Corentin Debailleul, chercheur en géographie urbaine (IGEAT-ULB)

Vidéosurveillance à Bruxelles : installer des caméras, mais pourquoi ?

Dans les rues de Bruxelles, le réseau de caméras de surveillance s'est considérablement élargi ces dernières années. Lutte contre l'insécurité et le terrorisme ou contre les dépôts clandestins, régulation du trafic routier, zone de basses émissions, cet outil de surveillance apparaît souvent comme la solution-miracle aux problèmes qui se posent aux autorités. Dans cet article, nous allons tenter de comprendre à quoi servent ces images capturées par les caméras de surveillance, comment elles sont utilisées et remplissent leurs promesses.[1]

Comment la vidéosurveillance s'est-elle développée ?

Connaître le nombre de caméras publiques est plus compliqué qu'il n'y paraît, tant les autorités qui installent ces yeux électroniques sont diverses : zones de police, communes, administrations bruxelloises, etc. La volonté de transparence sur cette question est aussi très aléatoire, comme l'expérimente actuellement la Ligue des droits humains dans le cadre de sa campagne de demandes d'informations sur les dispositifs de surveillance.[2] Néanmoins, on estime qu'il existe, en vrac, à Bruxelles : des dizaines de caméras pour la propreté ; environ 500 caméras dédiées à la circulation ; 300 pour la zone de basses émissions ; plus de 1000 pour la police locale ; et plusieurs milliers dans les stations et les véhicules de la STIB.

À Bruxelles, ce réseau de caméras de surveillance a grandi par à-coups, tantôt à l'occasion d'évènements sportifs d'envergure, tantôt lors de faits divers ou attentats suscitant un choc émotionnel fort. Si les premières caméras apparaissent dans les années 60 du côté de la STIB, c'est l'Euro de football en 2000 qui va jouer un rôle d'accélérateur. Ensuite, en 2003, la région bruxelloise décide de consacrer un budget d'un million et demi d'euros pour équiper les communes de caméras. Le réseau de caméras de police se développe alors pour quadrupler entre 2006 et 2016.[3]
Au milieu des années 2010, alors que la Région promeut la « smart city » et l'installation de capteurs de toutes sortes, les attentats au métro Maelbeek et à l'aéroport de Zaventem viennent plaider pour l'installation de plus de caméras, à plus haute définition. Plus question de se contenter des images floues d'un mystérieux « homme au chapeau » dont on perd rapidement la trace à sa sortie de l'aéroport. S'ensuit également un plaidoyer pour le déploiement de caméras capables de lire les plaques d'immatriculation, dites ANPR (pour *Automatic Number Plate Recognition*). Le discours anti-terroriste s'hybride alors avec des considérations sanitaires et environnementales : la pollution atmosphérique à Bruxelles cause de graves maladies respiratoires et la circulation automobile est pointée du doigt. La Région décide donc de mettre en place une « zone de basses émissions » qui exclut de son territoire, sous peine d'amendes, les véhicules les plus anciens, en commençant par les diesels.[4] Pour ce faire, des centaines de caméras ANPR sont déployées depuis 2018, capables de comparer les images captées dans la rue avec le registre national des immatriculations.

1 Merci à Aline Wavreille pour l'aide apportée à la rédaction de cet article.
2 https://transparencia.be/user/ligue_des_droits_humains
3 Pauline De Keersmaecker et Corentin Debailleul (2016), « Répartition géographique de la vidéosurveillance dans les lieux publics de la Région de Bruxelles-Capitale », *Brussels Studies*, Numéro 104, 2016.
4 https://lez.brussels

Vers une généralisation ?

Les images vidéo qui sont enregistrées par les caméras qui quadrillent le territoire bruxellois circulent ensuite sur des réseaux de fibre optique, appartenant soit aux zones de police, soit au réseau IRISnet mis en place par la Région en partenariat avec Orange. Via ces réseaux, les images convergent vers deux endroits : la première destination relève du dispatching de chaque zone, où une série de policiers est face à un mur d'écrans et en lien avec les patrouilles de terrain ; la seconde destination est « safe.brussels » organisme responsable du centre de crise régional et de la plateforme de « mutualisation de la vidéoprotection ». Cette plateforme permet aux différents acteurs publics comme la STIB, le Port de Bruxelles ou le Ministère des transports de partager leurs images entre eux mais surtout de donner à la police un accès immédiat à l'ensemble du réseau.

Malgré cette tendance à la régionalisation, d'un point de vue géographique, le déploiement de la vidéosurveillance à Bruxelles est loin d'être uniforme. La majorité des caméras se trouve dans le centre-ville de Bruxelles, en particulier dans les espaces commerciaux et touristiques. Ensuite, plus on s'éloigne de ce centre et moins on dénombre de caméras. Cette diminution se fait néanmoins de manière très inégale : en allant vers les quartiers plus aisés du sud-est (Boitsfort, Auderghem, Woluwé, etc.) on trouve beaucoup moins de caméras que si on se dirige vers le nord-ouest, et notamment vers les quartiers populaires jouxtant le canal comme Cureghem ou Molenbeek, qui sont, eux, particulièrement vidéosurveillés.

Pour quelle efficacité ?

Une caméra conçue pour être placée dans l'espace public et résister aux intempéries comme au vandalisme coûte plusieurs milliers d'euros. À ce montant, il faut généralement ajouter d'autres dépenses, telles que la consultance, l'installation, le fonctionnement et la maintenance. Au total, il faut compter entre 20 000 et 50 000 euros de frais par caméra, sans compter le personnel nécessaire pour visionner ou traiter les images. Dans la mesure où les plans d'installation de caméras publiques comptent souvent plusieurs dizaines voire centaines de caméras, les budgets se comptent en millions d'euros. La vidéosurveillance représente donc un coût très important et pèse lourd sur les finances publiques, notamment locales. Pourtant, les études s'accordent à dire que les caméras sont loin de remplir leurs promesses. Les effets sont généralement considérés comme minimes, voire nuls, à de rares exceptions près.[5] La question dès lors serait de comprendre pourquoi les communes, la Région et zones de police continuent d'investir dans cette technologie ? La réponse est sans doute avant tout politique : notre hypothèse est que faute de pouvoir s'attaquer réellement aux problèmes sociaux, les autorités doivent bien montrer qu'elles agissent pour lutter contre le sentiment d'insécurité…

Des caméras « intelligentes » ?

Pour contrer la critique de l'inefficacité des caméras, les fabricants ont proposé aux autorités publiques des logiciels d'analyse d'images. Une fois enclenchés, ces logiciels vont sélectionner des séquences jugées « problématiques » et envoyer des alarmes en cas de dégagement de fumée, de tag, de dépôts d'immondices, de gens qui courent ou qui errent près d'une voiture, etc. En région bruxelloise, la police utilise un logiciel fourni par la société montoise ACIC pour l'analyse des images en direct. En pratique, ces séquences jugées problématiques par le logiciel sont innombrables sur un territoire aussi large que Bruxelles, la police est alors submergée et dans l'impossibilité d'agir à chaque alarme, d'autant plus que les « faux positifs » sont nombreux. Mais la police utilise un autre type de programme pour faire de l'analyse *a posteriori*, dans le cadre d'enquêtes, par exemple. Le plus souvent, il s'agit du logiciel BriefCam, développé en

5 Élodie Lemaire (2019), *L'œil sécuritaire : mythes et réalités de la vidéosurveillance*, Paris : La Découverte.

Israël. Celui-ci propose un « résumé » de ce qu'une caméra a enregistré durant plusieurs heures. Il permet ensuite de trier les évènements sur base de critères de recherche comme la couleur des vêtements ou le genre d'un·e suspect·e.

Si ce second logiciel semble plus efficace, il n'en soulève pas moins des questions démocratiques. Tous ces programmes sont basés sur des algorithmes dont le code informatique est fermé, c'est-à-dire protégé par la propriété intellectuelle. Il est donc impossible d'en connaître le fonctionnement réel. Une partie du fonctionnement de la police est donc conditionné par les boites de développement informatique, leurs ingénieurs et les possibilités techniques actuelles, sans qu'il soit réellement possible de remettre en question leurs pratiques. De plus, même si le code était disponible et qu'il y avait une volonté d'en débattre, il ne serait pas forcément possible d'en comprendre le fonctionnement dans la mesure où de plus en plus d'algorithmes sont dorénavant produits par *machine learning*, c'est-à-dire en les entrainant sur des séries de données. À la propriété intellectuelle s'ajoute alors l'opacité du procédé, faisant du fonctionnement de tels dispositifs de véritables « boites noires ».[6] Résultat, on se retrouve souvent avec des logiciels qui reproduisent des dominations raciste ou sexiste, sans qu'il soit facilement possible d'en comprendre la source et de remédier au problème.

Dans la mesure où tout dispositif de surveillance a besoin de code pour fonctionner, la question de la sécurité des dispositifs utilisés se pose également. Des inquiétudes existent quant aux caméras chinoises disponibles à bas coût, mais dont il n'est pas certain que les données qu'elles récoltent ne sont pas envoyées vers la Chine. La Sûreté de l'État recommande donc aux pouvoirs publics de ne pas dépendre des géants du numérique chinois pour leurs infrastructures sensibles. Mais comme me le confiait le responsable de l'informatique d'une zone de police bruxelloise : « on a bien conscience que le problème est le même avec la technologie américaine, mais à choisir… »

A QUOI ALLONS-NOUS FAIRE FACE ?

Les dispositifs publics que l'on croise le plus souvent en rue ont une forme de dôme et sont généralement placés à cinq ou six mètres de hauteur, accrochés aux façades ou perchés sur des poteaux. Ces caméras balaient les espaces qu'elles surveillent et suivent généralement une séquence programmée à l'avance. Les agents peuvent en prendre le contrôle et orienter ces caméras, dans le cadre de manifestations par exemple. De plus en plus, les caméras sont disposées de manière à pouvoir capturer le visage des passants. Elles sont placées à hauteur du regard pour prendre des images dans un angle permettant l'identification. Ce changement d'approche est particulièrement visible dans les gares où, comme vous l'aurez peut-être remarqué, il est maintenant impossible d'entrer, de prendre un escalator ou de regarder les horaires sur les panneaux d'affichage sans se retrouver nez-à-nez avec une caméra. La police procède de façon similaire en installant des caméras fixes à haute définition face aux sorties de métro. Cette évolution est particulièrement inquiétante quand on sait que la direction de la SNCB ou le Ministère de l'Intérieur ont déjà communiqué par le passé leur volonté de recourir à des logiciels de reconnaissance faciale ; que cette fonctionnalité est proposée par le logiciel BriefCam ; et que la police fédérale a déjà été prise la main dans le sac à expérimenter la reconnaissance faciale hors de tout cadre légal…

6 Frank Pasquale (2015), *The Black Box Society, les algorithmes secrets qui contrôlent l'économie et l'information*, Fyp éditions.