental **d'articuler nos combats contre les technologies de surveillance policière aux autres causes**, aux autres luttes. En région parisienne, les questions de surveillance s'insèrent dans la dénonciation des ravages des Jeux Olympiques. À Marseille, elles sont le pendant de la critique de la gentrification qui gangrène le centre-ville populaire ou du combat contre l'industrie de l'armement qui contribue notamment à équiper l'armée israélienne. À Grenoble, elles se lient avec la lutte écologique contre une usine de fabrication de microprocesseurs, STMicro. Les ponts à imaginer sont nombreux et c'est en créant ces solidarités entre les différents fronts de lutte que nos voix deviendront plus fortes et puissantes.

Pour s'organiser, échanger et faire résonner nos mobilisations, l'initiative **Technopolice**, propose un **forum public**⁴⁹ ainsi qu'une **plateforme de documentation** en écriture collaborative basé sur le logiciel Etherpad (appelé le « Carré »)⁵⁰. De nombreux autres outils similaires visant à appuyer nos combats existent par ailleurs ou sont encore à inventer !

49 — Voir ici : <https://forum.technopolice.fr/>.

50 — Voir ici : <https://carre.technopolice.fr>.

C

Agir

Cette brochure a pour vocation d'être diffusée le plus largement possible afin d'expliquer au plus grand nombre le projet politique mortifère associé à la vidéosurveillance algorithmique. Il s'agit de **prendre prise**.

Dans les prochains mois, les expérimentations de la VSA légalisées par la loi sur les Jeux Olympiques auront lieu dans toute la France. Elles seront **un moment important de mobilisation**. Par ailleurs, le texte du décret prévoit que l'évaluation finale prenne en compte « *la perception par le public de l'impact des traitements algorithmiques sur la sécurité et l'exercice des libertés publiques* ». Il s'agit donc de faire valoir nos perceptions et **notre refus de ces technologies iniques**.

Les algorithmes de VSA vont être déployés lors de concerts, de festivals, de matchs de foots, de marchés de Noël. Ces événements sont tout autant d'occasions de faire valoir notre opposition. Là aussi soyons créatives et créatifs ! Notre refus peut se concrétiser aussi bien dans un courrier de **plainte à la CNIL**⁵¹ que dans une danse « suspecte » devant l'œil des caméras. C'est aussi le moment de « tenir la rue » pour **matérialiser la surveillance** qui se déploiera sur les personnes venues à ces événements et **informer** ces dernières qu'elles sont les cobayes d'une analyse algorithmique à grande échelle : **visibiliser** par tout moyen la présence de caméras, **tracter, coller** des affiches⁵²... les manières de faire sont multiples.

51 — Voir ici : <https://www.cnil.fr/fr/plaintes>.

52 — Visitez notre page de campagne : <https://laquadrature.net/vsa>

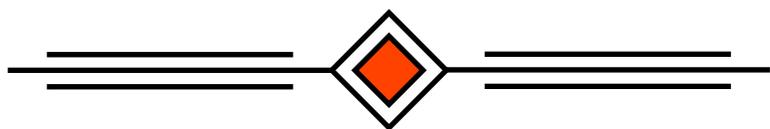
D

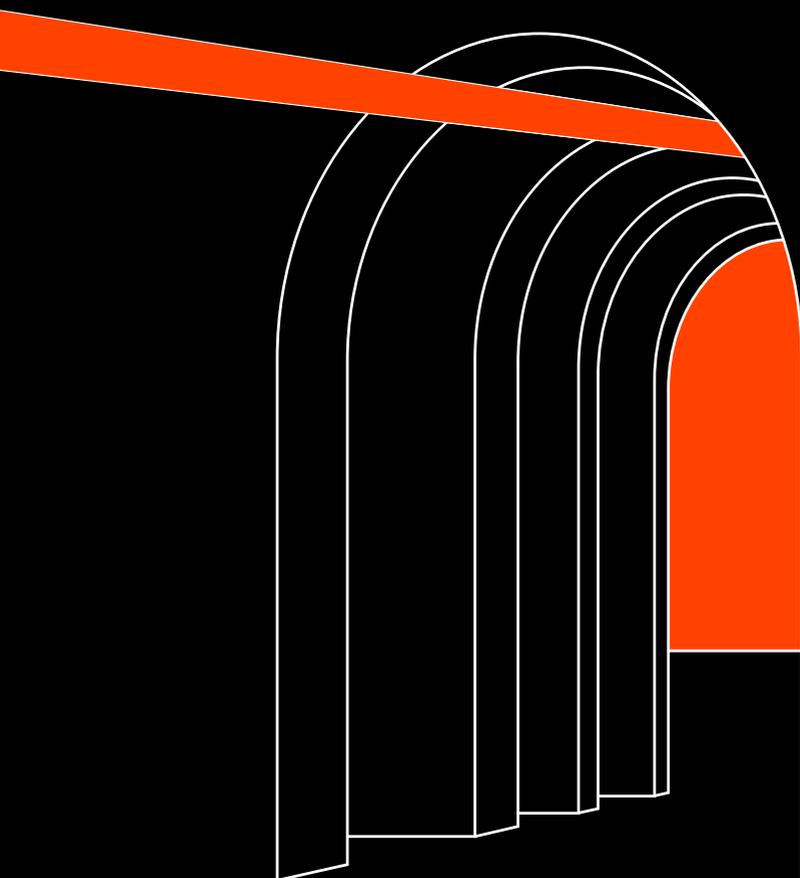
Reprendre la ville

Depuis toujours, **les gouvernants se méfient de la ville**. C'est que, depuis toujours, elle est le lieu de la contestation. Sur ses murs, on partage notre colère. Dans ses rues, on s'organise et on manifeste. On occupe ses places et ses ronds-points pour revendiquer nos droits. Alors, à coup de programmes d'urbanisme sécuritaire, les promoteurs de la Technopolice tentent de la contenir. Après l'invention de la police moderne sous l'Ancien Régime, après les percées haussmaniennes qui empêchent les barricades et les grandes places qui favorisent la police comme la Plaine de Marseille ou la Place de la République, c'est **la VSA qui est convoquée pour nous museler**.

La ville on y manifeste, mais on y flâne aussi. On y observe l'architecture, on la dessine ou on la prend en photo. On en prend soin, à notre manière. On y construit des contre-cultures émancipées des normes et des oppressions. On y danse, on y fait du skate, du graffiti. On s'y assoit, on y fait la fête, on passe le temps ou on l'explore dans tous ses recoins. La densité de ses espaces oblige à être créatives, à en investir les quais, les places, les bancs pour se retrouver et construire des sociabilités et des solidarités, ou juste ne rien faire. Dans la rue, on rencontre des inconnu-es, on se confronte à l'altérité. On aide à réparer un vélo ou à ramasser des courses tombées. On se délecte du joyeux chaos qu'elle nous donne à voir.

C'est pour continuer à habiter librement la ville que nous refusons la surveillance permanente, générale et invisible de la police, que nous voulons tenir en échec la vidéosurveillance algorithmique et son monde. La VSA ne passera pas !





Mai 2024



La
Quadrature
du Net