L’intelligence artificielle au sein de la vidéo surveillance

Sommaire :

L’intelligence artificielle permet de trier le flux d’informations collectées par les caméras de vidéosurveillance, voire de détecter automatiquement des comportements suspects. Il reste toutefois des limites techniques et réglementaires à son usage.

Pas plus qu’un autre, le secteur de la sécurité électronique n’est épargné par la transformation numérique. Les installateurs de système de contrôle d’accès, de vidéosurveillance ou d’alarme-intrusion ont tout d’abord connu le passage du filaire au tout IP. Ce qui a ouvert la voie à la télémaintenance. S’interfaçant avec la centrale des entreprises qu’ils protègent, ces professionnels peuvent détecter à distance d’éventuels dysfonctionnements de leurs équipements.

Plus récemment, le recours au drone civil permet de survoler des sites sensibles et assurer la protection de zones difficilement accessibles à l’homme. Mais la vague technologique qui suit devrait être plus disruptive encore puisqu’elle concerne les innovations portées par l’intelligence artificielle, notamment en matière de reconnaissance des formes et de visages.

Que se passerait-il si les systèmes de vidéosurveillances devenaient autonomes ?

Aujourd’hui, **les caméras de vidéoprotection déployées dans l’espace public ne permettent de constater qu’a posteriori un problème**, puisqu’il est impossible de placer un être humain derrière chacune d’elles.

Dopé à l’IA, le système pourrait demain trier les flux d’informations, l’opérateur portant son attention que sur les images qui requièrent son intervention. A terme, on peut imaginer un dispositif entièrement autonome capable de lancer automatiquement l’alerte et prévenir les forces de l’ordre après avoir détecté une agression ou une intrusion.

Les avancées en machine learning* et deep learning*, l’explosion du volume de données

– selon IDC, la quantité de données produites par les solutions de surveillance devrait progresser de 25 % par an d'ici à 2021 – et l'avènement de solutions de vidéosurveillance de haute résolution (4K), en mesure d'afficher une grande richesse de détails, laissent augurer des progrès notables dans les prochaines années.

« L'objectif est d'arriver à l'information la plus fiable et opérationnelle possible pour éviter les déclenchements d'alertes intempestifs, plaide Olivier Pradel, directeur corporate du groupe Anaveo (premier fabricant français de système de vidéosurveillance. Il est déjà possible d'identifier un véhicule à sa plaque d'immatriculation mais aussi à son type, une Clio rouge, par exemple. »

La détection comportementale encore perfectible

En revanche, les systèmes actuels de détection comportementale – repérer une personne armée d'un couteau ou en phase de commettre une infraction – montrent leurs limites. « Ils ne sont pas encore suffisamment fiables et ceux qui fonctionnent ne permettent pas en particulier ces détections-là, notamment en voie publique », note Elisabeth Sellos-Cartel, adjointe au délégué aux coopérations de sécurité chargée de la sécurité au ministère de l'Intérieur.

Selon elle, « les algorithmes sont plus pertinents quand il s'agit de détecter un objet resté anormalement longtemps à un endroit, la chute brusque d'un individu ou le maraudage. Dans un environnement humain dense, ils donnent toutefois lieu à beaucoup de fausses alertes. L'automatisation n'est donc pas encore intégralement possible et ces dispositifs nécessitent l'analyse d'un opérateur humain. »

La reconnaissance faciale, efficace… en Chine

Quant à la reconnaissance faciale, elle marche techniquement. La Chine l'a d'ailleurs généralisée. Deux méthodes sont possibles. La première consiste à comparer un flux d'images avec une base de données que l'on aura achetée ou constituée. Par exemple, les visages des salariés autorisés à circuler dans un espace vidéoprotégé. L'autre procédé consiste à donner une signature à une image. A un endroit précis, un individu portait des lunettes et des vêtements de telles couleurs et le système va ressortir toutes les personnes correspondantes.

« Nous ne sommes toutefois pas en Chine, tempère Elisabeth Sellos-Cartel. Ni le gouvernement à ma connaissance ni la société française ne souhaitent aller vers cette surveillance généralisée avec le risque que nos faits et gestes du quotidien soient interprétés à loisir au gré des recherches. »

Une technologie potentiellement liberticide

Avocate, directrice du département Sécurité numérique au sein du cabinet Lexing Alain Bensoussan Avocats, Polyanna Bigle abonde dans son sens. « En analysant un grand volume de données et en automatisant leur traitement, les dispositifs d'IA risquent d'être plus intrusifs et d'attenter à la liberté d'aller et venir, un droit fondamental de la personne. »

« Le principe de sécurité a toujours été opposé à la liberté, ce n'est pas nouveau, rappelle-t-elle. Un système de reconnaissance faciale fondé sur l'IA sera toutefois nettement plus performant que l'œil humain. Même si les personnes sont informées et consentantes, le risque est grand d'un risque d'atteinte à nos libertés individuelles. »

Les fabricants qui introduiront des algorithmes auto-apprenants (machine learning, deep learning) devront intégrer la protection des données personnelles dès la conception pour se conformer au RGPD mais aussi pour éviter tout risque de piratage.

De l'éthique des algorithmes et des codeurs

Tout ceci ne sera pas non plus sans incidence au plan contractuel pour les sous-traitants. « Un fabricant pourrait voir sa responsabilité engagée s'il n'a pas correctement conçu l'algorithme ou mis en place les garde-fous nécessaires, avance Polyanna Bigle. Il en va de même pour un installateur qui n'aurait pas utilement conseillé un client sur l'utilisation d'une base de données. »

Par ailleurs, que se passera-t-il en cas de dysfonctionnement du système, d'erreurs dans la reconnaissance automatique ?, questionne-t-elle. « Une personne pourrait être arrêtée par erreur ou, inversement, le système pourrait ne pas détecter une personne fichée. Le prestataire de services en charge de la vidéoprotection pourrait alors se retourner contre le fabricant et, ce dernier, contre le concepteur même du module d'IA. »

Pour notre juriste, le danger de l'IA réside dans le fait qu'elle est créée par l'homme, mais développe ensuite sa propre intelligence en apprenant par elle-même. Cela pose la question de l'éthique des algorithmes et des codeurs. « Un débat qui montre tout l'intérêt de conserver un œil humain, au propre comme figuré ». L'opérateur de vidéoprotection validera ou invalidera les choix proposés par la machine, gardant ainsi le dernier mot.

Des projets d'IA très encadrés en France

Si d'autres pays s'ouvrent à l'IA comme l'Espagne où la Guarda civil l'utilise pour reconnaître automatiquement les pickpockets dans les gares, ce type de projet est particulièrement encadré en France.

Une entreprise fermée au public qui souhaiterait organiser le suivi d'un individu en croisant une base images et fichier de captation doit, depuis le RGPD, réaliser une étude d'impacts. Elle doit

ensuite demander l'avis de la Cnil, en explicitant les finalités du traitement, les moyens mis en œuvre pour garantir l'intégrité et la confidentialité de données.

« La Cnil rendrait certainement un avis défavorable, estime Elisabeth Sellos-Cartel. La Commission a déjà rendu des avis favorables mais pas à des finalités de surveillance. Elle a validé le projet d'un groupe bancaire qui a mis en place la reconnaissance faciale pour sécuriser l'accès au compte de ses clients. Le bénéfice utilisateur est, là, évident. »

Le Code de la sécurité intérieure pour les lieux ouverts au public

Dans les lieux ouverts au public comme un commerce, un centre commercial, c'est le Code de la sécurité intérieure qui s'applique. La mise en fonctionnement d'un dispositif de vidéoprotection est soumise à une autorisation préalable délivrée par le préfet.

« En ce qui concerne l'analyse comportementale (cris, chutes, objets abandonnés…), l'autorisation préalable suffit dès lors qu'il s'agit uniquement d'alerter sur une situation alarmante, détaille Elisabeth Sellos-Cartel. En revanche si dans de tels lieux il s'agissait d'identifier directement une personne en particulier, il conviendrait également de déposer un dossier à la Cnil. »

deep-learning : ***Le Deep Learning, ou apprentissage profond, est l'une des principales technologies de Machine Learning et d'intelligence artificielle. Découvrez en quoi consiste cette technologie, son fonctionnement, et ses différents secteurs d'application.***

https://www.lebigdata.fr/deep-learning-definition

Machine learning : **Le Machine Learning est une technologie d'intelligence artificielle permettant aux ordinateurs d'apprendre sans avoir été programmés explicitement à cet effet. Pour apprendre et se développer, les ordinateurs ont toutefois besoin de données à analyser et sur lesquelles s'entraîner. De fait, le Big Data est l'essence du Machine Learning, et c'est la technologie qui permet d'exploiter pleinement le potentiel du Big Data. Découvrez pourquoi cette technique et le Big Data sont interdépendants.**

https://www.lebigdata.fr/machine-learning-et-big-data