



# Vidéo surveillance algorithmique

Novembre 2024

La vidéo-surveillance est un marché lucratif et de nombreuses communes s'équipent, et parfois sont contraintes de les installer par la préfecture.

## Les affres du technosolutionnisme

Fausse bonne idée de croire qu'une caméra pourra empêcher un délit de se commettre sous son objectif, mais cela permet aux enquêteurs et enquêtrices d'obtenir des informations. Mais l'utilisation la plus connue reste de permettre la détection très rapide, voire en temps réel, de faits commis répréhensibles. Cela nécessite la surveillance par des équipes dédiées au visionnage et au lancement d'alertes aux équipes qui pourraient ainsi intervenir sur place rapidement. Bien entendu cela demande des moyens humains considérables pour visionner des heures durant des coins de rue, ou des forêts dans le cadre de la lutte contre les incendies. Si la confiance placée dans les hommes et les femmes dans leur capacité de détection et de décision d'envoyer sur place des équipes d'intervention ne peut jamais être totale (fatigue, malveillance, etc.), leur responsabilité ou celle de leur hiérarchie en cas de non-intervention est clairement engagée.

## Surveillance automatisée, dit vidéo-surveillance algorithmique

Avec l'augmentation des capacités de calculs, l'idée d'automatiser la surveillance des images reçues s'est rapidement imposée et a été présentée comme à la fois une solution aux ressources humaines nécessaires et une diminution du risque de manquer des événements importants, mais cela pose au moins deux autres problèmes non moins importants que nous évoquerons ici, dans le cadre particulier de la « surveillance » de population. En effet la surveillance automatisée contre des risques, tel qu'un incendie, ne pose pas les mêmes questionnements.

## Les biais du modèle

Le premier problème est lié à la nature même du fonctionnement de la vidéo-surveillance algorithmique et aux algorithmes eux-mêmes. Ces « algorithmes » bien souvent liés à ce qui est communément appelé « Intelligence Artificielle »



(IA) sont créés à partir de nombreux paramètres et bases de connaissances. Le nombre de paramètres peut facilement dépasser les millions, voire les milliards dans certains modèles, aussi il est quasiment impossible pour un esprit humain de les appréhender tous et de déterminer avec certitude l'impact qu'un paramètre aura sur un autre. Le résultat final semble répondre aux attentes de l'institution qui déploie ce système. Cependant, cela masque un biais majeur : le modèle utilisé pour créer l'algorithme repose sur des critères validés, mais il peut facilement favoriser une action répréhensible commise par une personne contre une autre, si cette dernière passe inaperçue. En revanche, une autre action pourrait être mise en évidence et provoquer la réaction souhaitée. Tout cela se fait sans qu'un humain puisse expliquer pourquoi une action a été priorisée par rapport à une autre. De là à imaginer que la couleur de peau, le style vestimentaire, l'entourage et autres informations créées de facto une discrimination à l'origine de la détection... il n'y a qu'un pas que nous n'hésitons pas à franchir. En effet, les exemples de recherches de délits sur critères sociaux ou de géographie sont déjà légions et émaillées de scandales. Elles ont pour origine l'idée initiale que certaines populations seraient plus enclines à générer des nuisances.

Ce n'est que le début, car derrière ce biais se dessine celui de la Justice. En effet, si les choix de « dénonciation » sont effectués par une machine, par un algorithme, les populations ciblées par les biais de construction du modèle seront les seules à devoir répondre de leurs actes, tandis que celles omises par ce même biais ne seront pas inquiétées.

## **Présomption de culpabilité**

Imaginons un modèle dénué de tout biais : un autre problème se pose.

Notre société est basée sur le contrat social de « pas vu, pas pris ». Ce contrat offre la liberté à chacun et chacune d'agir avec pour seules contraintes le respect de la Loi et la crainte de la Justice. Une société de surveillance massive telle que le promet

la vidéosurveillance algorithmique place tous les éléments de la population au rang de suspect. Nous entrons alors dans une société de surveillance bien pire que les régimes les plus autoritaires, qu'ils soient fictifs ou réels. Les détracteurs de ces régimes ont raison de les dénoncer, mais nous ne devons pas nous laisser leurrer par cette seule dénonciation et ne pas combattre l'autoritarisme qu'ils imposent.

Enfin si la vidéosurveillance algorithmique promet de dépasser le besoin humain de vérification et de prise de décision sur l'attitude à adopter, avec les risques humains que cela entraîne, c'est bien toute la chaîne de valeur de protection des populations qui est anéantie, au profit des seuls intérêts du capital.

## **Vers une utilisation responsable de la vidéosurveillance**

Pour toutes ces raisons, et bien d'autres encore, et parce que ce n'est pas la technologie qui est mauvaise, mais l'utilisation que les capitalistes en font, que nous devons de toutes nos forces lutter contre la prolifération de la vidéosurveillance à des fins de contrôle des populations. Nous pouvons en revanche la promouvoir à des fins d'aide à la création de valeur comme la surveillance d'incendie, ou la recherche astronomique.

En savoir plus :

« Vidéosurveillance algorithmique, dangers et contre-attaque » article de La Quadrature du Net :

<https://www.laquadrature.net/toutsurlavsa/>

« Technocarte, cartographie des projets sécuritaires » réalisée par Technopolice :

<https://technopolice.fr/villes/>

Livre « Technopolice, la surveillance policière à l'ère de l'intelligence artificielle » de Félix Tréguer, chercheur associé au CNRS et membre de La Quadrature du Net, publié aux éditions Divergences (octobre 2024).