Mettre en marché les peurs urbaines : le développement des “ safe cities ” numériques

Myrtille Picaud

Myrtille Picaud, « Mettre en marché les peurs urbaines. Le développement des "*safe cities*" numériques », in Claudia Senik (dir.), *Sociétés en danger*, La Découverte, 2021, p. 139-156.

[Version auteure du texte, disponible sur Cairn]

Résumé

À Nice, Marseille, Saint-Étienne ou encore Valenciennes, se développent des projets mobilisant des dispositifs numériques de sécurité, souvent dénommés par les industriels « safe city », dans une relative opacité. Ces dispositifs numériques sont divers et destinés à protéger les espaces urbains : vidéosurveillance dite « intelligente », où des algorithmes d'analyse d'image signalent des mouvements de foule, des violences, intrusions ; plateformes d'hypervision, qui analysent divers fichiers municipaux et nationaux ; big data en ligne afin de prévenir les crimes ; forces de l'ordre connectées, etc.

Jusqu'à présent, ces dispositifs numériques de sécurité ont plutôt été analysés à travers les risques qu'ils poseraient aux libertés publiques, par une surveillance accrue de toute la population. Je propose d'analyser leur développement sous l'angle de la construction d'un marché. À qui profite le crime ? Mes recherches témoignent d'abord de l'investissement d'entreprises, des multinationales comme des start-ups, issues en particulier de la vidéosurveillance traditionnelle, de la défense, mais aussi du numérique. Néanmoins, la construction de ce marché est aussi le fait de représentants des pouvoirs publics, à l'échelle locale, dans les villes qui accueillent ces projets, mais aussi nationale et européenne, en vertu de son potentiel de croissance économique. L'analyse de l'offre des entreprises éclaire le ciblage spatial des dispositifs développés, qui sont plutôt destinés aux centres-villes, centres commerciaux, gares et autres lieux de circulation intense. Cela interroge la division spatiale du travail de contrôle : aux centres le numérique et dans les quartiers populaires la présence policière ? Cette recherche témoigne aussi du fort investissement, symbolique et économique, de dispositifs ciblant les délits de rue – et donc certains groupes sociaux –, à l'exclusion d'autres formes d'illégalismes. Les moyens publics investis dans le contrôle ne visent ni la délinquance financière, ni les dévoiements du recours aux locations meublées touristiques type Airbnb, qui pourtant déstructurent les marchés immobiliers locaux. En définitive, c'est ainsi la transformation de nos vies dans les espaces publics des métropoles contemporaines que cette enquête interroge.

Summary

In French cities such as Nice, Marseille, Saint-Étienne and Valenciennes, digital security projects for cities are being developed, often referred to as "safe cities". The digital devices are diverse and designed to protect urban spaces: so-called "smart" CCTV, where algorithms scan pictures to signal crowd movements, violence, intrusions; "hypervision" platforms, which cross-analyze municipal and national files; online big data to prevent crimes; connected law enforcement, etc.

Until now, these digital security devices have been analyzed through a lens emphasizing the risk they pose to civil liberties, with an increased surveillance of the whole population. I suggest their development can be studied from the angle of the construction of a market. Who benefits from crime control? First of all, my research shows how private firms, multinationals as well as start-ups, invest this market, coming from traditional video surveillance, defense, but also digital services. Nevertheless, the construction of this market is also supported by public authorities, at the local level, in the cities that experiment these projects, but also at the national and European levels, by virtue of this market's economic growth potential. The analysis of the firms' products sheds light on how these devices draw on urban targeting, as they are rather intended for city centers, shopping malls, train stations and other central places of intense traffic. This raises questions about the spatial division of control work: is it digital in the centers compared to the presence of police in working-class neighborhoods, or a mixture of both? This research also shows how these devices strongly target street crime - and therefore certain social groups. This excludes other forms of illegality, since the public resources invested do not target financial crime for instance, nor the development of illegal furnished tourist rentals such as Airbnb, which nonetheless destructure local real estate markets. In the end, it is the transformation of our lives in the public space of contemporary cities that this research examines.

Mettre en marché les peurs urbaines
Le développement des « safe cities » numériques

A Nice, Marseille, Saint-Etienne ou encore Valenciennes, se développent en effet des projets de « safe city », pendant sécuritaire de la « smart city ». L'un des objectifs de l'industrie de la sécurité française est de développer ces « villes sûres », qui désignent des dispositifs numériques destinés à lutter contre les dangers pesant sur l'espace urbain : vidéosurveillance « intelligente », où l'analyse d'image s'appuie sur des algorithmes de détection de mouvements de foule, de violences, d'intrusion ; des plateformes dites d'hypervision, liant analyse de divers fichiers municipaux et nationaux et *big data* en ligne afin de prévenir les crimes ; forces de l'ordre connectées ; etc. Certaines applications sont destinées aux particuliers, comme Flag ! qui propose le signalement à la Police des violences à caractère homophobe. La reconnaissance faciale est quant à elle envisagée pour assurer la sécurité des Jeux Olympiques et paralympiques à venir en 2024 à Paris. L'usage croissant d'instruments numériques dans le secteur de la sécurité urbaine se fait à grande vitesse mais dans une relative opacité.

Ces dispositifs se sont trouvés au cœur de forts débats récemment, notamment autour de « StopCovid », l'application pour téléphone qui permettrait de tracer des cas de Covid-19 dans le but de diminuer la contagion. A aussi été débattu le recours à différents dispositifs de contrôle pendant le confinement, tels que des drones par la police à Paris. Leur utilisation a finalement été suspendue le 18 mai 2020 par le Conseil d'Etat, suite à un recours de la Ligue des droits de l'homme et la Quadrature du Net. Celles-ci, avec d'autres associations, avaient lancé la campagne Technopolice, destinée à lutter contre l'expansion de projets de sécurité numérique pour l'espace urbain. Leur développement s'est en effet accéléré après les attentats ayant eu lieu notamment à Saint-Denis, Paris et Nice.

Les grandes métropoles sont aujourd'hui présentées comme les « gagnantes » de la mondialisation et les lieux du renouveau économique de l'économie des plateformes numériques, à l'instar d'Airbnb ou de Uber. En parallèle, elles sont aussi ciblées de façon croissante par des politiques de sécurité. La sécurité des villes n'est toutefois pas un sujet nouveau. Dans ses écrits sur la ville, Max Weber (2014) voyait déjà la garnison militaire comme contribuant au développement du marché dans les villes. Michel Foucault (2004) a approfondi l'étude du rôle de la sécurité dans le développement économique, en analysant les dispositifs de sécurité comme une forme de rationalité politique, liant gestion des populations, territoires et libéralisme.

Les villes ont longtemps été considérées à travers le prisme de l'insécurité, comme lieux de désorganisation sociale, par les premières recherches urbaines de l'École de Chicago notamment (Park, Burgess et McKenzie, 1925). Cette représentation nourrit également les discours politiques et médiatiques sur l'incivilité et les violences urbaines en France. Différentes politiques, aux finalités sécuritaires et sociales, comme la politique de la ville, ont été mises en œuvre afin de lutter contre ces phénomènes. Dans de nombreuses métropoles, cela a favorisé le recours à la vidéosurveillance, qui a ouvert la voie au développement contemporain des « safe cities », présentées comme des remèdes aux failles de la vidéosurveillance. Par

exemple, dans la vidéosurveillance dite « intelligente », les opérateurs derrière les caméras seraient aidés par l'analyse algorithmique des images, ce qui permettrait d'envoyer une alerte lorsque sont repérés certains comportements (violences, déplacements de foules, etc.).

L'explosion des capacités de calcul et des données produites (Cukier et Mayer-Schönberger, 2014), grâce notamment aux téléphones et capteurs connectés, offre de nouvelles possibilités pour ces formes de sécurité urbaine. Cela est particulièrement le cas dans un « âge actuarial » (Harcourt, 2005), où les données sur les comportements sont utilisées pour cibler des groupes sociaux ou des espaces perçus comme étant « à risque » (Amoore, 2013). Néanmoins, les recherches sur la vidéosurveillance témoignent d'usages très différenciés et souvent loin des promesses initiales (Lemaire, 2019). Cela appelle à la prudence quant à la croyance en l'efficacité de dispositifs numériques de sécurité pour l'espace urbain, surtout au regard des risques qu'ils posent quant au respect des libertés publiques.

Mais que se passe-t-il, lorsque les « menaces » et le « danger » deviennent un marché ? Qui sont les acteurs de cette montée en puissance des « safe cities » ?

Les « territoires de confiance » au cœur de la politique industrielle de sécurité

L'expansion des expérimentations de dispositifs numériques pour les villes fait l'objet de nombreux discours médiatiques. Néanmoins, peu de recherches se penchent sur leur développement dans le cadre d'un marché de la sécurité urbaine. La mise en marché de la sécurité, un domaine régalien, a pu être interprétée comme une « privatisation » ou un retrait de l'État. Les recherches actuelles sur la sécurité mettent plutôt en avant la multilatéralisation[1] du travail de police, afin de désigner la multiplication des agents, publics et privés, qui le prennent en charge.

Le développement de projets de « safe cities » peut ainsi se comprendre comme la construction d'un marché (numérique) de la sécurité urbaine. Celle-ci s'opère dans un contexte de transformation du marché de la sécurité, qui joue un rôle croissant, avec l'appel par l'Etat à un « continuum de sécurité (Malochet et Ocqueteau, 2020) « entre services de police et de gendarmerie, élus locaux, police municipale, entreprises, mais aussi citoyens », selon l'ancien ministre de l'Intérieur Christophe Castaner[2]. L'Union Européenne soutient également ce marché de la sécurité, auquel au moins 11 milliards d'euros ont été dédiés entre 2014 and 2020, avec un focus important sur le développement de nouvelles technologies. En 2016, le marché global de la sécurité privée en France représentait un chiffre d'affaires de 34 milliards d'euros (1,5% du PIB) et 285 000 personnes employées[3]. En Europe, il était de 170 milliards d'euros (2,8 millions d'employés) et de 688 milliards d'euros dans le monde. La construction du marché de la sécurité numérique pour l'espace urbain doit se comprendre à l'aune des

[1] Ce terme désigne un double mouvement « de diversification des acteurs en charge des missions de police (au-delà des polices publiques étatisées), mais aussi d'un brouillage accru entre *policing* (au sens de distribution de la sécurité par l'utilisation potentielle de la contrainte), médiation et prévention » (de Maillard et al., 2015, p. 295).
[2] https://www.aefinfo.fr/depeche/597901
[3] La définition du périmètre du marché de la sécurité fait l'objet de discussions et peut donner lieu à la variation des chiffres cités. Nous reprenons ici les communications de l'Observatoire de la filière industrielle de sécurité (Decision Etudes & Conseil, 2018).

transformations du marché de la sécurité français, avec la concurrence d'entreprises étrangères. En effet, l'Observatoire de la filière industrielle de sécurité observe une baisse de la croissance annuelle moyenne du marché de la sécurité privée depuis 2013, en raison de la présence de plus en plus prégnante d'entreprises étrangères, notamment chinoises et nord-américaines.

A l'échelle nationale, la politique industrielle de sécurité s'est donné pour objectif l'essor des « territoires de confiance », avec le renforcement de la filière industrielle française par rapport à ses concurrents étrangers. En 2020, le ministre de l'Intérieur Christophe Castaner participe à la signature du contrat de filière 2020-2022 du Comité stratégique de filière (CSF) Industries de sécurité. Il sera présidé par Marc Darmon, Président du Conseil des industries de la confiance et de la sécurité (CICS) et Directeur général adjoint de Thales, groupe français du secteur de l'aéronautique, sécurité, défense et biométrie. Le CSF entend positionner l'industrie française comme leader mondial de la sécurité de la ville intelligente, « la sécurité des villes et des territoires intelligents, s'inscri[van]t comme un élément essentiel à maîtriser pour garantir la tranquillité, la résilience et l'attractivité des territoires. » (CNI, 2020, p. 37).

L'évolution législative est également au centre du « déploiement de territoires intelligents et sûrs », ce marché étant présenté comme faisant face à de nombreux freins et manquant d'ambition. Le développement des projets de « safe cities » est en effet encadré par le droit, à l'échelle nationale et européenne, notamment en ce qui concerne la protection des données. La concurrence d'entreprises étrangères est souvent associée aux possibilités d'expérimentation qu'elles auraient dans leurs pays, qui seraient interdites en France en raison des lois de protection des données et des libertés individuelles. La Chine est un exemple récurrent dans les discours de représentants d'entreprises françaises, afin d'insister sur la nécessité de l'évolution du cadre légal, dans l'objectif d'une plus grande compétitivité des entreprises françaises. La comparaison chinoise permet également de dédramatiser l'usage de la sécurité numérique (par exemple de la reconnaissance faciale) et de miner la critique politique sur les risques associés, en faisant valoir l'enjeu du développement économique national.

Le marché des « safe cities » est ainsi présenté comme une opportunité de croissance pour les entreprises françaises en perte de vitesse face à une concurrence étrangère croissante. Ce marché offre aussi une occasion de repositionnement à des entreprises du secteur de la sécurité, qui disposaient initialement de dispositifs moins adaptables aux demandes variées des collectivités et à l'intégration de systèmes de sécurité déjà installés :

> « Je pense que c'est une rencontre de technique, une offre qui n'était pas, on va pas dire 'pas mature', mais qui n'était pas adaptée au changement rapide. Cette offre digitale nous a ouvert l'appétit sur le fait de dire "on peut adresser". Mais on s'est d'abord dit, indépendamment du marché français, notre façon de faire, avec des gros systèmes, pas digitaux, qui étaient parti pour faire un développement en mode tunnel, […] maintenant on fait des aller-retour, on est vachement plus digital. […] Le marché maintenant il est disrupté par… Si c'est pas nous qui le faisons – on est aussi attaqué par des gens qui proposent des offres digitales en mode service et en mode *cloud*. Y'a aussi, on s'est rendu compte que nos concurrents – enfin certains concurrents, pas nos vieux concurrents, qui sont comme nous – mais on a vu rentrer une nouvelle compétition… […] Des concurrents chinois sur la sécurité, des concurrents américains. Après c'est des zones d'influence. Et en France on va avoir des acteurs locaux qui sont très forts dans certaines villes. » *(Directeur de branche « collectivités territoriales », entreprise dans le secteur de la sécurité, entretien à Paris le 22.10.2019)*

La construction du marché des dispositifs numériques pour la sécurité se situe donc à la croisée des transformations du marché de la sécurité français et du développement de dispositifs numériques pour l'espace urbain. Celui-ci, parfois désigné par le terme « smart city », a d'abord été initié par des firmes des NTIC nord-américaines, avant d'être investi par un ensemble d'entreprises de différents secteurs. Ce développement a conduit de grands groupes à s'intéresser à des contrats liés aux collectivités territoriales, en pariant sur leur multiplication et sur des économies d'échelle s'ils parvenaient à remporter de nombreux marchés. Il contraint aussi des entreprises, plutôt issues du secteur de la vidéosurveillance traditionnelle, ou de la sécurité et défense, à investir dans la production de dispositifs liés aux technologies numériques, mais aussi à transformer leur fonctionnement en interne. La sécurité peut être conçue davantage comme un service, il ne s'agit plus de simplement installer une plateforme ou un système de vidéosurveillance, mais d'accompagner son utilisation, son évolution, etc. En 2016, les entreprises du secteur de la sécurité (marchande) consacraient ainsi 1,7 milliards d'euros en recherche et développement, quand un groupe comme Thales y dédie 1 milliards d'euros en 2019 et a créé.

Les grands événements, centraux dans le développement de dispositifs de sécurité

Afin d'accélérer le développement de projets de « safe cities », la politique industrielle de sécurité s'appuie sur différents projets et événements perçus comme fédérateurs et favorisant le développement de technologies et de leurs usages. C'est notamment le cas des Jeux Olympiques et Paralympiques (JOP) prévus à Paris en 2024, qui apparaissent dans le contrat de filière 2020-2022 du Comité stratégique de filière (CSF) Industries de sécurité comme premier projet structurant. Un tel événement est présenté comme nécessitant une sécurité exceptionnelle, en raison des risques associés et de sa résonnance médiatique internationale. Les JOP, comme les grands événements sportifs, offrent depuis longtemps une vitrine permettant de démontrer le savoir-faire national en matière de sécurité et d'obtenir par la suite des contrats dans d'autres pays (Bennett et Haggerty, 2011).

Des rencontres et tables rondes réunissant représentants de groupes d'intérêt, d'entreprises de sécurité et des pouvoirs publics abordent ainsi les enjeux sécuritaires liés aux grands événements, tels que la coordination entre acteurs publics et privés, le développement de nouvelles technologies de sécurité, l'encadrement légal de leur utilisation, la place des entreprises françaises dans l'obtention des marchés, etc. Ces événements rassemblent tant les organisateurs des JOP, de la Coupe du Monde de Rugby, que des cadres du ministère de l'Intérieur, préfets, députés et cadres de grandes entreprises de sécurité et biométrie. Ils témoignent de la mobilisation des représentants des pouvoirs publics et des élus, afin de favoriser l'évolution du cadre législatif s'appliquant à des dispositifs de sécurité. En outre, les JOP justifieraient le recours à des dispositifs de sécurité exceptionnels, parfois présentés comme transitoires, à l'instar de la reconnaissance faciale dans l'espace public. Ces dispositifs, très contestée par les associations de défense des libertés publiques, sont envisagés afin de faciliter la gestion de flux et d'autorisations d'accès à différents espaces, par exemple dans le Village Olympique qui sera situé à Saint-Denis :

> « Se pose aussi la question de l'accès au Village olympique et de savoir ce que les technologies apportent en termes de garanties supplémentaires. Par exemple la vidéo-protection associée à la reconnaissance faciale ou la détection d'événements anormaux. Mais on doit arriver à lever les freins juridiques qui freinent les expérimentations en situation réelle. […] Donc on doit bien peser le pour et le contre, mais on doit pas perdre de temps et trouver le vecteur législatif dans les 18 mois qui viennent pour pouvoir tester en situation réelle des choses comme la reconnaissance faciale. » (*Pascal Bolot, directeur de la protection et de la sécurité de l'Etat (DPSE) au secrétariat général de la défense et de la sécurité nationale (SGDSN), service du Premier ministre, Rencontre « Safe and Smart JO » à la Préfecture d'Ile-de-France le 05.02.2019, notes ethnographiques*)

Les grands événements sportifs, comme les JOP, la Coupe du monde de rugby accueillie en France en 2023, sont centraux dans la mise en œuvre de dispositifs de sécurité pour l'espace urbain. Emblématiques, ils sont susceptibles de favoriser un consensus politique sur l'évolution du cadre règlementaire. La mise en œuvre de dispositifs de sécurité lors de ces événements festifs, apolitiques et consensuels, peut également contribuer à en banaliser l'usage pour le public. Finalement, ils permettent l'expérimentations de dispositifs qui nécessitent un calibrage en conditions réelles. Par exemple, le fonctionnement d'un algorithme d'analyse d'image varie fortement, s'il est testé « en laboratoire » ou sur des caméras qui filment une rue, pour laquelle l'exposition lumineuse variera, ainsi que la position de la caméra, l'habillement des individus, leur visibilité, leur nombre, leur mobilité, etc. Il doit donc être « entrainé » dans ces conditions afin d'être plus fiable.

Cette fonction d'expérimentation est soutenue par les institutions de recherche françaises. L'Agence Nationale de la Recherche (ANR) a ainsi proposé un appel à projets « Flash », dispositif de financement accéléré destiné à soutenir un « besoin urgent de recherches dont la pertinence scientifique est en lien avec un évènement nécessitant une forte réactivité sur des thématiques ciblées »[4]. Cet appel « Flash » porte sur des projets menés par un consortium constitué d'au moins un organisme de recherche public et une société commerciale. Six projets ont été retenus, pour un budget global de 2,8 millions d'euros cofinancé par l'ANR et le Secrétariat général de la défense et de la sécurité nationale (SGDSN). « L'ensemble des solutions alors éprouvées dans un environnement opérationnel, pourraient constituer des opportunités pour la filière des industries de sécurité et *in fine* testées en conditions réelles à l'occasion d'au moins un des grands évènements qu'accueillera la France avant les JOP 2024. »[5] La moitié des projets sélectionnés portent sur le contrôle des mouvements de foule (GIRAFE, OKLOS, MAASTeR), l'un d'entre eux proposant de développer des « stratégies prédictibles de gestion des foules pourront en être déduites pour adapter les dispositifs de sécurité »[6]. Un quatrième projet propose de coupler un système d'identification biométrique au contrôle d'accès (EASIMob), quand le cinquième (DISCRET) propose de détecter les situations atypiques ou critiques en utilisant les données de téléphonie mobile et du réseau social Twitter.

Les grands événements apparaissent ainsi comme des projets-clef pour le développement, l'expérimentation et la légitimation des projets de sécurité numérique. Les crises fournissent elles aussi des occasions à l'évolution des normes : c'est ce qu'ont montré les attentats de 2015, qui ont fortement impacté les représentations de la sécurité. Mais c'est aussi le cas de l'épidémie

[4] https://anr.fr/fr/actualites-de-lanr/details/news/lancement-des-projets-laureats-de-lappel-a-projets-flash-jop24/#
[5] *Ibid*.
[6] *Ibid*.

de Covid-19 en 2020, avec la mise en œuvre de dispositifs tels que StopCovid (parmi d'autres), et ce, malgré les risques aux libertés publiques. Les entreprises Atos et Thales, que l'on retrouve dans nombre de projets de « safe city », appartiennent d'ailleurs à « l'écosystème des contributeurs » de cette application. Si ces événements facilitent la représentation des dispositifs numériques de sécurité comme des solutions aux enjeux contemporains, le soutien à leur développement ne se limite pas aux temps de crise. Atos et Thales sont ainsi parmi les grandes entreprises auxquelles ont le plus bénéficié le budget européen dédié à la recherche en sécurité, cumulant respectivement 6,5 et 4,6 millions d'euros pour différents projets.

L'expérimentation de projets de sécurité numérique dans les villes

Des projets divers voient le jour dans différentes métropoles en France : Nice, Marseille, Saint-Etienne, etc. Ils sont souvent très médiatisés, et leur politisation contribue aux luttes locales, tout en s'inscrivant dans des politiques d'image destinées à renforcer l'attractivité et le développement économique. La sécurité est un élément important des nombreux classements internationaux de villes et il existe aussi des listes des « Safe cities » internationales. La vidéosurveillance dite « intelligente », par l'analyse d'images à des fins de reconnaissance faciale, de détection d'objets, etc., est l'un des dispositifs qui attire la plus grande attention. Il existe néanmoins une très grande variabilité de l'offre, de même que les données produites et analysées à des fins de sécurité sont diverses et issues de façon croissante d'entreprises privées (ex. réseaux sociaux ou téléphonie mobile), tout comme les algorithmes utilisés.

Des multinationales comme des *start-up* développent ainsi des logiciels d'analyse de données, des plateformes d'hypervision, des caméras intelligentes, etc. C'est le cas d'entreprises de défense, aéronautique et sécurité, à l'instar de Thales, dont le chiffre d'affaire était de 18,4 milliards d'euros en 2019. Thales a fortement investi le numérique, dédiant par exemple 1 milliard d'euros en Recherche & Développement, créant des Digital Factory à Paris, Montréal et Singapour, destinées à favoriser le développement de produits en interne et acquérant des entreprises, telle que Gemalto en 2019, spécialisée dans la gestion de l'identité (des personnes et objets) et de la sécurité numériques. Thales est à la tête d'un consortium de 15 entreprises[7], qui développe un démonstrateur de « safe city » qui doit être testé à Nice et dans le quartier d'affaires de la Défense. Ce projet a été soutenu par le Programme d'Investissement d'Avenir (PIA) opéré par Bpifrance et a obtenu 10,9 millions d'euros sous forme de subventions et d'avances récupérables. A Nice, il comprend différents éléments :

> « Les marchés visés sont ceux de la sécurité des villes et des zones d'intérêt commun, de la sécurité des écoles (biométrie *wearable*, analyse comportementale par vidéo), des patrouilles de police, des systèmes de commandement et de contrôle, des systèmes vidéo de sécurité routière et des systèmes de simulation de déplacement de foule. Le projet permettra à chaque partenaire d'atteindre le marché plus rapidement avec un contenu fonctionnel plus riche sur des marchés mondiaux où la concurrence est exacerbée. »[8]

[7] Les membres du consortium sont : Thales, Arclan Systems, Business Card Associates, Deveryware, Egidium, Gemalto (racheté par Thales), Geol Semantics, Igo, Inria (institution de recherche), Luceor, Onhys, Idemia, Sis, Sysnav et Yncréa (institution de recherche).

[8] presse.bpifrance.fr/investissements-davenirle-projet-innovant-safecity-pour-renforcer-la-securisation-des-villes-intelligentes-sur-le-territoire-obtient-un-financement-du-programme-dinvestissements-davenir-pia/

Néanmoins, la « safe city » n'est pas l'apanage des entreprises de sécurité et défense. Celles des secteurs des NTIC, ou encore de l'énergie et des services urbains, dont on donne ici quelques exemples, s'y intéressent également. C'est le cas d'Amazon, qui développe des logiciels de reconnaissance faciale ainsi que les caméras de vidéosurveillance Ring, destinées aux particuliers, dont l'installation est recensée par certaines polices au Royaume-Uni[9]. ATOS recueille et en analyse des données urbaines afin « d'aider la ville à offrir un environnement sécurisé à ses citoyens pour améliorer la qualité de vie », un dispositif mis en œuvre dans le quartier nocturne de la ville d'Eindhoven, aux Pays-Bas. Est également proposée « City Safe », solution de communication sécurisée pour les forces de sécurité, une version civile d'un dispositif initialement destiné aux militaires de l'opération Sentinelle. Finalement, des multinationales comme Engie, l'un des plus grands groupes du secteur de l'énergie, ont également développé une activité dans le domaine de la sécurité urbaine. L'une de ses filiales développe ainsi une offre de « safe city » basée notamment sur l'hyperviseur SenCity. L'entreprise gère l'Observatoire de la tranquillité publique à Marseille, qui analyse des données diverses à des fins de sécurité, ou encore la vidéosurveillance pour la Préfecture de Paris. Engie mène par ailleurs le consortium d'entreprises ayant récemment remporté le marché public de « territoire intelligent » de la métropole d'Angers.

Les entreprises privées ne sont toutefois pas seules dans la construction de ce marché de la sécurité urbaine numérique. Celui-ci est en effet soutenu aussi par les représentants des pouvoirs publics, à commencer par ceux des collectivités locales qui les accueillent. La « safe city » s'est en effet muée en objet de concurrence interurbaine, s'inscrivant dans des politiques d'attractivité et de développement économique local. Si la sécurité tend aujourd'hui à transcender de façon croissante les oppositions politiques, nombre des villes emblématiques des projets de « safe city », telles que Valenciennes, Marseille, Nice, ou encore Saint-Etienne, ont des maires à droite de l'échiquier politique.

Certaines métropoles sont devenues centrales dans l'expérimentation de projets de sécurité numérique pour l'espace urbain. C'est notamment le cas de la Ville de Nice, qui coordonne le 13e partenariat de l'Agenda urbain de l'Union européenne dédié à la sécurité urbaine. Elle accueille un grand nombre de projets portant sur la sécurité urbaine : l'expérimentation de la reconnaissance faciale à l'entrée de lycées avec l'entreprise états-unienne Cisco (finalement annulée, à la suite du recours au Tribunal Administratif de Marseille de plusieurs associations de défense des libertés) ; Engie Ineo a développé, installé et assure la maintenance de la vidéoprotection à Nice, où l'entreprise a également formé les agents municipaux à son utilisation. Edicia y a déployé, comme à Marseille, un système d'information et de communication à destination de la police, les « données de la sécurité publique collectées par SMART POLICE permettent l'alimentation de l'observatoire de la ville de Nice et des hiérarchies intermédiaires sous forme de cartes, d'indicateurs de tendances, de bilan d'activité… permettant en temps réel ainsi qu'à froid, de gouverner la Police »[10]. Des entreprises utilisent également des solutions d'analyse algorithmique d'images, comme Nomadys en partenariat avec CASD. En 2019, la reconnaissance faciale y est expérimentée lors

[9] www.telegraph.co.uk/politics/2020/03/29/police-recruit-householders-create-network-doorbell-cameras/
[10] https://www.edicia.fr/clients

du Carnaval de Nice, sur des volontaires, avec l'entreprise israélienne de reconnaissance faciale AnyVision et Confidentia, entreprise de cybersécurité basée à Monaco.

Les élus et représentants des forces de sécurité de la Ville de Nice, touchée en 2016 par un attentat ayant fait 86 morts sont particulièrement mobilisés dans le développement de projets de sécurité numérique pour l'espace urbain. Ainsi que l'énonce Christian Estrosi, maire Les Républicains de la ville, « Vous pouvez me proposer qu'on en revienne aux arbalètes et aux armes du chevalier Bayard à Marignan. La guerre du 21e siècle se mène avec les armes du 21e siècle. »[11]

Dans d'autres métropoles comme Lille, Lyon, Montpellier ou Strasbourg, des projets portés par CASD, entreprise centrale dans le réseau en raison de son implantation ancienne dans les réseaux urbains de vidéosurveillance, concernent l'expérimentation de vidéosurveillance « intelligente », avec des algorithmes analysant les images. Ce même type d'algorithmes, afin de repérer des objets, des colis abandonnés, certains types de mouvements, est mis en œuvre dans le métro francilien par la RATP, notamment dans des stations centrales telles que les gares ou à Châtelet. D'autres cas présentés ici concernent la fusion de postes de contrôle de différents services municipaux, dont la sécurité, comme le projet de « ville intelligente » de Dijon (regroupement des PC Sécurité, PC Police Municipale, Centre de Supervision Urbaine, PC Circulation, Allo Mairie et PC Neige). Finalement, certains projets se centrent sur une plateforme destinée à mieux gérer la sécurité urbaine, voire à prédire les risques, grâce à l'analyse de données diverses (trafic routier, sécurité, hôpitaux, analyse des réseaux sociaux, etc.). C'est le cas de l'Observatoire de la tranquillité publique à Marseille, développé pour 1,8 millions d'euros par Engie Ineo, ou de 3DEXPERIENCity Virtual Rennes, de Dassault, qui « aura pour objectif de faciliter le partage de données à distance afin de simuler, planifier et piloter la ville de façon transversale et collaborative, pour élaborer des politiques publiques efficaces », y compris dans le domaine de la sécurité.

Enjeux urbains de la sécurité numérique

Quels sont les enjeux du déploiement de la sécurité numérique dans les espaces urbains ? Les recherches sur le développement de dispositifs numériques de sécurité s'attachent le plus souvent à en discuter les implications en termes de respect des libertés et de contrôle des données personnelles (Scheinin et Sorell, 2015), d'inégalités sociales (Buolamwini, 2017) ou en pointant l'avènement d'un capitalisme de la surveillance (Zuboff, 2019). Néanmoins, la plupart de ces travaux n'interroge pas les enjeux que posent ces dispositifs en termes de gestion et d'appropriation de l'espace urbain. On propose ici deux pistes de réflexion, en pointant comment ces dispositifs peuvent influer sur l'aménagement des espaces urbains et leur appropriation ordinaire.

La littérature sur les dispositifs de sécurité revient sur deux formes idéal-typiques de transformations de l'aménagement urbain qu'ils peuvent occasionner : d'une part, des formes de clôture et de séparation des groupes sociaux, à l'image des résidences fermées, menant à un « urbanisme éclaté » (Graham et Marvin, 2001). D'autre part, un renforcement du contrôle

[11] *Ibid*.

social mettant en jeu la visibilité (et la surveillance), sans que les groupes sociaux ne soient séparés, par le ciblage de certains d'entre eux, selon leur appartenance de classe et ethnique notamment (Coleman, 2004).

Les grands événements témoignent de la façon dont le recours à des dispositifs de sécurité numérique favorisent la clôture et la privatisation d'espaces, le plus souvent de façon temporaire. L'Euro 2016, avec ses « Fan zone », telle que celle du Champ de Mars (trois barrières successives de contrôles de sécurité mobilisant police, agents municipaux et agents de sécurité), gérée par Lagardère Sports et pouvant accueillir 90 000 personnes, en est exemplaire, comme le seront probablement les JOP de 2024. Ces espaces clos permettent un meilleur fonctionnement des dispositifs numérique de sécurité, en particulier la vidéosurveillance dite « intelligente ». La clôture temporaire d'espaces expérimentée à grande échelle pendant l'Euro 2016 est par la suite entrée dans la Loi sécurité intérieure et lutte contre le terrorisme du 30 octobre 2017. Ces dispositifs, qui augmentent les coûts d'organisation, conduisent aussi à faire payer l'entrée pour des manifestations auparavant gratuites.

Si la clôture d'espaces peut avoir lieu de façon temporaire, les enjeux économiques liés à la mise en œuvre de dispositifs lourds pour de grands événements, comme les JOP à Saint-Denis, peut encourager à les maintenir et donc s'inscrire de façon durable dans l'espace urbain. Ces dispositifs numériques posent aussi la question de l'invisibilité du contrôle et donc de la difficulté de s'y soustraire. Les enjeux du consentement au recueil de données personnelles sont très différents lorsque l'on parle de la consultation d'un site internet ou de dispositifs inscrits dans l'espace urbain, où ils ne sont d'ailleurs pas toujours visibles.

La mise en œuvre de dispositifs numériques dans l'espace public est également susceptible d'influer sur l'appropriation de celui-ci par différents groupes sociaux. La gestion de foules, comme on l'a vu à propos des JOP de 2024, est une thématique très présente dans le développement de dispositifs numériques de sécurité. La supervision de foules vise premièrement à permettre une circulation fluide, tout en maintenant la sécurité et en évitant les débordements, par exemple grâce à des algorithmes d'analyse d'image qui remontent des alertes en cas d'événement inhabituel. Florent Castagnino (2019) montre que cela conduit à un déplacement de la définition de ce qui est « suspect », par la catégorisation mathématique et informatique des événements, l'anormalité étant alors entendue au sens statistique et moral du terme. Il s'agit alors que la masse d'individus ne se transforme pas en « foule », au sens que donnait déjà à ce terme la psychologie sociale à la fin du 19^{e} siècle.

Des logiciels offrent ainsi différentes métriques, tels que des calculs de densité, etc., et proposent leurs services en amont de l'aménagement d'espaces publics, afin de gérer au mieux les flux dans les espaces publics. Les simulations que développent ces entreprises spécialisées dans la modélisation des flux piétons témoignent d'une vision particulière de l'occupation de l'espace public : celui-ci n'accueille jamais d'individus stationnaires, il s'agit seulement d'espaces passants ; les individus qui le traversent se déplacent au maximum par deux, il n'y a jamais de groupes. C'est le cas par exemple des simulations proposées par l'entreprise Onhys, spécialisée dans la modélisation de flux piétons, qui prend part au démonstrateur « Safe city » à Nice (voir figure ci-dessous).

Figure 1. Exemples de simulations de flux piétons pour la gestion urbaine, par l'entreprise Onhys

Source : https://www.youtube.com/watch?v=uhFu-rkI5LY

On retrouve une vision normative des espaces urbains, circulatoires et individuels, qui peut ensuite s'incarner dans la façon dont ils sont aménagés, à l'aide de ces logiciels. Or, les modes d'occupation de l'espace public sont centraux dans les luttes entre groupes sociaux pour l'appropriation de l'espace urbain. En outre, le recours aux dispositifs numériques ne répond pas uniquement à une logique sécuritaire mais contribue aussi à la rationalisation de la gestion de l'espace : les algorithmes de simulation de foules dans un centre commercial permettent certes d'anticiper des plans d'évacuation en cas d'urgence, mais ils offrent surtout la possibilité de définir des parcours imposés aux visiteurs ou de varier le montant des baux commerciaux et des panneaux publicitaires selon la fréquentation prédite.

Le développement de dispositifs de gestion des foules ne concerne pas seulement les grands événements tels que les JOP 2024. Il s'attache aussi à la gestion de manifestations politiques dans l'espace public. Outre la circulation de dispositifs de la gestion de grands événements vers les manifestations, certains projets sont spécifiquement dédiés à ces dernières. C'est le cas par exemple du projet soutenu par l'Agence Nationale de la Recherche, porté en France par l'INRIA et Onhys, avec la Gendarmerie nationale, intitulé OPMoPS, pour « Mouvements organisés de piétons dans les espaces publics : Préparation et gestion des parades urbaines et des manifestations à fort potentiel de conflit » :

> « Les parades de groupes très controversés ou les manifestations politiques sont considérés comme une menace majeure pour la sécurité urbaine, puisque les opinions diamétralement opposées des participants et des opposants peuvent conduire à la violence ou même à des attaques terroristes. […] Les problèmes techniques spécifiques auxquelles [sic] le consortium franco-allemand devra faire face sont les suivants : méthodes d'optimisation pour planifier des itinéraires de l'UPM, transport vers et depuis l'UPM, planification du personnel FCS et de leur localisation, contrôle des UPMs en utilisant des caméras fixes et

> mobiles, ainsi que des méthodes de simulation, en incluant leur visualisation, et en mettant un accent particulier sur le comportement social. »[12]

Ces questions, déjà investies auparavant, ont connu un regain après les manifestations des « Gilets jaunes », qui étaient présentées comme désorganisées, ne suivant pas de parcours déposé et donc plus difficiles à contrôler. Ainsi, l'importance de la sécurité des grands événements dans le développement de dispositifs numériques de sécurité doit aussi se comprendre comme une zone d'expérimentation, dépolitisée, de dispositifs circulant possiblement par la suite au contrôle des manifestations politiques. Cela s'est déjà vu, avec notamment la circulation d'instruments juridiques[13], du contrôle des supporters de football aux manifestants. La sécurité des grands événements et de leurs publics apparaît donc centrale dans le développement de dispositifs et témoigne également d'un processus de sécurisation croissante de l'occupation de l'espace public par des groupes, organisés ou non, qui peut s'accompagner de leur stigmatisation.

Ainsi, la sécurité numérique dans les espaces publics ne pose pas uniquement des questions liées aux libertés publiques ou au recueil de données personnelles. Elle contribue également aux transformations des formes de l'espace urbain, et des modes d'appropriation des espaces publics. En cela, la sécurité, dans ses différentes formes, joue aussi un rôle dans les inégalités entre les groupes sociaux qui résident dans les villes.

Conclusion

L'essor des dispositifs numériques pour la sécurité urbaine est relativement récent, en ce qui concerne leur expérimentation en France. Néanmoins, la construction de marché s'ancre dans trois phénomènes : les transformations du marché de la sécurité privée, la croissance des objets connectés et des possibilités d'analyse de données massives et finalement la représentation des villes comme des lieux du renouveau économique. Les projets de « safe cities » témoignent ainsi d'un phénomène plus global de multiplication des agents, publics et privés, investissant la définition et la production de la sécurité urbaine. Si les enjeux pour les libertés publiques sont souvent soulignés, c'est aussi de la façon de vivre dans les villes qu'il est question. Sans aller jusqu'à y voir un urbanisme militaire, il semble nécessaire de s'interroger, au-delà de l'enjeu de la surveillance, sur l'avenir urbain qu'offre cette sécurité numérique, le plus souvent invisible, à nos vies dans les métropoles européennes. C'est un angle que doivent aussi interroger les études actuelles sur la mise en œuvre réelle des projets de « safe cities », en examinant leurs usages, leurs détournements, mais aussi leur réception par les habitants des villes, qui ne sont pas tous égaux face à ces dispositifs de sécurité numérique.

[12] https://www.onhys.com/projects/post/opmops

[13] En 2006, la loi relative à la lutte contre le terrorisme crée les interdictions *administratives* de stade, décrétées même en l'absence d'infractions antérieures, afin de lutter contre le « hooliganisme ». Le 10 avril 2019, est votée la loi visant à renforcer et garantir le maintien de l'ordre public lors des manifestations, qui rend possible l'interdiction administrative de manifester, inspirée des supporters. Cet article de la loi est finalement censuré par le Conseil Constitutionnel. De même, en 2018, les défilés de « Gilets jaunes » avaient réactivé l'idée d'un fichier des « casseurs », semblable aux recensements des supporters ultra.

Bibliographie

AMOORE L., 2013, *The politics of possibility: Risk and security beyond probability*, Durham, NC, Duke University Press.

BENNETT, C.J., HAGGERTY, K.D. (dirs.), 2011, *Security Games: Surveillance and Control at Mega-Events*, New York, Routledge.

BUOLAMWINI J.A., 2017, « Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers », Mémoire de master, Master of Science at the Massachusetts Institute of Technology, MIT.

CASTAGNINO F., 2019, « Rendre "intelligentes" les caméras : déplacement du travail des opérateurs de vidéosurveillance et redéfinition du soupçon », Working Paper de la chaire « Villes et numérique », 2019/05, Paris, Sciences Po, Ecole urbaine.

CNI, 2020, « Contrat Stratégique de la Filière. Industries de sécurité 2020/2022 », Paris, Conseil National de l'Industrie.

COLEMAN R., 2004, *Reclaiming the Streets: Surveillance, Social Control and the City*, Collompton, Willan Publishing.

CUKIER K., MAYER-SCHÖNBERGER V., 2014, *Big Data : La révolution des données est en marche*, Paris, Robert Laffont.

DECISION ETUDES & CONSEIL, 2018, « Observatoire de la filière industrielle de sécurité 2017-2018. Rapport Final », Paris, Observatoire de la filière industrielle de sécurité.

FOUCAULT M., 2004, *Sécurité, territoire, population : cours au Collège de France, 1977-1978*, Paris, Seuil : Gallimard.

GRAHAM S., MARVIN S., 2001, *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*, Londres, Routledge, 512 p.

HARCOURT B.E., 2005, « Against Prediction: Sentencing, Policing, and Punishing in an Actuarial Age », *SSRN Electronic Journal*.

LEMAIRE É., 2019, *L'oeil sécuritaire. Mythes et réalités de la vidéosurveillance*, Paris, La Découverte.

MAILLARD J. DE, ZAGRODZKI M., BENAZETH V., ZASLAVSKY F., 2015, « Des acteurs en quête de légitimité dans la production de l'ordre public urbain : L'exemple des inspecteurs de sécurité de la Ville de Paris », *Déviance et Société*, *39*, 3, p. 295-319.

MALOCHET V., OCQUETEAU F., 2020, « Gouverner la sécurité publique », *Gouvernement et action publique*, *VOL. 9*, 1, p. 9-31.

PARK R.E., BURGESS E.W., MCKENZIE R.D., 1925, *The City*, Chicago, University of Chicago Press.

SCHEININ M., SORELL T., 2015, « Merging the ethics and law analysis and discussing their outcomes », SURVEILLE Deliverable D4.10 Synthesis report from WP4, Florence, Surveillance: Ethical issues, legal limitations, and efficiency (FP7 – SEC-2011-284725).

WEBER M., 2014, *La ville*, Paris, La Découverte.

ZUBOFF S., 2019, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, London, Profile Books, 704 p.