Vidéo-surveillance : Où vont nos données ?

Yoann Nabat

Vidéo-surveillance : où vont nos données ?

Yoann Nabat

Remise au-devant de l'actualité récente sous la forme d'une injonction au maire de Lyon, la vidéosurveillance sur la voie publique ne s'est jamais aussi bien portée. Pour autant, quel est son encadrement juridique en France et quels en sont ses usages réels ?

Juridiquement, la possibilité d'installer des caméras de surveillance sur la voie publique (qu'il s'agisse de rues ou de routes voire autoroutes) ou dans les lieux publics (transports en commun, bâtiments administratifs, etc.) relève de la compétence des autorités publiques. La décision peut donc être prise par un maire, le président d'une communauté de communes, le directeur d'une prison ou le responsable d'un service de transports par exemple.

Un cadre juridique restreint

Si la caméra filme la rue, l'installation du système est subordonnée à une autorisation du préfet (valable cinq ans), et nécessite un avis de la « commission départementale de vidéoprotection », présidée par un magistrat. En cas d'urgence liée par exemple à un projet terroriste, cet avis peut être repoussé temporairement.

La mise en place de la vidéo-surveillance doit répondre de finalités prévues par la loi. Celles-ci sont néanmoins, comme souvent en la matière, rédigées de manière particulièrement large : « protection des bâtiments et installations publics », « prévention des atteintes à la sécurité », etc.

Depuis 2011, les acteurs privés comme les commerçants peuvent également mettre en place de tels caméras aux abords immédiats de leur établissement, après autorisation du maire.

Dans tous les cas, une limite importante se trouve dans l'interdiction formelle de filmer, même accidentellement, des lieux d'habitation. Les caméras doivent être orientées de telle manière à ne pas viser de maisons ou d'immeubles, ou, à défaut, équipées de système de floutage des façades.

La Loi Informatique et Libertés, également d'application pour ces dispositifs lorsqu'ils permettent la collecte et l'enregistrement de données identifiantes, c'est-à-dire permettant de reconnaître des individus dans la rue ou dans les commerces, impose également un processus particulier, nécessitant parfois l'autorisation de la CNIL.

Les établissements privés ouverts aux publics (bars, restaurants, etc.) peuvent également mettre en place ces dispositifs à l'intérieur de leurs locaux mais selon des modalités plus rigoureuses.

Enfin, en dehors de ces règles et même si ce n'est pas prévu par la loi, la Cour de cassation autorise la mise en place de vidéo-surveillance spéciale et ponctuelle pour les besoins d'une enquête judiciaire.

Le développement d'une vidéo-surveillance parallèle

Ces systèmes classiques de vidéo-surveillance par caméras installées se doublent aujourd'hui de nouveaux dispositifs qui ne répondent pas de cet encadrement juridique classique. Il s'agit d'une part de l'usage des drones, et d'autre part des caméras individuelles utilisées par les forces de l'ordre.

L'utilisation des drones comme dispositif de vidéo-surveillance par les forces de l'ordre fait l'objet d'une véritable saga juridique débutée notamment lors du confinement, passant par plusieurs interdictions données par le Conseil d'État, une intégration dans la loi Sécurité globale et enfin une censure par le Conseil constitutionnel.

Si le gouvernement tient autant à autoriser le recours à ces dispositifs, c'est qu'ils permettent, désormais équipés de caméras de très haute résolution, une couverture virtuellement illimitée en vidéo-surveillance de tout le territoire. Leur usage, très périlleux pour les libertés fondamentales, doit néanmoins encore trouver un équilibre juridique.

En parallèle, se généralise également le déploiement de « caméras-piétons » qui équipent les forces de l'ordre et même les agents assermentés de sociétés de transport, autorisant l'enregistrement des images et du son de certaines interventions ou contrôles.

Un devenir incertain des données

Que deviennent toutes les images ainsi collectées, qu'il s'agisse des outils classiques de vidéo-surveillance sur la voie publique ou de celles des nouveaux dispositifs de captation vidéo ?

La première catégorie d'images est traitée par le service qui a demandé l'installation des caméras, qu'il s'agisse d'une municipalité ou d'une autre structure publique. Cela doit être prévu explicitement, ainsi que la durée de conservation des images qui ne peut excéder un mois.

Les vidéos collectées par les caméras individuelles des forces de l'ordre sont quant à elles transmises aux services de police ou de gendarmerie et conservées six mois.

Durant leur temps de conservation, l'ensemble de ces données peut faire l'objet de réquisitions, c'est-à-dire de demandes par les services de police ou de gendarmerie dans le cadre d'une enquête ou d'une instruction. Dans ce cas, plus de durée maximum car les vidéos intègrent le dossier pénal.

Depuis l'adoption de la loi Sécurité globale, les images captées par les caméras individuelles des forces de l'ordre peuvent également, en parallèle de leur enregistrement, être transmises en flux direct au centre de commandement.

Une exploitation limitée

Comment assurer le traitement efficace de ces milliers d'heures d'enregistrement ? Si certaines villes décident de s'équiper de centres de traitement voyant se relayer un personnel 24h/24, la difficulté est bien réelle. Ce n'est pas tout d'avoir des caméras, encore faut-il avoir des humains derrière les écrans.

Cette problématique est-elle en passe de se voir résolue par les nouveaux usages de la vidéosurveillance, fondés sur les outils algorithmiques, la reconnaissance faciale voire l'intelligence artificielle ?

Le recours à de tels outils a en tout cas de quoi séduire les décideurs publics, et ce à l'ère des « smart cities » ou « villes intelligentes ». Pourtant, ils constituent bien davantage une forme nouvelle de « techno-police » et posent de vrais problèmes sur nos libertés fondamentales.

De nouveaux usages problématiques

Que penser en effet de la possibilité laissée aux policiers et aux gendarmes d'utiliser leurs outils de reconnaissance faciale (prévus notamment dans le cadre du principal fichier de police) sur les images obtenues par les caméras embarquées ?

Rien n'interdira ainsi que demain, lors d'une manifestation, les nombreux policiers présents, tous équipés de telles caméras (qui ont vocation à être généralisées) reçoivent dans leurs oreillettes, en direct, l'identité et les informations relatives aux personnes qui se trouvent en face d'eux, leur signalant tel ou tel individu déjà connu. Cette pratique se réaliserait en dehors du cadre juridique relativement contraint des contrôles d'identité.

De même, les expérimentations de recours à la reconnaissance faciale par les caméras de vidéosurveillance classiques se multiplient, même si la CNIL reste encore, heureusement, très vigilante et si l'interdiction reste le principe. La question de son utilisation lors des prochains Jeux olympiques de Paris a d'ailleurs été évoquée, même si elle semble aujourd'hui écartée.

La reconnaissance faciale n'est pas la seule technologique pouvant se nourrir des images de vidéosurveillance. L'utilisation de techniques de reconnaissance automatique de plaque (LAPI) permettant la vidéo-verbalisation de nombreuses infractions et l'identification immédiate de véhicules est désormais possible dans notre droit et tend, là aussi, à se généraliser.

Enfin, le recours à des formes d'intelligence artificielle, de « police prédictive », peut également contribuer à l'exploitation de ces données, au moins, pour le moment, en suggérant aux forces de l'ordre où regarder parmi le flux d'images.

Nombreux risques et faible efficacité

Pourtant, ces outils constituent des risques très importants pour nos libertés individuelles, au premier rang desquels figure la liberté d'aller et venir. Demain, en effet, la généralisation des caméras couplées à la reconnaissance faciale et à la lecture automatique des plaques pourra permettre, au moins virtuellement, la géolocalisation de tout individu sur le territoire. Or, l'exercice plein de cette liberté nécessite une forme

d'anonymat : je n'irais en effet sans doute pas aussi librement rencontrer une personne ou me rendre à une réunion politique si je sais que mon déplacement peut être enregistré.

Tous les outils techniques sont déjà en place pour cela, même si l'encadrement juridique y fait encore, heureusement, en partie barrage. Le fichier des cartes d'identité et des passeports contient ainsi une photographie de chacun d'entre nous, mais n'est pas accessible aux forces de l'ordre et n'autorise pas la reconnaissance faciale. Un simple texte réglementaire pourrait néanmoins modifier ce point, même si ce n'est, pour le moment, pas à l'ordre du jour.

D'une solution miracle, la vidéo-surveillance, semble constituer l'illustration d'une technologisation des formes de contrôle et de surveillance, à l'efficacité douteuse, mais aux dangers réels. Stocksnap/ pixabay, CC BY-NC-ND

Ces transformations sont d'autant plus préoccupantes que l'efficacité réelle de la vidéo-surveillance sur la délinquance et la criminalité n'a jamais été démontrée. Une longue étude récente menée notamment par Laurent Muchielli en atteste :

> « Les résultats soulignent la grande faiblesse de la contribution de la vidéosurveillance à la lutte contre la criminalité. »

Au mieux, elle ne fait que déplacer la délinquance d'un quartier à un autre.

L'efficacité sur la résolution des enquêtes est également difficile à évaluer, mais semble marginale, comme le pointait l'année dernière la Cour des comptes qui en dénonçait le prix exorbitant pour un résultat très limité. Cela est notamment dû à la quantité d'images et aux faiblesses structurelles des outils (dont certains subissent même des biais racistes).

D'une solution miracle, la vidéo-surveillance, renommée habilement depuis quelques années déjà vidéo-protection, semble ainsi constituer l'illustration d'une technologisation des formes de contrôle et de surveillance, à l'efficacité douteuse, mais aux dangers réels.

Elle incarne ce « paradigme du techno-solutionnisme », plus empreint de considérations politiques et industrielles que de souci véritable du bien commun.