HAL
open science

Peur sur la ville. La sécurité numérique pour l'espace urbain en France

Myrtille Picaud

To cite this version:

Myrtille Picaud. Peur sur la ville. La sécurité numérique pour l'espace urbain en France. [Rapport de recherche] 01/2021, Chaire "Villes et numérique", Ecole urbaine de Sciences Po. 2021. halshs-03138381

HAL Id: halshs-03138381

https://shs.hal.science/halshs-03138381

Submitted on 11 Feb 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SciencesPo
CITIES AND DIGITAL TECHNOLOGY CHAIR

Working Paper

> N°01/2021

Peur sur la ville. La sécurité numérique pour l'espace urbain en France

Myrtille Picaud

SciencesPo

CITIES AND DIGITAL TECHNOLOGY CHAIR

The "Cities and Digital Technology" Chair of Sciences Po's Urban School has been launched in March 2017 to better grasp the impact of digital technologies on urban governance. Funded by three sponsoring firms (La Poste, RTE, Caisse des Dépôts), the Chair aims to create new research fields exploring the interaction between digital technology and cities in an empirical and comparative perspective.

Peur sur la ville. La sécurité numérique pour l'espace urbain en France

Myrtille Picaud

Postdoctorante au Labex Futurs Urbains et au Laboratoire Techniques, Territoires et Sociétés (LATTS)

Chercheuse associée à la chaire « Villes et numérique » de l'École urbaine de Sciences Po et au Centre d'études européennes et de politique comparée (CEE), docteure associée au Centre européen de sociologie et de science politique (CESSP)

myrtille.picaud@sciencespo.fr

Résumé

A Nice, Marseille, Saint-Etienne ou encore Valenciennes, se développent des projets de « safe city », pendant sécuritaire de la « smart city ». A la vidéosurveillance « intelligente », où l'analyse d'image s'appuie sur des algorithmes de détection de mouvements de foule, de violences, d'intrusion s'ajoutent 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. Qui sont les acteurs de cette montée en puissance des « safe cities » ? Quels sont les effets sur les villes et leurs habitants de cette façon de mesurer les risques et de les prévenir, voire de les instrumentaliser ? On examine le développement de l'offre de dispositifs numérique de sécurité urbaine en France. La première partie se focalise sur la construction du marché de la sécurité numérique pour les espaces urbains, en l'inscrivant dans les transformations du marché de la sécurité privée et le développement d'une politique industrielle de la sécurité, dans laquelle la sécurité des grands événements joue également un rôle central. La seconde partie revient sur les expérimentations de projets de sécurité numérique dans des métropoles en France, éclairant les approches différentes de la sécurité urbaine, selon le secteur d'activité des entreprises. Finalement, la troisième partie analyse les enjeux proprement urbains du recours à ces dispositifs, sur l'aménagement des espaces urbains, leur mode d'occupation et en distinguant quels espaces sont ciblés en priorité.

Mots clés : marché ; sécurité ; numérique ; urbain ; ville ; entreprises ; jeux olympiques

Table des matières

Résumé 3
Introduction 5
1 Le marché des dispositifs numériques de sécurité pour l'espace urbain 6
Le marché global de la sécurité privée en France 7
Les « safe cities » et « territoires de confiance » au cœur de la politique industrielle de sécurité 9
Les grands événements, centraux dans le développement de dispositifs de sécurité 12
2 Les « safe cities » : expérimentations et approches 15
L'expérimentation de projets de sécurité numérique dans les métropoles 16
Approches différenciées de la sécurité urbaine 20
3 Enjeux urbains du déploiement de la sécurité numérique 24
Transformations des espaces urbains 24
Le ciblage différencié des espaces urbains 25
Modes d'occupation de l'espace public 27
Conclusion 29
Bibliographie 31
Liste des figures 35
Liste des encadrés 35
Liste des cartes 35

Introduction

L'explosion des capacités de calcul et des données produites (Cardon, 2015 ; Cukier et Mayer-Schönberger, 2014 ; Pentland, 2013 ; Van Dijck, 2014), grâce notamment aux téléphones et capteurs connectés (Townsend, 2013), offre de nouvelles possibilités pour la sécurité urbaine. Dans le cadre d'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 ; Gautron et Monniaux, 2016 ; Lakoff et Klinenberg, 2010), se développent par exemple des offres de police « prédictive » (Benbouzid, 2018 ; Brayne, 2017 ; Egbert, 2019). À celles-ci s'ajoutent aujourd'hui un nombre très important de dispositifs numériques, mis en œuvre par différentes catégories d'agents, afin de préserver la sécurité urbaine.

A Nice, Marseille, Saint-Étienne 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[1]. 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'État, 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[2], 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.

Néanmoins, la sécurité urbaine n'est pas un sujet nouveau. 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 ; Shaw, 1968 ; Thrasher, 1929). Des travaux montrent que cette représentation nourrit également les discours politiques et médiatiques sur l'incivilité (Body-Gendrot, 2012 ; Gayet-Viaud, 2017) et les violences urbaines en France (Collovald, 2001 ; Roché, 2004). La recherche à ce sujet s'est donc principalement centrée sur l'instrumentalisation politique des enjeux de sécurité, dans les politiques nationales (Tissot, 2007) et locales (Freyermuth, 2013 ; Le Goff, 2005).

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 » ? Quels sont les effets sur les villes et leurs habitants de cette façon de mesurer les risques et de les prévenir, voire de les instrumentaliser ?

[1] « Ces signalements alimenteront une cartographie la plus précise possible facilitant le travail des pouvoirs publics pour développer efficacement des politiques publiques et des actions ciblées en faveur de la lutte contre les violences sexistes, anti-LGBT et sérophobe. » https://www.flagasso.com/actualites/item/l-application-flag-le-lancement.html

[2] https://technopolice.fr/

On examine ici le développement de l'offre de dispositifs numérique de sécurité urbaine en France. La première partie se focalise sur la construction du marché de la sécurité numérique pour les espaces urbains, en l'inscrivant dans les transformations du marché de la sécurité privée et le développement d'une politique industrielle de la sécurité, dans laquelle la sécurité des grands événements joue également un rôle central. La seconde partie revient sur les expérimentations de dispositifs de sécurité numérique dans des métropoles en France. Cela témoigne des différentes approches de la sécurité urbaine, selon le secteur d'activité des entreprises. Finalement, la troisième partie analyse les enjeux proprement urbains du recours à ces dispositifs numériques de sécurité, sur l'aménagement des espaces urbains, leurs modes d'occupation et en distinguant quels espaces sont ciblés en priorité.

1 Le marché des dispositifs numériques de sécurité pour l'espace urbain

L'expansion des expérimentations de dispositifs numériques pour les villes fait l'objet de nombreux discours médiatiques. Néanmoins, peu de recherches se penchent sur le développement d'un marché de la sécurité urbaine et l'offre de dispositifs numériques. Or, ceux-ci sont ancrés dans les transformations du marché de la sécurité privée, la croissance des possibilités offertes par les objets connectés et l'analyse de données massives. Les villes apparaissent également comme les lieu du renouveau économique, notamment à travers l'économie des plateformes numériques (Abdelnour et Méda, 2019 ; Barns, 2020), et donc des marchés locaux pour la sécurité.

La mise en marché de la sécurité, un domaine régalien, a pu être interprétée comme une « privatisation » ou un retrait de l'État (Avant, 2005 ; Renou, 2005). D'importants travaux mettent toutefois en valeur le rôle majeur de ce dernier, comme d'instances supranationales, dans la structuration de différents marchés en France et en Europe (Bourdieu, 2000 ; Dubuisson-Quellier, 2016 ; Fligstein, 2001 ; François, 2007). De même, le développement des marchés militaires (Magnon-Pujo, 2011) éclaire la redéfinition des frontières de l'État (Abrahamsen et Williams, 2009 ; Hibou, 1998) plutôt que sa disparition. Les travaux actuels mettent en avant la multilatéralisation[3] du travail de police, afin de désigner la multiplication des agents, publics et privés, qui le prennent en charge. Qu'en est-il pour la sécurité numérique des espaces urbains ?

On revient d'abord sur les transformations du marché global de la sécurité privée en France et la concurrence croissante d'entreprises étrangères, notamment chinoises ou états-uniennes. Ensuite, on examine l'inscription des projets de « safe cities » dans une politique industrielle de sécurité, soutenue par des représentants des pouvoirs publics à l'échelle locale, nationale, mais aussi européenne. Finalement, on analyse le rôle des grands événements tels que les Jeux Olympiques et Paralympiques (JOP) dans le développement du marché de la sécurité numérique pour les espaces urbains.

[3] 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). Voir (Jones et Newburn, 1998 ; de Maillard et Zagrodzki, 2015).

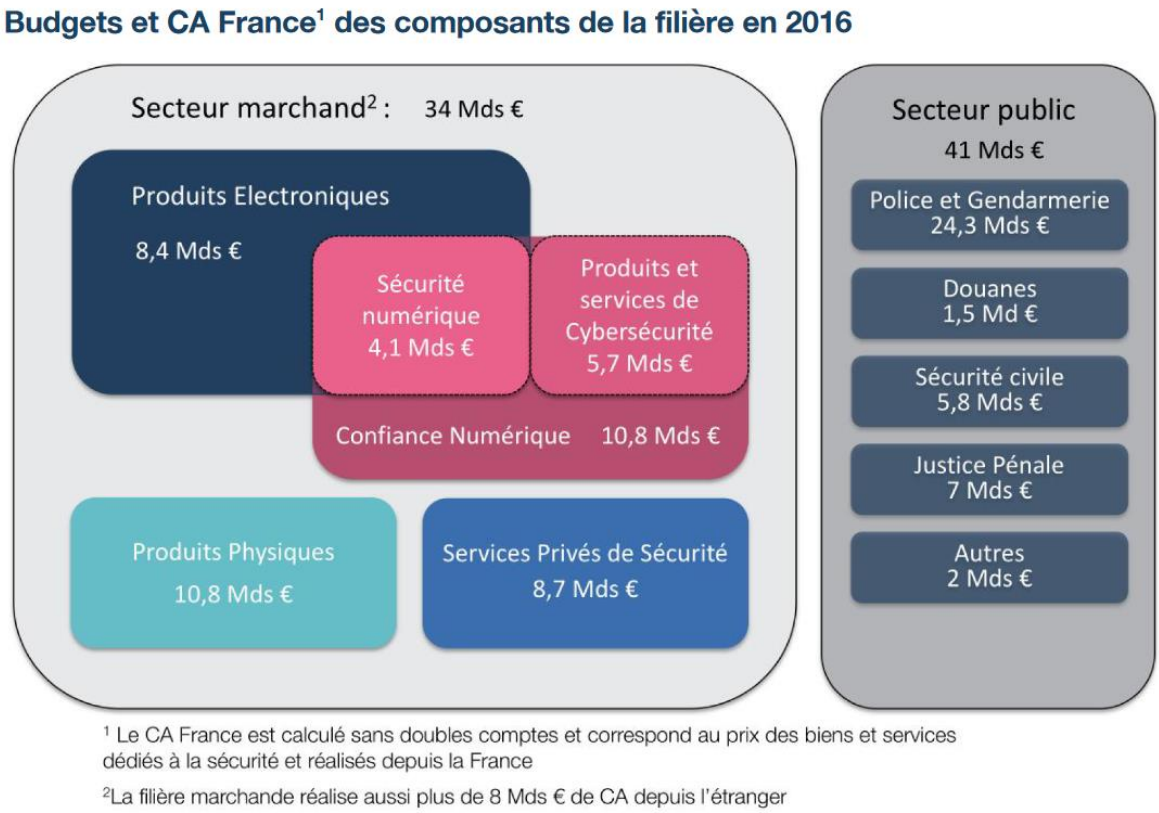
Le marché global de la sécurité privée en France

Dès le début des années 2000, les « établissements publics et les collectivités locales (municipalités) sont devenus une clientèle de première importance pour la surveillance à distance privée et la gestion commerciale contractuelle, trait dominant de la sécurité urbaine » (Ocqueteau, 2004a, p. 115). La sécurité en ville contribue en effet de façon centrale au développement du marché de la sécurité privée. À la fin des années 1980, est théorisée la « coproduction des polices de la ville » (Warfman et Ocqueteau, 2011a), qui se traduit par l'accroissement du chiffre d'affaires des entreprises spécialisées dans la surveillance à distance, à l'instar de la vidéosurveillance, alors même que l'économie entre en récession. En 1996, la vidéosurveillance dans les espaces publics et les sites privés accueillant du public est réglementée par un décret (Warfman et Ocqueteau, 2011b). En 2011, la Loi d'orientation et de programmation pour la performance de la sécurité intérieure favorise à son tour la multiplication des caméras dans les espaces urbains.

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[4] (voir Figure 1 ci-dessous). En Europe, il était de 170 milliards d'euros (2,8 millions d'employés) et de 688 milliards d'euros dans le monde. Les entreprises de ce marché présentent une forte hétérogénéité. À la fin des années 1990, c'était déjà le cas (Ocqueteau, 2004b, p. 90), avec de nombreuses très petites entreprises et une production de valeur ajoutée très concentrée sur les entreprises les plus importantes (en 1995, 5,5% comportaient plus de 100 salariés et généraient 65,6% de la valeur ajoutée). Au milieu des années 2010, le chiffre d'affaires des petites et moyennes entreprises, la majorité, représente 6,8 milliards d'euros, quand il atteint 13,1 milliards pour la minorité d'entreprises de taille moyenne (entre 250 et 4 999 salariés) ou de grandes entreprises, qui totalisent 4,2 milliards d'euros de chiffre d'affaires (Decision Etudes & Conseil, 2018).

[4] La définition du périmètre du marché de la sécurité fait l'objet de discussions (Ocqueteau, 2004b) 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).

Figure 1. Budgets et chiffres d'affaire des secteurs public et privé de la sécurité en 2016



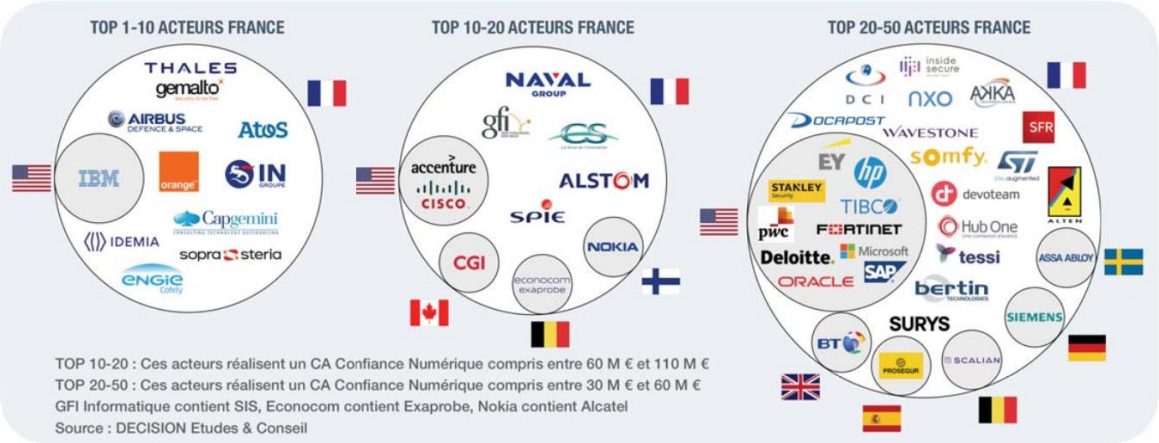
Source : (Decision Etudes & Conseil, 2018)

On constate une même hétérogénéité et concentration de la valeur ajoutée dans le secteur de la « confiance numérique », dont le chiffre d'affaires réalisé en France en 2018 serait de 12,4 milliards d'euros (Decision Etudes & Conseil, 2019). Cette filière regroupe les entreprises proposant des services et produits de cybersécurité (55% du CA), ainsi que de sécurité numérique (45% du CA : identification, contrôles d'accès, traçage et localisation, renseignement, etc.), avec respectivement 3% de grandes entreprises et d'ETI, un tiers de PME et près des deux tiers de microentreprises. Or, les grandes entreprises représentent 52% du chiffre d'affaires total. Les activités de « Systèmes et contrôle d'accès électronique » et « Autres dispositifs d'authentification et d'identification des personnes » sont celles dont le chiffre d'affaires est le plus élevé.

Avec 5,6% de croissance annuelle moyenne entre 2013 et 2016, le marché de la sécurité privée connaît une croissance supérieure à la moyenne nationale. Les produits électroniques, et en particulier numériques, sont particulièrement concernés par cette forte croissance. Néanmoins, selon l'Observatoire de la filière industrielle de sécurité, cette croissance baisse continuellement depuis 2013, une tendance qui se poursuivrait sur la période 2017-2022, en raison de la présence de plus en plus prégnante d'entreprises étrangères, notamment chinoises et nord-américaines. Celle-ci se donne également à voir dans les rachats d'entreprises françaises, avec en particulier l'acquisition d'Oberthur Technologies puis de Morpho par un fond états-unien, Advent International, ce qui a abouti à la création d'Idemia, l'une des plus grosses entreprises mondiales de biométrie, dont la direction et le siège social demeurent en France pour l'instant. L'Observatoire

de la filière de la Confiance Numérique relève également que les entreprises françaises sont concurrencées par des entreprises étrangères implantées en France (voir Figure 2 ci-dessous).

Figure 2. Entreprises dominantes de la filière dite « Confiance numérique » selon la nationalité



Source : (Decision Etudes & Conseil, 2019, p. 3)

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

La construction du marché de la sécurité numérique pour l'espace urbain doit se comprendre à l'aune des transformations du marché de la sécurité français, avec la concurrence d'entreprises étrangères, et du développement croissant de dispositifs numériques dédiés à l'espace urbain (Picaud, 2020), lié à l'explosion des capacités de calcul et des données produites, grâce notamment aux téléphones et capteurs connectés (Townsend, 2013). Il s'inscrit aussi dans l'histoire urbaine de la vidéosurveillance et la multiplication des agents, publics comme privés, investis dans la sécurité des collectivités territoriales, qui ont fortement contribué au développement du marché de la sécurité privée. On distingue ici la « sécurité numérique » de la vidéosurveillance traditionnelle par le recours à des capteurs numériques divers, qui permettent le recueil de différentes données (au-delà de l'image), et leur analyse grâce à des modélisations ayant recours notamment aux algorithmes, particulièrement au *machine learning*. C'est le cas par exemple de la vidéosurveillance dite « intelligente », ou « automatisée », dans laquelle les images de surveillance sont analysées par des algorithmes afin de repérer des personnes ou des événements spécifiques, comme par exemple une voiture qui remonterait une rue en sens interdit. Cette sécurité numérique est souvent présentée comme un remède aux failles de la vidéosurveillance « traditionnelle » (Castagnino, 2019). Dans la brochure *Pixel*, éditée par l'Association nationale de la vidéoprotection, Guillaume Cazenave, directeur général de la start-up Two-I qui propose de l'analyse d'image, explique ainsi que le « développement de l'analyse vidéo est confronté à deux principaux obstacles, liés aux limitations des capacités cognitives », la baisse de l'attention et l'insuffisante mémoire visuelle des opérateurs

(AN2V, 2020, p. 106). Le recours à l'analyse d'images, de sons et d'autres données est ainsi présenté comme un palliatif à ces « faiblesses »[5].

La construction du marché de la sécurité urbaine est soutenue par les représentants des pouvoirs publics. À l'échelle locale, elle représente un enjeu dans la concurrence interurbaine pour l'attractivité et le développement économique. À l'échelle nationale et européenne, il s'agit aussi d'un marché en croissance, fortement soutenu. Ainsi, l'Union Européenne, a dédié au moins 11 milliards d'euros à la sécurité par l'Union Européenne entre 2014 et 2020 (Jones, 2017), avec un focus important sur le développement de nouvelles technologies. Le budget dédié à la recherche en sécurité a bénéficié principalement à de très grandes entreprises : Thales a bénéficié de 33,1 millions d'euros, Airbus de 14,2 millions d'euros et Atos 14,1 millions d'euros[6] entre 2007 et 2016 de subventions pour des projets dans ce cadre. La Commission Européenne subventionne également des projets sur la protection des espaces publics, dans le cadre de l'Internal Security Fund (25 millions d'euros en 2017, 9,5 millions en 2018). L'initiative Urban Innovative Actions du Fonds européen de développement régional (100 millions d'euros en 2018) plaçait la sécurité urbaine au sein des quatre priorités pour le développement de solutions innovantes aux défis urbains[7].

À l'échelle nationale, la politique industrielle de sécurité s'est donnée pour objectif l'essor des dispositifs numériques pour l'espace urbain et le renforcement de la filière industrielle française par rapport à ses concurrents étrangers. En 2020, Christophe Castaner, ministre de l'Intérieur, Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'Économie et des Finances, et Marc Darmon, Président du Conseil des industries de la confiance et de la sécurité (CICS) et Directeur Général Adjoint de Thales, ont signé le contrat de filière 2020-2022 du Comité stratégique de filière (CSF) Industries de sécurité. Ce CSF sera présidé par Marc Darmon. Ce comité comprend cinq projets, dont « Les territoires de confiance » (parfois nommés, parmi les représentants de l'industrie « safe cities »), afin de « [p]ositionner l'industrie française comme leader mondial de la sécurité de la ville intelligente » (CNI, 2020) :

> « C'est un sujet clé aujourd'hui qui fédère tout le périmètre de la filière. En effet, il requiert le concours d'acteurs de la cybersécurité, de l'identité numérique ou encore des spécialistes de la biométrie, mais également de la sécurité physique ou électronique, puisqu'il est question de sécuriser toute une ville, bâtie entre autres sur les technologies du numérique. Un périmètre aussi large représente un marché potentiel très important. Les territoires connaissent des mutations profondes induites par de nouvelles approches conceptuelles (smart city, résilience) et par la transformation numérique. Une économie nouvelle se développe rapidement autour des données et des nouveaux usages. À une demande de services plus globaux s'ajoutent des enjeux de compétitivité et de souveraineté. Dans ce contexte, la sécurité des villes et des territoires intelligents, s'inscrit comme un élément essentiel à maîtriser pour garantir la tranquillité, la résilience et l'attractivité des territoires. La protection de l'ensemble des données et leur utilisation pertinente ne peuvent se faire qu'en appliquant les principes de sécurité dès la conception des produits et services. » (CNI, 2020, p. 37)

Le projet associe des collectivités partenaires : région Grand Est, ville de Nice et métropole Nice Côte d'Azur, métropole de Rennes, métropole de Lyon, métropole de Lille, métropole de Chartres, Syndicat d'électrification de la Loire. Dans l'objectif du développement d'une offre de services

[5] L'analyse d'image ne répond toutefois pas aux critiques sur l'inefficacité des politiques recourant à la vidéosurveillance, ou aux enquêtes témoignant des usages différenciés de celle-ci (Bétin, Martinais et Renard, 2003 ; Germain, Douillet et Dumoulin, 2012 ; Gormand, 2017 ; Lemaire, 2019).

[6] https://www.tni.org/en/publication/infographic-the-eus-security-industrial-complex

[7] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190320_swd-2019-140-security-union-update-18_en.pdf

numériques pour la sécurité des espaces urbains, sont listés des engagements de l'État et des collectivités. Ils comprennent la mobilisation de leur part de financements et de ressources pour lancer ces projets, la mise à disposition du territoire, de ses données et expertises métier afin d'expérimenter des dispositifs numériques, ou encore l'aide à « [l'exploration] des freins légaux et réglementaires ». L'évolution législative est également au centre de l'axe visant à « faciliter le déploiement de territoires intelligents et sûrs », ce marché étant présenté comme faisant face à de nombreux freins et manquant d'ambition.

La concurrence d'entreprises étrangères est en effet souvent ramenée 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 :

> « Quand on voit ce qu'on peut faire en France et ce qu'on peut faire dans d'autres pays dans le monde, je sais pas en Middle East, ou à Singapour, qui n'ont pas de – ou en Chine ! Il y a eu une émission il y a une dizaine de jours sur la sécurité en Chine, et typiquement d'ailleurs, ces gens n'ayant pas d'organisme… Enfin en tout cas, la CNIL chez eux est quand même assez inexistante… Donc ils montraient très bien qu'on identifiait très clairement les gens, et on les rappelait à l'ordre pour leurs comportements, en faisant des intru – enfin ce qu'on appellerait en France des intrusions inacceptables, pour notre culture en tout cas, de français. Et donc à ce propos, ça pose un problème aux industriels qu'on est, parce que même pour essayer des nouvelles technologies, on est confronté à la CNIL, et j'ai pas d'avis à donner sur la CNIL, c'est ce qui est en vigueur dans notre pays et qu'on doit respecter, mais du coup notre capacité d'essai, à grande échelle, de faire des tests, est beaucoup plus limitée et du coup les Chinois sont en train d'améliorer leur technologie beaucoup plus rapidement, parce qu'ils arrêtent pas de le tester. En vraie grandeur. » *(Directeur stratégie et marketing, entreprise dans le secteur de la sécurité, entretien à Paris, le 26.03.2018)*

La comparaison avec la Chine permet d'insister sur la nécessité de l'évolution du cadre légal, dans l'objectif d'une plus grande compétitivité des entreprises françaises. Ce discours s'appuie souvent aussi sur des explications culturalistes (« ce qu'on appellerait en France des intrusions inacceptables, pour notre culture en tout cas, de français »). Celles-ci permettent aux représentants d'entreprises d'insister sur l'impossibilité, en France, pour ces dispositifs de muer en surveillance généralisée et en entrave aux libertés publiques – parce que cela ne ferait pas partie de la « culture » française, à la différence de pays comme la Chine. La comparaison chinoise est donc régulièrement convoquée afin de dédramatiser l'usage de ces dispositifs (tels que 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 », ou des dispositifs numériques de sécurité destinés à l'espace urbain, est ainsi construit par les représentants de groupes d'intérêt comme des pouvoirs publics. Il est présenté comme une opportunité de croissance pour les entreprises françaises 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 allers-retours, 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 (Picaud, 2020). 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, du secteur de l'aéronautique, sécurité, défense et biométrie, y dédie 1 milliards d'euros en 2019 et a créé des Digital Factory à Paris, Montréal et Singapour, destinées à favoriser le développement de produits en interne.

Le développement de projets de « safe cities » en France peut ainsi se comprendre comme l'expérimentation de dispositifs numériques de sécurité, dans le cadre d'une concurrence entre entreprises de secteurs et de pays différents, pour s'établir sur ce marché.

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

Les enjeux urbains étaient déjà au cœur de la « politique industrielle de sécurité ambitieuse à horizon 2025 pour la France » présentée par le Comité de filière industrielle de sécurité, créé en 2018, préalable au Comité stratégique de filière (CSF) Industries de sécurité. L'une des cinq ambitions de cette politique industrielle était de faire de la France « leader mondial dans le domaine des *safe cities* ». Afin d'atteindre ces objectifs, cette politique « s'organisera[it] autour de projets emblématiques fédérateurs, notamment au profit des Jeux Olympiques de Paris 2024 ». Les JOP se retrouvent également dans le contrat de filière 2020-2022 du CSF Industries de sécurité, où ils constituent le premier projet structurant cité : Sécurité des grands événements et des Jeux Olympiques de Paris 2024. Ceux-ci sont vus comme un accélérateur du développement de nouvelles technologies et de la structuration de la filière et une opportunité pour faire évoluer le cadre légal. 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. C'est le cas lors des rencontres « Safe and Smart JO », à l'initiative de

la Coordination nationale pour la sécurité des JO et des grands événements sportifs internationaux (CNSJ) placée sous la direction du Préfet Pierre Lieutaud, et de *S&D Magazine*, ainsi que des « Jeudi de la sécurité », organisés par cette même revue spécialisée dans la sécurité et défense. Ces événements se tiennent le plus souvent à la Préfecture de Région (Ile-de-France) ; lors de Milipol, salon international des professionnels de la sécurité ; ou au MEDEF à Paris. Ils 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.

Ces rencontres 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, de tels événements justifieraient le recours à des dispositifs de sécurité exceptionnels, parfois présentés comme transitoires, à l'instar de la reconnaissance faciale dans l'espace public, très contestée par les associations de défense des libertés publiques (voir Encadré 1). Ces dispositifs sont envisagés afin de faciliter la gestion de flux et d'autorisations d'accès à différents espaces, pour les publics, ou pour les professionnels et athlètes, 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'État (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. Ces grands événements emblématiques sont susceptibles de favoriser un consensus politique sur la nécessité de faire évoluer le cadre règlementaire afin de permettre leur autorisation. Cela est particulièrement le cas en France, pays marqué par plusieurs attentats successifs à partir de 2015, où la thématique de la sécurité a été fortement réinvestie, politiquement et médiatiquement. 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, ces événements offrent autant d'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.

Encadré 1. La reconnaissance faciale

La reconnaissance faciale représenterait un marché mondial estimé à 7 milliards de dollars d'ici 2024[8]. Cette technologie est basée sur le traitement de données biométriques – des données sensibles au sens du Règlement général sur la protection des données européen – et interdite sauf exception, par exemple avec le consentement des individus. Il est donc possible de mettre en œuvre, dans certaines conditions et quand cela est proportionné, des solutions de reconnaissance faciale pour l'authentification des personnes. L'utilisation dans l'espace public pour

[8] https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html

l'identification, et à des fins sécuritaires, est soumise à la Directive Police-Justice. Elle est à ce jour interdite, car non encadrée par des textes. La CNIL appelait dès 2018 à un débat sur les éléments techniques, juridiques et éthiques[9] de cette technologie et en novembre 2019 à « tracer des lignes rouges au-delà desquelles aucun usage, même expérimental, ne peut être admis »[10]. La reconnaissance faciale avait par exemple été expérimentée auprès de volontaires lors du carnaval de Nice, afin de tester son efficacité. Les associations de défense des libertés publiques soulignent quant à elles la dimension invasive de cette technologie, qui transforme le visage en traqueur, ainsi que son invisibilité dans l'espace public, conférant à « l'État un pouvoir de contrôle total sur la population, dont il ne pourra qu'être tenté d'abuser contre ses opposant·es politiques et certaines populations »[11].

La Commission Européenne souhaite encadrer (plutôt qu'interdire) ces systèmes d'identification biométrique à distance. Plus généralement, à propos du recours à l'intelligence artificielle, les commissaires souhaitent favoriser l'émergence de dispositifs « éthiques » (GEHN IA, 2019), un enjeu central dans l'acceptabilité sociale de ce type de technologie. En effet, la façon dont sont développés les algorithmes, selon les données de départ sur lesquelles ils s'appuient, contribue à la formation de « biais », qui reflètent en réalité des inégalités sociales et les représentations des individus qui développent ces algorithmes : par exemple, les visages utilisés pour entrainer les algorithmes surreprésentent les hommes ou les individus blancs. Pour cette raison, les algorithmes reconnaissent jusqu'à présent moins bien les femmes ou les personnes noires (Buolamwini, 2017). Ces biais, parfois difficiles à établir, peuvent poser de graves problèmes si la reconnaissance faciale est utilisée à des fins sécuritaires, puisqu'une correspondance peut être détectée alors qu'il ne s'agit pas de la bonne personne, ce qui conduit notamment au sur-contrôle des groupes les moins bien reconnus, comme les hommes noirs (Fussey et Murray, 2019), déjà sur-ciblés par les contrôles policiers (Jobard et al., 2012). La Commission européenne insiste ainsi sur l'importance de créer des algorithmes « éthiques », en recourant par exemple à des bases de données représentant les différents visages de la population, notamment en termes de genre et d'ethnicité[12], une solution technique envisageable à terme.

Les JOP, comme la Coupe du monde de rugby, fournissent ainsi une occasion unique de tester ces dispositifs, sur une masse importante de personnes. Cet enjeu est souligné par le terme « accélérateur » pour l'industrie de la sécurité, régulièrement utilisé dans les communications des groupes d'intérêt à ce sujet. Cette 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 »[13]. Cet appel « Flash » porte sur des projets menés par un consortium constitué d'au moins un organisme de recherche public ou assimilé et une société commerciale. Il comporte cinq thématiques privilégiées : Alerte aux populations (du haut vers le bas) ; Remontée d'alerte par la population (du bas vers le haut) ; Gestion des mouvements de foules, à partir du support d'un système de vidéosurveillance ; Gestion et contrôle des itinéraires (dont voies olympiques) ; Contrôle et surveillance de zones réservées.

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

[9] https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf
[10] https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf
[11] https://www.laquadrature.net/2019/12/19/rf_securitaire/
[12] P. 19, https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en
[13] https://anr.fr/fr/actualites-de-lanr/details/news/lancement-des-projets-laureats-de-lappel-a-projets-flash-jop24/#

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. »[14] 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 »[15]. 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.

« La sécurité des grands évènements, qu'ils soient sportifs (JO, mondiaux, etc.), culturels (grands concerts), diplomatiques (G7, G20), ou autres » (CNI, 2020, p. 9) est ainsi présentée comme un secteur en croissance. L'avènement des JOP en 2024 occasionne une forte mobilisation, sur les plans légaux et de l'expérimentation de nouveaux dispositifs, dans l'optique de structurer la filière et de renforcer la compétitivité des entreprises françaises dans ce domaine, en particulier la gestion de foules.

2 Les « safe cities » : expérimentations et approches

Des projets divers voient le jour dans différentes métropoles en France : Nice, Marseille, Saint-Étienne, etc. Ces projets sont souvent très médiatisés, et leur politisation contribue aux luttes politiques 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 (Cardon, 2015). Le recours à ces dispositifs s'inscrit en outre dans des configurations locales et des rapports de pouvoir préexistants (Baudot, 2015 ; Bigo et Bonelli, 2019), opposant différents groupes professionnels (cadres municipaux, forces de l'ordre publiques, entreprises de gardiennage, bailleurs sociaux) qui contribuent à produire des usages très différenciés d'une même technologie (Lemaire, 2019), souvent loin des promesses initiales.

Il ne s'agit donc pas ici d'interroger l'efficacité de ces technologies ou leur mise en œuvre effective, mais d'examiner qui contribue au développement des dispositifs numériques de sécurité pour les espaces urbains ? En effet, ces dispositifs sont développés dans des cadres et entreprises très divers. Or, la diversité des pratiques « prétendant dire et faire la sécurité » (Guittet, 2016) au sein des entreprises privées est rarement étudiée en elle-même, alors que celles-ci mêlent des entreprises du secteur des NTIC, comme ATOS, ou de la défense, comme Thales. Que nous apprend donc la diversité des dispositifs et des entreprises qui les développent ?

[14] *Ibid.*
[15] *Ibid.*

L'expérimentation de projets de sécurité numérique dans les métropoles

Afin d'examiner les différents dispositifs mis en œuvre en France, ainsi que les entreprises investies dans ce marché, on propose d'examiner les expérimentations de projets de sécurité numérique pour l'espace urbain dans des métropoles. Ces dispositifs concernent des projets différents : démonstrateurs « safe city » ou dispositifs mutualisant un ensemble de services urbains, dont la sécurité ; expérimentations ou mise en œuvre pérenne ; vidéosurveillance ou plateformes d'analyse de données ; espaces publics ou espaces gérés de façon privée (type métro francilien ou gares), etc. En outre, ces projets ne sont pas toujours publicisés et il peut être difficile de connaître précisément les entreprises impliquées, la nature exacte du dispositif choisi. Ces éléments doivent donc être gardés en mémoire dans l'analyse qui suit.

Encadré 2. Méthodologie du recueil de données sur les projets de dispositifs numériques de sécurité dans les métropoles

Les données présentées ici sont issues de sources variées, de trois types. D'abord, une dizaine d'entretiens réalisés avec des représentants « collectivités » ou « sécurité » de certaines entreprises participant à des projets de sécurité dans l'espace urbain. Ces entretiens sont anonymisés ici. Ensuite, les données recueillies par les membres participant à la campagne Technopolice[16], portée notamment par des associations de défense des libertés publiques. Ceux-ci recensent ces projets et ont réalisé des demandes d'accès aux documents administratifs permettant d'obtenir des échanges mail entre collectivités et entreprises, des contrats et conventions, etc.

Finalement, ces informations sont complétées par une revue de presse et l'analyse des brochures de présentation de leur offre de « safe city » de dizaines d'entreprises (récupérées sur leurs sites) et de magazines d'associations sectorielles. Ont été utilisés par exemple la brochure *Pixel*, éditée chaque année par l'AN2V, l'Association nationale de la vidéoprotection, ainsi que la brochure *Safe city*, réalisée par le GICAT, qui représente les intérêts des industriels français de la Défense et de Sécurité terrestres et aéroterrestres ; la FIEEC, qui rassemble 22 syndicats professionnels dans les secteurs industriels et technologiques de l'électricité, de l'électronique, du numérique et des biens de consommation. Tous deux sont membres du Conseil des Industries de la Confiance et de la Sécurité (CICS), qui a également participé à la réalisation de cette brochure, avec le Comité de la filière industrielle de sécurité (CoFIS). Ces brochures présentent des études de cas spécifiques ou les entreprises y mentionnent leurs « références », c'est-à-dire les collectivités ayant accueilli leurs produits et services. Ces informations permettent de connaître des projets autrement peu médiatisés. Ont été exclues des données présentées les entreprises dont l'offre était constituée seulement de vente de caméras ou autres objets électroniques.

Certains projets présentés ici ont été avortés en raison de procédures judiciaires, à l'instar de la mise en œuvre de reconnaissance faciale dans des lycées à Nice et à Marseille par Cisco. D'autres projets, comme celui d'IBM pour le programme Cité Intelligente à Montpellier, qui comprenait un module de gestion transversale des risques, étaient des expérimentations qui sont désormais terminées. Ils sont toutefois mentionnés car ils témoignent de la mobilisation de ces collectivités comme des entreprises mentionnées dans le domaine de la sécurité numérique pour l'espace urbain. À l'inverse, certains projets comme l'expérimentation de reconnaissance faciale dans un stade à Metz ne sont pas inclus, car il ne s'agit pas d'espaces d'accès public.

Une analyse de réseau est réalisée afin d'examiner quelles métropoles sont concernées par les projets de sécurité numérique pour l'espace urbain et quelles entreprises investissent ce domaine (voir

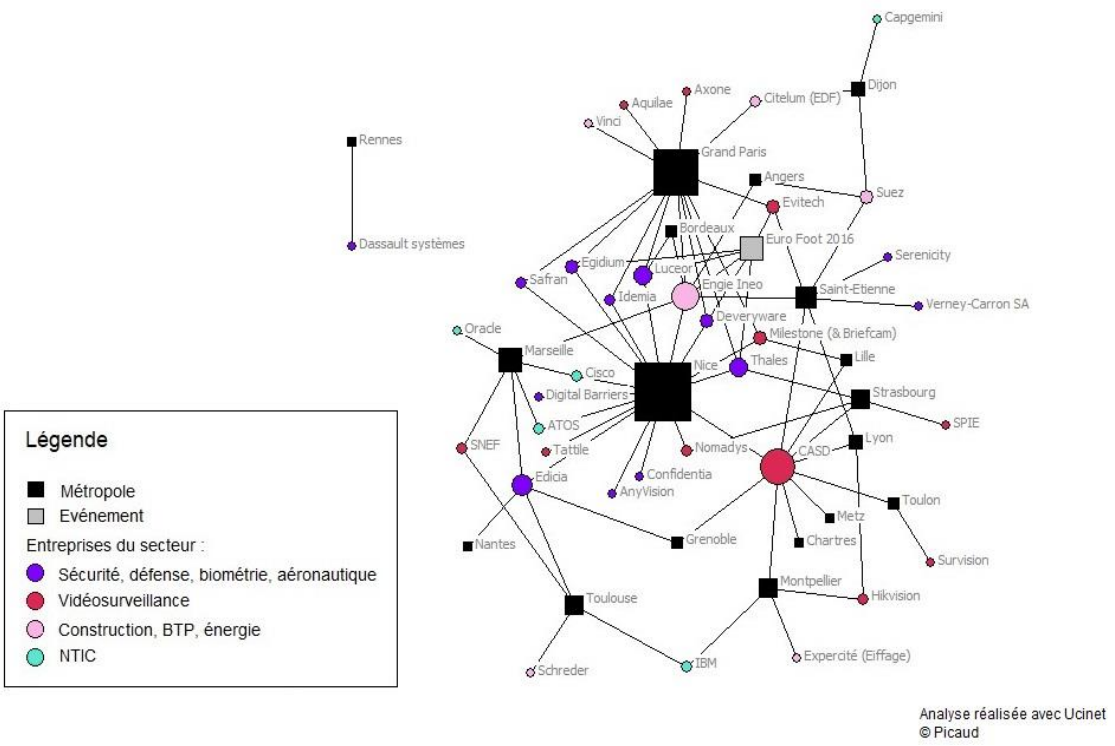
Figure 3 ci-dessous). Les liens concernent les projets ayant lieu dans une même métropole. Ils concernent 18 métropoles, sur les 22 existantes (en comptant le Grand Lyon malgré son statut particulier). Ils ne sont toutefois pas nécessairement mis en œuvre à l'échelle de l'ensemble de la

[16] https://technopolice.fr/villes/

métropole ni par la Métropole. Par exemple, les projets cités pour le Grand Paris concernent à la fois la Défense, ou encore les espaces gérés par la RATP. De même, l'implantation de Briefcam (entreprise rachetée par Milestone) dans la métropole lilloise concerne la ville de Roubaix, où elle propose de l'analyse algorithmique d'images de vidéosurveillance. Le choix des métropoles découle toutefois du fait que de nombreux projets en dépendent ou sont développés à cette échelle.

Finalement, l'Euro de football de 2016, dont les compétitions se sont tenues dans différentes métropoles, a été intégré à l'analyse afin de montrer le rôle joué par les grands événements dans le développement de dispositifs numériques. Si l'Euro s'est tenu dans différentes villes, il semblerait que la plupart des projets de sécurité numérique aient concerné les « Fan zones » situées en région parisienne.

Figure 3. Analyse de réseaux bipartis des entreprises et métropoles développant des projets de sécurité numérique pour l'espace urbain, selon le secteur d'activité principal des entreprises et la centralité de degré



Exemple de lecture : la SNEF, active dans le domaine de la vidéosurveillance, Schreder, une entreprise dans le secteur de l'éclairage (*smart lighting*), IBM, dans le secteur des NTIC, et Edicia, du secteur de la sécurité, développent ou ont développé des projets de sécurité numérique dans la métropole toulousaine.

Cette analyse de réseaux bipartis montre d'abord d'une densité de liens relativement faible (0,12). Cela témoigne d'un marché en construction, encore peu concentré, qui relève pour l'instant souvent d'expérimentations de projets plutôt que de leur mise en œuvre généralisée. L'isolement de projets dans plusieurs métropoles éclaire également les tentatives d'entrée dans ce marché (français) de certaines entreprises, à travers des démonstrateurs destinés à prouver leur savoir-faire. C'est le cas aussi dans des villes qui n'apparaissent pas ici, car il ne s'agit pas de métropoles, à l'instar de Valenciennes. Dans cette dernière, l'entreprise chinoise Huawei (Artigas, 2019), très

performante dans le domaine de la reconnaissance faciale, aurait offert à la municipalité 240 caméras d'une valeur de deux millions d'euros[17]. Certaines métropoles apparaissent quant à elles relativement périphériques – il s'agit le plus souvent de celles (ou des villes) gouvernées depuis longtemps par des partis de gauche. Il se peut également que certaines données manquent à l'analyse présentée ici, nombre de projets de développant de façon relativement confidentielle.

On constate néanmoins la centralité de certaines métropoles dans la mise en œuvre de projets de sécurité numérique pour l'espace urbain. La métropole de Nice est celle dont la centralité de degrés est la plus importante, suivie du Grand Paris, qui arrive en second malgré le rôle de capitale de la Ville de Paris, le statut particulier de la Préfecture de Police, et surtout un nombre (plus de 7 millions de personnes) et une densité de population exceptionnels, avec une forte concentration de l'activité économique. À titre de comparaison, la métropole de Nice comprend environ 540 000 habitants, mais la volonté politique y est très forte dans le domaine de la sécurité. En termes de centralité de degré, on trouve ensuite l'Euro de football, puis les métropoles de Marseille, Toulouse, Saint-Étienne, Montpellier et Strasbourg, puis Lyon et Dijon.

Dans les deux métropoles (pour le Grand Paris le projet prend pour objet le quartier de la Défense), un même consortium d'entreprises, porté par Thales, développe un démonstrateur de « safe city ». Les 15 entreprises[18] ne sont pas inclues dans l'analyse de réseau, qui ne retient que les plus centrales : Safran, Idemia, Thales, Deveryware, Egidium et Luceor. 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. À Nice, le projet 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. »[19]

La Ville de Nice, qui coordonne le 13e partenariat de l'Agenda urbain de l'Union européenne dédié à la sécurité urbaine, 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 »[20]. Des entreprises utilisent également des solutions d'analyse algorithmique d'images, comme Nomadys en partenariat avec CASD. En 2019, la reconnaissance

---

[17] https://www.europe1.fr/societe/valenciennes-huawei-a-offert-240-cameras-de-surveillance-a-la-ville-3943387

[18] 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).

[19] https://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/

[20] https://www.edicia.fr/clients

faciale y est expérimentée lors du Carnaval de Nice, sur des volontaires, avec l'entreprise israélienne de reconnaissance faciale AnyVision et Confidentia, entreprise de cybersécurité basée à Monaco. Sandra Bertin, directrice de la police municipale de Nice, affirme à ce propos :

> « La visée est scientifique, mais avec pour but évidemment, d'obtenir une réflexion commune. Une réflexion aujourd'hui de nos parlementaires, du gouvernement, qu'ils puissent se servir de cette expérimentation, en disant, en en tirant des conséquences : est-ce que c'est probant ; est-ce que ça ne l'est pas. Si c'est probant, dans quelle mesure ; ça ne l'est pas, dans quelle mesure. Si on avait la possibilité d'inscrire demain les personnes qui sont fichées au motif de radicalisation à caractère terroriste, et bien on aurait l'opportunité de pouvoir suivre en temps réel leurs déplacements et de pouvoir ainsi se prémunir, en les interdisant par exemple d'approcher les zones de grands rassemblements. »[21]

Les élus et représentants des forces de sécurité de la Ville de Nice, touchée en 2016 par un attentat ayant fait 86 morts, auquel cette directrice de la police municipale aurait assisté en direct derrière les caméras de vidéosurveillance, 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. »[22]

Dans d'autres métropoles, 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.

Si les attentats ont accéléré la mise en œuvre d'expérimentations de projets de « safe city » ou de vidéosurveillance « intelligente », l'enjeu sécuritaire était un enjeu politique déjà présent à Nice comme dans les autres collectivités locales (Freyermuth, 2013 ; Mucchielli, 2010, 2012). L'orientation politique des élus des collectivités semble influer sur l'investissement dans les projets de sécurité numérique pour l'espace urbain : les élus des villes et métropoles de Nice, Marseille, Saint-Étienne, Angers, Toulouse, Chartres et Metz (depuis 2020) sont à droite (principalement Les Républicains), de même que le Président de la métropole du Grand Paris. Traditionnellement plutôt à droite, la Ville de Bordeaux a élu un maire EELV en 2020 et la métropole est désormais dirigée par un élu PS. De même, la Ville de Marseille est passée à gauche en 2020. Les élus de la Ville de

[21] Propos retranscrits par l'auteure, énoncés dans le documentaire de Sylvain Louvet, *Tous surveillés : 7 milliards de suspects*, France, 2019.
[22] *Ibid.*

Paris, ainsi que de Nantes et Montpellier (ville et métropole), sont quant à eux affiliés au Parti Socialiste, alors qu'à Grenoble ce sont les Verts, tout comme à Strasbourg et à Lyon depuis 2020.

En ce qui concerne les entreprises, on observe la centralité de CASD et d'Engie Ineo, toutes deux très implantées dans la gestion de systèmes urbains de vidéosurveillance, et secondairement d'Edicia, qui propose principalement des services de « smart police », en France et dans d'autres pays comme les États-Unis. Apparaissent toutefois de nombreuses entreprises, issues de secteurs divers, ce qui témoigne de l'éclatement relatif de ce marché : BTP, construction, énergie ; NTIC, vidéosurveillance « classique » ; sécurité, défense et biométrie. Cette diversité d'entreprises apparaissait dès la fin des années 1990 :

> « L'offre des technologies de communication est largement aux mains de grands opérateurs de réseaux interconnectés sur le plan national (tels France Telecom, EDF, GDF), ou d'acteurs de réseaux additionnés (tels que Générale des Eaux, Bouygues et Philips, Lyonnaise des Eaux, Schlumberger). Ces groupes privés sont en concurrence sur les téléservices et cherchent à faire vivre des filiales en les spécialisant exclusivement dans la télésurveillance et dans la télésécurité, dans la mesure où ils parient sur des marchés rentables. » (Ocqueteau, 2004a, p. 117)

Les entreprises du secteur de la vidéosurveillance et de la défense et sécurité apparaissent les plus nombreuses dans ce domaine, contrairement à celles du secteur du BTP, construction, énergie (en dehors d'Engie Ineo, filiale d'Engie) ou encore des NTIC. La présence d'entreprises issues du secteur de la défense et de la biométrie, principalement françaises, telles que Thales, Dassault Systèmes, Verney-Carron, Idemia (initialement Morpho, rachetée par un fond états-unien), est toutefois fortement liée à la sécurité de grands événements, comme l'Euro 2016, qui a permis de tester différents dispositifs de sécurité en s'appuyant sur la gestion des « Fan Zones ». Celles-ci ont constitué une innovation, par la délimitation de périmètres de sécurité et la gestion privée de ces espaces, sécurisés grâce à la collaboration entre police nationale, polices municipales, agents de sécurité privée et dispositifs numériques, à l'instar d'Event Monitor, proposé par Egidium. À l'instar des JOP, cet événement semble ainsi avoir offert un terrain d'expérimentation pour la mise en œuvre de dispositifs de sécurité et la collaboration entre différentes entreprises dans ce domaine, avant une mise en œuvre dans des espaces urbains. Les entreprises du secteur de la défense sont aussi présentes par le biais du projet de « safe city développé récemment à Nice et dans le quartier de la Défense. Cela témoigne de leur entrée relativement récente dans ce marché, à l'inverse de celles du secteur traditionnel de la vidéosurveillance, l'offre de certaines, tout en restant relativement basique, s'étant adaptée en intégrant des propositions « smart » au fur et à mesure de l'évolution technologique dans ce domaine.

Approches différenciées de la sécurité urbaine

Les dispositifs mis en œuvre par les entreprises divergent. D'abord, parce que la temporalité de leur utilisation n'est pas toujours la même. Elle peut se faire en amont, pour l'aménagement urbain, en temps réel ou a posteriori (par exemple pour élucider une affaire). Ensuite, les types de dispositifs varient et proposent différentes formes de sécurité. Les plateformes de centralisation et d'analyse de données côtoient le contrôle de la circulation routière, des dispositifs liés au cadre de vie, tels que la lumière « intelligente » (qui s'allume de façon adaptative). Des applications numériques sont destinées aux forces de l'ordre ou aux résidents. Des logiciels de modélisation des flux piétons peuvent permettre d'anticiper des situations d'urgence et influer sur les plans d'aménagement urbain. À cela s'ajoute la vidéosurveillance (ou audiosurveillance) dite « intelligente », qui peut

s'appuyer sur l'identification d'objets (colis abandonnés), de situations « anormales » (au sens statistique du terme, inhabituelles), la détection d'intrusions dans des zones limitées, la lecture de plaques d'immatriculation, l'identification de personnes, l'analyse de comportements voire celle d'expressions ou d'émotions exprimées par les visages.

Néanmoins, un même dispositif peut également présenter des différences liées à l'approche spécifique des membres de l'entreprise, selon son secteur d'origine, leurs liens avec les représentants des pouvoirs publics, les collaborations passées avec les métiers de la sécurité et en particulier les forces de l'ordre publiques. Trois discours de représentants « collectivités » ou « smart city » dans des entreprises liées pour l'une aux NTIC, pour la seconde aux services urbains et pour la troisième à la sécurité, sont reproduits ci-après (voir Encadré 3). Ils portent tous sur le développement de dispositifs de sécurité numérique, en particulier des plateformes d'analyse de données et de l'analyse « intelligente » de vidéosurveillance, pour des collectivités en France ou à l'étranger. Ces extraits d'entretien témoignent de la diversité d'approches d'un même dispositif.

Encadré 3. Discours sur la sécurité numérique de responsables « collectivités » de trois entreprises de la sécurité, des NTIC et des services urbains

Entreprise dans le domaine des NTIC, à propos d'une collectivité dans un autre pays européen

« Pour la police municipale, ce qu'on a fait pour eux, c'est qu'on a récupéré les informations venant des caméras vidéo installées, les caméras image, les caméras son […]. Et puis également toutes les informations qu'on a traitées de manière anonyme, sur les réseaux sociaux. Et notamment pour tous ceux qui se donnent rendez-vous à tel endroit, "tiens, on se retrouve à tel endroit à 19h". **Donc en croisant toutes ces informations avec les modèles mathématiques, on a mis au point un système qui permet en fait à coup sûr à la police municipale de prévoir là où il risque d'y avoir des attroupements. Et des risques**. Donc… donc on a aidé le client à choisir en amont quel type de données il fallait prendre, où les prendre. Donc une fois qu'on a dit ça, et bien il faut monter tout le système c'est-à-dire **récupérer l'information image, l'infirmation son, l'information des réseaux sociaux, il faut à un moment donné les rendre compatibles dans des formats, etc.** On monte ça dans une plateforme. Une plateforme c'est des matériels informatiques, avec des serveurs assez puissants. […] On réunit toutes ces données et après on les traite pour donner en sortie un tableau de bord, pour la police municipale, pour qu'elle sache où positionner les troupes, quelques heures avant le match et quelques heures après le match. […] C'est évolutif et c'est du quasi… **c'est pas du temps réel parce que c'est de l'anticipation**, mais c'est de la gestion de données de haut débit. » *(Responsable « collectivités territoriales » d'une entreprise des NTIC, entretien à Paris le 08.10.2019)*

Entreprise dans le domaine des services urbains

« En fait la Ville voulait s'assurer que… l'ensemble des mécanismes et moyens, organisations, qui étaient faits pour… je dirais, assurer la [sécurité], n'étaient pas décalés par rapport à la réalité de ce qui allait se passer. **Le problème, c'est qu'on tombe un peu dans le prédictif**. C'est-à-dire qu'à un moment donné, pour être très bons sur la gestion d'un incident, il faudrait connaître l'incident avant qu'il arrive, ce qui est pas logique, parce que ça arrive rarement, sinon ça se saurait. *Retour vers le futur*, ce n'était qu'un film. Donc là on a un objet […] avec un maximum de données sur plein de choses, petit à petit, selon le type de sujets… parce que c'est pas la même chose si c'est un événement, si c'est le stade de foot qui se remplit, c'est pas la même chose que si c'est une manif', etc. Donc y'a plein de sous-cas particuliers. **On commence à optimiser les mécanismes qui sont en jeu dans… quelle est la circulation qu'il faut faire, ou interdire, ou etc., quels sont les meilleures rondes policières, à quels endroits il risque d'arriver quoi ?** Donc, on a des *prédictions*, on peut quand même les appeler comme ça, qui sont pas si mauvaises sur des risques d'accidents, des risques de mouvements de foule, enfin selon ce que c'est, évidemment ! Et c'est ça, petit à petit qu'on a construit, à partir de tout hein. Y'a des données twitter, comme y'a des données météo, comme y'a des données… de mains courantes de la police, enfin on en a… […] Des algorithmes

qui permettent de dire, attention à ce carrefour-là, y'a plus de chances d'avoir un accident un lendemain – qu'est-ce que c'est qu'on avait trouvé ? Un lendemain de match de foot s'il a plu. Pourquoi, je suis pas devin, j'en sais rien, mais il se trouve que c'est vrai. » *(Entretien avec un directeur dans le domaine « smart city » et innovation d'une grande entreprise de services urbains, à Paris le 07.03.2019)*

Entreprise dans le domaine de la sécurité

« On fait une cartographie de ce qu'on appelle les *pains*, le client, c'est quoi ses problèmes aujourd'hui et on regarde si on sait les résoudre. Et après on essaie de dire comment on peut les résoudre. Est-ce qu'on peut, et comment. **Et dans le comment, y'a nous comme monde de technologie, mais y'a vous aussi, qui devez vous coordonner entre vous**. Donc est-ce que c'est mieux que les pompiers causent avec les gendarmes, est-ce qu'il vaut mieux que votre opérateur qui regarde la caméra là, il faut qu'il change dans sa façon de faire la ronde, et pour qu'il change il faudrait qu'on lui donne des *inputs* pour lui dire regarde là et là, et aujourd'hui il le fait à la main ou il est habitué à regarder que la caméra, ou quand il a le temps. Donc y'a une phase d'observation et de discussion. […] C'est quoi qu'il faut déployer, y'a-t-il une zone sensible, si c'est autour d'un stade de foot, oui effectivement on va mettre plus, mais faudra pas se tromper que le stade de foot est alimenté par une rue, une grande artère, ils arrivent par là donc faut anticiper, parce qu'une fois qu'il sont là c'est trop tard. Donc faut anticiper. Donc y'a toute cette démarche là en termes d'ingénierie. C'est-à-dire que déployer un système ce n'est pas mettre des boites et du logiciel. **C'est aussi savoir comment ces boites et ces logiciels sont utilisés et éventuellement comment on complète ce qu'ils font de base pour amener à une réponse.** […] **La techno propose mais à un moment donné aussi il faut qu'elle soit en adéquation avec les usages, avec ce qu'il est possible de faire et avec le raisonnable quoi.** Si on met trois heures à rentrer dans le stade parce que y'a de la sécurité partout… on tue le stade. Au bout d'un moment aussi. Donc faut aussi trouver le juste milieu. » *(Directeur de branche « collectivités territoriales », entreprise dans le secteur de la sécurité, entretien à Paris le 22.10.2019)*

Que révèle la comparaison de ces présentations de dispositifs de sécurité numérique ? Les deux premiers témoignent d'une approche centrée sur l'analyse de données à visée prédictive. Le croisement de données massives, issues de différentes sources publiques comme privées (entrées d'hôpitaux, police, météo, trafic routier, données sociodémographiques de type INSEE, réseaux sociaux, etc.), permettrait d'établir des corrélations afin de parvenir à une gestion optimisée, plus efficiente, des forces de sécurité. Les recherches sur les professionnels de la sécurité témoignent effectivement de l'usage de dispositifs numériques à des fins de rationalisation de l'action publique davantage que de surveillance (Castagnino, 2018) : par exemple, l'utilisation d'un algorithme destiné à prédire où et quand les crimes sont susceptibles de se dérouler sert principalement à gérer les patrouilles de police (Benbouzid, 2018) ou de gendarmes (Gosselin, 2019), en ciblant les espaces à surveiller en priorité. Les algorithmes d'analyse des données peuvent alors être issus des sciences de la nature, comme c'est le cas pour l'application Predpol, utilisée par les forces de l'ordre états-uniennes, qui s'appuie sur un modèle initialement destiné à la sismologie (Benbouzid, 2017). Ces algorithmes sont aussi de façon croissante issus de l'analyse de données en ligne, développés par des entreprises des NTIC, selon un des enquêtés[23].

On retrouve dans les deux premiers discours une approche plutôt techno-centrée, qui considère l'optimisation de la sécurité sous l'angle de la prédiction des risques et d'un gouvernement par la performance (Bezes, 2020) qui s'appliquerait à la gestion des espaces urbains. Ce point de vue est cohérent avec l'ancrage sectoriel des deux entreprises, l'une dans les NTIC et l'autre concernant une filiale numérique d'une entreprise de services urbains. Elle s'ancre également dans la trajectoire

[23] « Aujourd'hui, tout ce qu'il y a, ça s'inverse, y'a plutôt du grand public qui va vers le militaire. Enfin […], les Facebook et autre, ils sont plutôt grand public. » *(Directeur de branche « collectivités territoriales », entreprise dans le secteur de la sécurité, entretien à Paris le 22.10.2019)*

de ces deux responsables, diplômés de l'Université en sciences de la nature avec une spécialisation dans l'informatique ou le traitement d'images, et ayant ensuite travaillé dans des entreprises liées aux NTIC.

Le dernier extrait d'entretien témoigne quant à lui d'une approche un peu différente, liée à l'ancrage dans le secteur de la sécurité et de la défense de l'entreprise. L'enquêté, ingénieur de formation, a réalisé sa carrière au sein de celle-ci, initialement dans le développement d'algorithmes et la biométrie, avant de devenir responsable de ligne produit. L'attention de l'enquêté à l'enjeu de la coordination des forces (publiques et privées) de sécurité est un marqueur important de sa position sectorielle. Il se détache d'une analyse techno-centrée, en positionnant l'expertise de son entreprise dans la capacité à identifier précisément les enjeux locaux de sécurité, à coordonner les différents acteurs, mais aussi à proposer des dispositifs qui s'inscrivent dans les usages concrets des agents qui les utiliseront ensuite. Or, cette question apparaît très secondaire, voire inexistante dans le discours des autres enquêtés, par qui le monde de la sécurité semble moins bien connu, notamment ses enjeux autour des compétences de chaque groupe professionnel et les luttes autour de celles-ci.

L'approche présentée par le troisième enquêté témoigne aussi de l'importance de la dimension de gestion de crise, marquée par les pratiques du secteur de la défense, dans laquelle il est central que la coordination des différents groupes soit efficace en cas de problème. Celle-ci est déployée de façon prioritaire, par rapport à la dimension prédictive des dispositifs évoqués par les deux autres enquêtés, dont l'efficacité en termes de réduction des crimes et délits, ou de gestion des foules, n'est pour l'instant pas vérifiée. Néanmoins, le positionnement d'entreprises du secteur de la sécurité et défense comme orchestrateurs de la coordination entre différentes entités publiques (administrations des collectivités territoriales, forces de l'ordre, etc.) doit interroger sur la place centrale que leur offrent la gestion et définition de ces plateformes dans le gouvernement urbain. L'étude empirique de cas précis, des configurations et rapports de force dans le développement et la mise en œuvre de ces projets, devra éclairer ces questions.

S'opposent ainsi deux visions de la sécurité, l'une d'elles davantage centrée sur la prédiction et la rationalisation de la gestion des forces de sécurité, l'autre sur leur coordination et la mise en œuvre de protocoles de gestion de situation spécifiques (matchs, manifestations, etc.). Ces deux approches semblent relever de deux secteurs différents, celui des NTIC et l'analyse de mégadonnées, et celui de la sécurité et défense. L'usage quotidien de ces dispositifs dans la gestion urbaine doit ainsi être exploré plus avant, à travers des études de cas localisées, afin de mieux comprendre de quelles façons cela transforme (ou non) les pratiques des agents concernés. Comme le soulignait Frédéric Ocqueteau, à propos de l'investissement de la vidéosurveillance par des entreprises issues de secteurs divers, et notamment des services urbain : « [c]onvaincre un client de mobiliser des technologies nouvelles à son profit, et cela est tout aussi vrai pour les polices publiques, les élus locaux ou les particuliers, n'est pas suffisant si l'on ignore parallèlement les efforts d'adaptation des utilisateurs ou usagers potentiels aux contraintes matérielles et aux investissements de sens et de pratiques qu'ils mettent dans ces technologies coûteuses pour leur organisation ou leurs administrés. » (Ocqueteau, 2004a, p. 117)

Concurrencées par des entreprises issues du secteur de l'énergie, des services urbains et des NTIC, les entreprises du domaine de la sécurité ont donc investi cette dimension numérique, employant également des dispositifs issus de la défense (algorithmes de reconnaissance d'objets,

cryptographie, etc.), appliqués au secteur urbain et alliant leur « connaissance métier » à de nouvelles compétences. Celles-ci peuvent être mises en œuvre dans des projets à travers des partenariats, comme c'est le cas dans le projet « SafeCity » à Nice et à la Défense, auxquels collaborent de nombreuses entreprises. Elles peuvent également être acquises par le rachat d'entreprises, comme Thales l'a fait. Le groupe, au chiffre d'affaires de 18,4 milliards d'euros en 2019, a investi plus d'un milliard d'euros en Recherche & Développement, a créé des Digital Factory à Paris, Montréal et Singapour, destinées à favoriser le développement de produits en interne. Le groupe a également consacré plus de 5 milliards d'euros aux acquisitions d'entreprises depuis 2017, comme celle de Gemalto (gestion de l'identité des personnes et objets et sécurité numériques) en 2019. Il est aujourd'hui leader mondial dans le domaine de l'identité et sécurité numériques, exclusivement dans le domaine civil.

3 Enjeux urbains du déploiement 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 (CNIL, 2018 ; McGregor, Murray et Ng, 2019 ; Scheinin et Sorell, 2015), une question à laquelle s'est également intéressée la Commission Européenne. Les commissaires souhaitent effectivement favoriser l'émergence de dispositifs « éthiques » (GEHN IA, 2019), un enjeu central dans leur acceptabilité sociale. D'autres chercheurs ont examiné la façon dont les inégalités sociales se traduisaient par des biais dans le fonctionnement des algorithmes. Des travaux sur le développement de technologies numériques décrivent plus généralement l'avènement d'un capitalisme de la surveillance (Masutti, 2020 ; 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 revient ici sur quelques-uns de ces enjeux : les transformations de l'aménagement urbain ; le ciblage d'espaces particuliers par ces dispositifs ; le ciblage de certains modes d'occupation de l'espace.

Transformations des espaces urbains

La littérature sur les dispositifs de sécurité revient sur deux formes idéal-typiques de transformations de l'espace 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 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). Quels peuvent être les effets du recours aux dispositifs de sécurité, sur ces formes de mise en visibilité et de clôture de l'espace ?

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. Celle-ci autorise la création de périmètres lors de grands événements jugés « à risque », au sein desquels la police et/ou des agents de sécurité privée peuvent inspecter ou fouiller personnes et véhicules. Ces dispositifs, qui augmentent les coûts d'organisation, conduisent aussi à faire payer l'entrée pour des manifestations auparavant gratuites.

Le recours à ces dispositifs est ainsi susceptible d'être associé à des formes de clôture et de segmentation de l'espace urbain, qui permettent de mieux gérer les circulations grâce à des dispositifs de surveillance à distance. 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 peut encourager à les maintenir et donc s'inscrire de façon durable dans l'espace urbain :

> « Pour les JO […], l'investissement doit être durable. En clair, ou s'il est pas durable, il faut qu'il soit au regard de ce qu'on y met, mais pas qu'il reste à la fin des JO des trucs dont on ne sait plus que faire. La sécurité après les JO doit rester aussi, donc faut être capable justement de les déployer à la demande pour les réactiver quand on en aura besoin et pas quelque chose qui va être installé à demeure et qui servira une fois tous les 18 mois, auquel cas c'est pas rentable. » *(Directeur de branche « collectivités territoriales », entreprise dans le secteur de la sécurité, entretien à Paris le 22.10.2019)*

Cette question se pose ainsi pour la mise en œuvre de sécurité numérique dans le Village Olympique, situé dans la ville de Saint-Denis, dont les résidents appartiennent en grande partie aux classes populaires. La mise en œuvre de dispositifs de sécurité, coûteux et potentiellement durables, tels que la reconnaissance faciale, devrait ainsi faire l'objet d'un débat politique.

Finalement, 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. C'est ce que montre la mise en œuvre par la London Metropolitan Police d'un dispositif de reconnaissance faciale, étudiée par deux chercheurs (Fussey et Murray, 2019, p. 101), à l'entrée du centre commercial Westfield Stratford : les individus refusant de consentir à ce dispositif doivent le contourner en marchant 1,3 km, ou passer par le métro souterrain (et donc valider un ticket).

Le ciblage différencié des espaces urbains

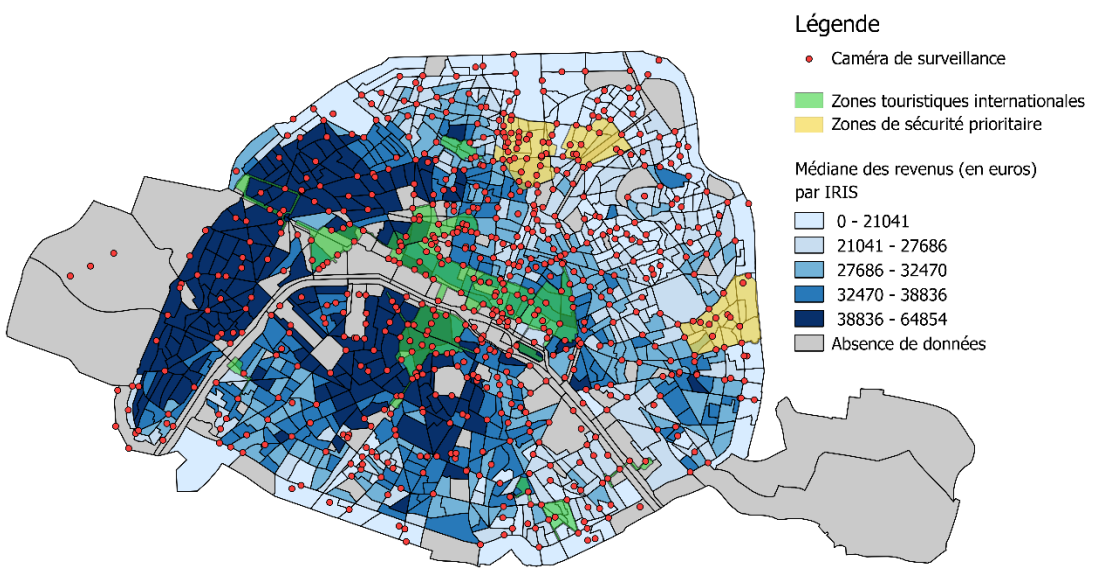
La mise en œuvre de la sécurité numérique dans les espaces urbains doit aussi interroger quels types d'espaces ils ciblent. À Saint-Étienne, le projet (finalement annulé) d'installation de micros intelligents, destinés à repérer des situations anormales, des coups de feu, etc., concernait un quartier populaire et était soutenu par des subventions de l'ANRU.

De quelles façons la sécurité contribue aux mutations urbaines et aux inégalités sociospatiales ? Différents travaux peuvent être relus sous cet angle. Ainsi, des phénomènes de ségrégation et d'entre-soi (Cousin, 2014 ; Oberti et Préteceille, 2016), dans lesquels la recherche de sécurité contribue à la segmentation de l'offre au sein du marché immobilier et à des formes de clôture urbaines, à l'image des résidences fermées (Elguezabal, 2015 ; Glasze, Webster et Frantz, 2005). Les mobilisations politiques de résidents dans les processus de gentrification (Collet, 2015 ; Tissot,

2011) ou face aux projets de rénovation urbaine (Epstein, 2013) et commerciale (Hubbard, 2017), témoignent également du rôle de la sécurité dans les transformations de l'aménagement et de la composition socio-spatiale des espaces urbains. Mais qu'en est-il des dispositifs de sécurité numérique ? Les quartiers populaires et leurs résidents sont-ils davantage ciblés par les dispositifs de sécurité numérique ?

En l'absence de données précises sur les dispositifs numériques de sécurité, les enquêtes sur la géographie de la vidéosurveillance peuvent fournir quelques hypothèses. L'une d'entre elles, à Bruxelles, témoigne du ciblage des quartiers accueillant les institutions européennes, dans le centre, ainsi que des quartiers populaires, avec une part importante de population immigrée, tels que Molenbeek (De Keersmaecker et Debailleul, 2016). À Londres, la mise en œuvre de reconnaissance faciale dans l'espace public par la London Metropolitan Police ciblait principalement le centre-ville, des centres commerciaux, des zones de sortie nocturne (Fussey et Murray, 2019).

Carte 1. Caméras de vidéosurveillance à Paris selon les revenus des résidents et les zones touristiques et de sécurité



Sources : Données de la Préfecture de Police (2019), du Ministère de l'Économie (2018) et de l'INSEE (2014)
Carte réalisée avec Quantum GIS
© Picaud

La cartographie des caméras de surveillance de la Préfecture de police à Paris (voir Carte 1 ci-dessus) témoigne plutôt de la concentration des caméras dans les quartiers du centre et les zones touristiques, ainsi que dans l'une des zones de sécurité prioritaire, celle qui s'étend sur les quartiers Barbès - Goutte d'Or, La Chapelle - Marx Dormoy, et Château Rouge – Marcadet. Ceux-ci accueillent des populations aux revenus plus faibles que dans le reste de la capitale, et sont également très fréquenté par des populations immigrées ou d'origine étrangère, issues en particulier de pays du continent africain (Chabrol, 2013). Cette zone de sécurité comprend aussi la Gare du Nord. D'autres quartiers accueillant des groupes sociaux moins dotés apparaissent quant à eux peu

surveillés, quoiqu'il serait intéressant d'avoir ces données pour le Grand Paris plutôt que pour la seule capitale afin de pouvoir approfondir cette analyse.

On peut donc émettre l'hypothèse que les dispositifs de sécurité se concentrent en priorité dans des zones centrales, où la circulation de personnes est forte, par exemple en raison de nœuds de transports, de centres commerciaux, de zones touristiques, etc. Le recours aux dispositifs numériques pourrait être ciblé sur la gestion de flux importants d'individus, dans des espaces où leur nombre rend plus complexe la gestion par des agents humains, en particulier lorsque le ralentissement de la circulation occasionne trop de coûts, notamment économiques (par exemple, retard ou arrêt d'un métro, d'un train, etc.). Ce constat serait certainement renforcé si les caméras de surveillance installées par des entités privées (commerces, RATP, etc.) étaient incluses dans cette carte. La mise en œuvre de projets de « safe city », comme celui de Nice, plutôt dans le centre-ville, ou de la Défense, ainsi que l'expérimentation de vidéosurveillance « intelligente » dans la station centrale Châtelet de la RATP tendent également à soutenir cette hypothèse, qui demande toutefois à être vérifiée par des enquêtes approfondies. On pourrait alors se demander quelle division du travail s'opère entre dispositifs numériques de sécurité et de surveillance, et présence des forces de l'ordre publiques et d'agents de sécurité privée, dans les quartiers centraux, commerciaux et d'affaires, d'une part, et populaires, d'autre part.

Modes d'occupation de l'espace public

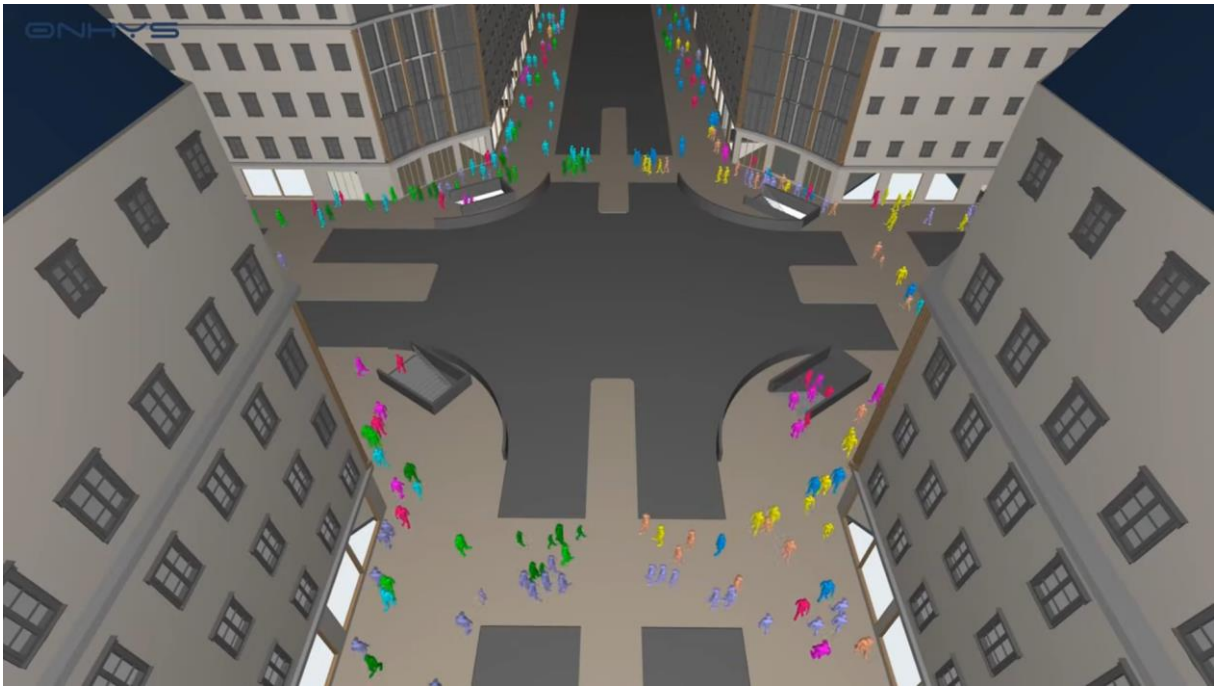
La mise en œuvre de dispositifs numériques dans l'espace public est également susceptible d'influer sur l'appropriation de celui-ci par différents groupes sociaux. On revient ici sur un aspect, la présence de groupes dans l'espace public. La gestion de foules, comme on l'a vu à propos des JOP de 2024, 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 19e siècle (Le Bon, 2013).

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 (sauf lorsqu'ils patientent à un passage piéton), 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 4 ci-dessous).

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 (Clerval, 2011). 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. Ces éléments, comme l'auto-organisation d'espaces commerciaux, tels que les *Business Improvement Districts* (*BID*s) anglo-américains[24] (Steel et Symes, 2005), ou la sécurisation des gares (Bonnet, 2012), éclairent les liens qui unissent sécurité des villes et développement économique local.

Figure 4. Exemples de simulations de flux piétons pour la gestion urbaine, par l'entreprise Onhys



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

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

[24] Les *BID*s, répandus au Royaume-Uni ou aux États-Unis, sont des organisations regroupant les propriétaires immobiliers de quartiers commerciaux afin d'améliorer les conditions d'activité. Elles prélèvent une taxe destinée à financer des services, notamment de sécurité privée.

> opposants peuvent conduire à la violence ou même à des attaques terroristes. En raison du mouvement des parades urbaines et des manifestations (ci-après abrégé par UPM) à travers une grande partie des villes, il est particulièrement difficile pour les forces de sécurité civile (en abrégé ci-après par FCS) de garantir la sécurité dans ce type d'évènements urbains sans mettre en danger l'un des indicateurs les plus importants d'une société libre. […] 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. Les méthodes seront applicables à la préparation et l'organisation de UPMs, ainsi qu'à la gestion de situations critiques d'UPMs ad hoc ou pour faire face à des incidents inattendus. »[25]

Ces questions, déjà investies auparavant, ont connu un regain d'intérêt encore plus fort 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[26], 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 qui peuvent circuler ensuite à d'autres contextes, avec des implications politiques très différentes. Cela témoigne également de la stigmatisation de l'occupation de l'espace public par des groupes, organisés ou non, perçus comme des risques et des menaces.

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, ainsi qu'aux inégalités dans la façon dont sont sécurisés les différents espaces et ciblés les groupes qui y résident.

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. La construction de ce marché est investie en premier lieu par les acteurs du marché de la sécurité et la défense, mais aussi par des grands groupes des NTIC et des services urbains. Leurs approches de la sécurité urbaine sont différentes. Les représentants des pouvoirs publics, à l'échelle locale, nationale et européenne, sont eux aussi parti

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

[26] 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.

prenantes du développement de ce marché, qui recouvre aussi des enjeux politiques, électoraux et de développement économique. Les grands événements, tels que les JOP, offrent un terrain d'expérimentation, de structuration de la filière et aussi une possibilité de faire évoluer le cadre légal, qu'investissent les groupes d'intérêt, représentants des entreprises et des pouvoirs publics. Des associations de défense des libertés publiques s'attachent néanmoins à lutter contre cela.

Si les enjeux autour des libertés publiques sont souvent évoqués à propos de la sécurité numérique pour l'espace urbain, cela est plus rarement le cas pour les enjeux proprement urbains du recours à ces dispositifs. Quoique cette réflexion appelle à la réalisation d'enquêtes empiriques sur la mise en œuvre locale de projets spécifiques, trois enjeux ressortent néanmoins de l'analyse : les transformations de l'aménagement urbain, avec des formes de clôture de l'espace ; le ciblage d'espaces particuliers par ces dispositifs, notamment les lieux de passage, parmi lesquels les centres-villes, quartiers commerciaux et d'affaire ; le ciblage de certains modes d'occupation de l'espace, avec la stigmatisation des groupes, en particulier dans le cas de manifestations. Ces éléments pointent la façon dont la sécurité numérique s'inscrit dans une forme de rationalisation de la gestion des espaces urbains, destinée à assurer les circulations de biens et de personnes et l'activité économique, par leur contrôle. Sans aller jusqu'à y voir un urbanisme militaire (Graham, 2010), croisé avec une disneyfication des villes (Shearing et Stenning, 1984), 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.

Bibliographie

ABDELNOUR S., MEDA D., 2019, *Les nouveaux travailleurs des applis*, Paris, Presses Universitaires de France.

ABRAHAMSEN R., WILLIAMS M.C., 2009, « Security Beyond the State: Global Security Assemblages in International Politics », *International Political Sociology*, *3*, 1, p. 1-17.

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

AN2V, 2020, « Pixel 2020. Le guide de la vidéoprotection », Paris, Association nationale de la vidéoprotection.

ARTIGAS A., 2019, « Beneath the surface of the Safe City: surveillance in the times of Chinese supremacy? », *Working paper de la chaire « Villes et numérique »*, 01/2019, Paris, Sciences Po, Ecole urbaine.

AVANT D.D., 2005, *The market for force: The consequences of privatizing security*, Cambridge University Press.

BARNS S., 2020, *Platform Urbanism: Negotiating Platform Ecosystems in Connected Cities*, Palgrave Macmillan (Geographies of Media).

BAUDOT P.-Y., 2015, « La donnée et le système. Comment socialiser un instrument d'action publique ? Le cas du système d'information partagé-personnes handicapées (2006-2014) », *Gouvernement et action publique*, *2*, 2, p. 25-56.

BENBOUZID B., 2017, « Des crimes et des séismes », *Reseaux*, *n° 206*, 6, p. 95-123.

BENBOUZID B., 2018, « Quand prédire, c'est gérer », *Réseaux*, *211*, 5, p. 221-256.

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

BETIN C., MARTINAIS E., RENARD M.-C., 2003, « Sécurité, vidéosurveillance et construction de la déviance : l'exemple du centre-ville de Lyon », *27*, 1, p. 3-24.

BEZES P., 2020, « Le nouveau phénomène bureaucratique. Le gouvernement par la performance entre bureaucratisation, marché et politique », *Revue française de science politique*, *70*, 1, p. 21-47.

BIGO D., BONELLI L., 2019, « Nous ne sommes pas un Big Brother ! », *Cultures & Conflits*, *114-115*, 2, p. 199-226.

BODY-GENDROT S., 2012, *Globalization, Fear and Insecurity - The Challenges for Cities North and South*, Basingstoke, Palgrave Macmillan.

BONNET F., 2012, « Contrôler des populations par l'espace ? Prévention situationnelle et vidéosurveillance dans les gares et les centres commerciaux », *Politix*, *97*, 1, p. 25-46.

BOURDIEU P., 2000, *Les Structures sociales de l'économie*, Paris, Seuil.

BRAYNE S., 2017, « Big Data Surveillance: The Case of Policing », *American Sociological Review*, *82*, 5, p. 977-1008.

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.

CARDON D., 2015, *À quoi rêvent les algorithmes. Nos vies à l'heure des big data*, Paris, Le Seuil.

CASTAGNINO F., 2018, « Critique des surveillances studies. Éléments pour une sociologie de la surveillance », *Deviance et Societe*, *Vol. 42*, 1, p. 9-40.

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.

CHABROL M., 2013, « Continuités d'usages et maintien d'une centralité commerciale immigrée à Château-Rouge (Paris) », *Les Annales de la recherche urbaine*, 108, p. 97–107.

CLERVAL A., 2011, « L'occupation populaire de la rue : un frein à la gentrification ?: L'exemple de Paris intra-muros », *Espaces et sociétés*, *144-145*, 1, p. 55-71.

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

CNIL, 2018, *Rapport d'activité 2017. Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*, Paris, Commission nationale de l'informatique et des libertés.

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

COLLET A., 2015, *Rester bourgeois : Les quartiers populaires, nouveaux chantiers de la distinction*, Paris, La Découverte.

COLLOVALD A., 2001, « Des désordres sociaux à la violence urbaine », *Actes de la recherche en sciences sociales*, *136-137*, 1, p. 104.

COUSIN B., 2014, « Entre-soi mais chacun chez soi », *Actes de la recherche en sciences sociales*, *204*, 4, p. 88-101.

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

DE KEERSMAECKER P., DEBAILLEUL C., 2016, « Répartition géographique de la vidéosurveillance dans les lieux publics de la Région de Bruxelles-Capitale », *Brussels Studies. La revue scientifique électronique pour les recherches sur Bruxelles / Het elektronisch wetenschappelijk tijdschrift voor onderzoek over Brussel / The e-journal for academic research on Brussels*.

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

DECISION ETUDES & CONSEIL, 2019, « L'Observatoire de la filière de la Confiance Numérique », Paris, Alliance pour la Confiance Numérique.

DUBUISSON-QUELLIER, S. (dir.), 2016, *Gouverner les conduites*, Paris, Presses de Sciences Po.

EGBERT S., 2019, « Predictive Policing and the Platformization of Police Work », *Surveillance & Society*, *17*, 1/2, p. 83-88.

ELGUEZABAL E., 2015, *Frontières urbaines. Les mondes sociaux des copropriétés fermées*, Rennes, Presses Universitaires de Rennes.

EPSTEIN R., 2013, *La rénovation urbaine. Démolition-reconstruction de l'État*, Paris, Presses de Sciences Po.

FLIGSTEIN N., 2001, *The Architecture of Markets: An Economic Sociology of Twenty-First Century Capitalist Societie*, Princeton, Princeton University Press.

FRANÇOIS P., 2007, « Le marché et le politique: Le rôle de l'action publique dans le développement du monde de la musique ancienne », *Revue française de science politique*, *57*, 5, p. 629.

FREYERMUTH A., 2013, « L'offre municipale de sécurité : un effet émergent des luttes électorales. Une comparaison des configurations lyonnaise, niçoise, rennaise et strasbourgeoise (1983-2001) », *Revue internationale de politique comparée*, *20*, 1, p. 89-116.

FUSSEY P., MURRAY D., 2019, « Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology », Essex, University of Essex.

GAUTRON V., MONNIAUX D., 2016, « De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme », *Archives de politique criminelle*, 38, p. 123-135.

GAYET-VIAUD C., 2017, « French Cities' Struggle Against Incivilities: from Theory to Practices in Regulating Urban Public Space », *European Journal on Criminal Policy & Research*, *23*, 1, p. 77-97.

GEHN IA, 2019, « Lignes directrices en matière d'éthique pour une IA digne de confiance », Rapport du Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle constitué par la Commission Européenne en Juin 2018, Bruxelles, Commission Européenne.

GERMAIN S., DOUILLET A.-C., DUMOULIN L., 2012, « The Legitimization of Cctv as a Policy Tool: Genesis and Stabilization of a Socio-Technical Device in Three French Cities », *British Journal of Criminology*, *52*, 2, p. 294-308.

GLASZE G., WEBSTER C., FRANTZ K., 2005, *Private Cities: Global and Local Perspectives*, Londres, Routledge.

GORMAND G., 2017, *L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier*, thesis, Grenoble Alpes.

GOSSELIN C., 2019, *La police prédictive: enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique*, Paris, Institut d'aménagement et d'urbanisme de la région d'Île-de-France.

GRAHAM S., 2010, *Cities under siege: the new military urbanism*, Londres, Verso.

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

GUITTET E.-P., 2016, « Approches méthodologiques de la sécurité : engagements, obstacles et défis . Introduction », *Cultures & Conflits*, 102, p. 7-15.

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

HIBOU B., 1998, « Retrait ou redéploiement de l'État ? », *Critique internationale*, *n° 1*, 4, p. 151-168.

HUBBARD P., 2017, *The Battle for the High Street*, Londres, Palgrave Macmillan UK.

JOBARD F., LEVY R., LAMBERTH J., NEVANEN S., 2012, « Mesurer les discriminations selon l'apparence : une analyse des contrôles d'identité à Paris », *Population*, *67*, 3, p. 423–451.

JONES C., 2017, « Market Forces. The Development of the EU Security-Industrial Complex », The Transnational Institute.

JONES T., NEWBURN T., 1998, *Private Security and Public Policing*, Oxford, Clarendon Press.

LAKOFF A., KLINENBERG E., 2010, « Of risk and pork: urban security and the politics of objectivity », *Theory and Society*, *39*, 5, p. 503-525.

LE BON G., 2013, *Psychologie des foules*, Paris, Presses Universitaires de France.

LE GOFF T., 2005, « L'insécurité "saisie" par les maires. Un enjeu de politiques municipales », *Revue française de science politique*, *55*, 3, p. 415-444.

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

MAGNON-PUJO C., 2011, « La souveraineté est-elle privatisable ? », *Politix*, *95*, 3, p. 129-153.

MAILLARD J. DE, ZAGRODZKI M., 2015, « Plural Policing in Paris. Cooperation and Differentiation », *Policing and Society*, *25*, 2.

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.

MASUTTI C., 2020, *Affaires privées. Aux sources du capitalisme de surveillance*, C&F Editions.

MCGREGOR L., MURRAY D., NG V., 2019, « International Human Rights Law as a Framework for Algorithmic Accountability », *International and Comparative Law Quarterly*, *68*, 2, p. 309-343.

MUCCHIELLI L., 2010, « «Insécurité»,«sentiment d'insécurité»: les deux veines d'un filon politique », *Après-demain: journal mensuel de documentation politique*, *16*, p. 3–6.

MUCCHIELLI L., 2012, *Vous avez dit sécurité ?*, Champ social.

OBERTI M., PRETECEILLE E., 2016, *La ségrégation urbaine*, Paris, La Découverte.

OCQUETEAU F., 2004a, *Polices entre État et marché*, Paris, Presses de Sciences Po.

OCQUETEAU F., 2004b, « Chapitre 3. Definir et compter des hommes, des services, des entreprises », *Academique*, p. 75-111.

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

PENTLAND A., 2013, « The data-driven society », *Scientific American*, *309*, 4, p. 78-83.

PICAUD M., 2020, « « Smart cities » ? Le marché des dispositifs numériques pour l'espace urbain en France », Working Paper de la chaire « Villes et numérique », Paris, Sciences Po, Ecole urbaine.

RENOU X., 2005, *La Privatisation de la violence. Mercenaires et sociétés militaires privées au service du marché*, Marseille, Agone.

ROCHE S., 2004, *Sociologie politique de l'insécurité. Violences urbaines, inégalités et globalisation*.

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).

SHAW C., 1968, *The Natural History of a Delinquent Career*, 2e édition, New York, Greenwood Press Publishers.

SHEARING C., STENNING P., 1984, « From the Panopticon to Disney World: The development of discipline », dans DOOB A., GREENSPAN E. (dirs.), *Perspectives in Criminal Law*, Aurora, Canada Law Book, p. 335-349.

STEEL M., SYMES M., 2005, « The Privatisation of Public Space? The American Experience of Business Improvement Districts and their Relationship to Local Governance », *Local Government Studies*, *31*, p. 321-334.

THRASHER F.M., 1929, *The Gang*, Chicago, University of Chicago Press.

TISSOT S., 2007, *L'État et les quartiers. Genèse d'une catégorie de l'action publique*, Paris, Seuil.

TISSOT S., 2011, *De bons voisins. Enquête dans un quartier de la bourgeoisie progressiste*, Paris, Raisons d'agir.

TOWNSEND A.M., 2013, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*, New York, W. W. Norton & Company.

VAN DIJCK J., 2014, « Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology », *Surveillance & Society*, *12*, 2, p. 197-208.

WARFMAN D., OCQUETEAU F., 2011a, *La sécurité privée en France*, Paris, Presses Universitaires de France.

WARFMAN D., OCQUETEAU F., 2011b, « Annexe I – Étapes historiques de la réglementation des activités de la sécurité privée », *Que sais-je ?*, p. 119-122.

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.

Liste des figures

Figure 1. Budgets et chiffres d'affaire des secteurs public et privé de la sécurité en 2016 8
Figure 2. Entreprises dominantes de la filière dite « Confiance numérique » selon la nationalité 9
Figure 3. Analyse de réseaux bipartis des entreprises et métropoles dans les projets de sécurité numérique pour l'espace urbain, selon le secteur d'activité principal des entreprises et la centralité de degré 17
Figure 4. Exemples de simulations de flux piétons pour la gestion urbaine, par l'entreprise Onhys 28

Liste des encadrés

Encadré 1. La reconnaissance faciale 13
Encadré 2. Méthodologie du recueil de données sur les projets de dispositifs numériques de sécurité dans les métropoles 16
Encadré 3. Discours sur la sécurité numérique de responsables « collectivités » de trois entreprises de la sécurité, des NTIC et des services urbains 21

Liste des cartes

Carte 1. Caméras de vidéosurveillance à Paris selon les revenus des résidents et les zones touristiques et de sécurité 26