Villes sous contrôle et technologisation du maintien de l'ordre. Entretien avec Félix Tréguer

Marion Lecoquierre, Félix Tréguer

Carnets de géographes

15 | 2021
Les dimensions spatiales du maintien de l'ordre

Villes sous contrôle et technologisation du maintien de l'ordre. Entretien avec Félix Tréguer

Marion Lecoquierre et Félix Tréguer

Édition électronique
URL : https://journals.openedition.org/cdg/6846
ISSN : 2107-7266

Éditeur
UMR 245 - CESSMA

Référence électronique
Marion Lecoquierre et Félix Tréguer, « Villes sous contrôle et technologisation du maintien de l'ordre. Entretien avec Félix Tréguer », *Carnets de géographes* [En ligne], 15 | 2021, mis en ligne le 30 avril 2021, consulté le 18 mai 2021. URL : http://journals.openedition.org/cdg/6846

Villes sous contrôle et technologisation du maintien de l'ordre. Entretien avec Félix Tréguer

Marion Lecoquierre et Félix Tréguer

NOTE DE L'ÉDITEUR

Entretien mené le 4 septembre 2020 par Marion Lecoquierre, mis à jour par échanges de mails jusqu'en janvier 2021.

1 Le maintien de l'ordre passe de plus en plus par l'intermédiaire de technologies qui permettent une surveillance élargie de l'espace, notamment urbain, ainsi que des personnes : vidéosurveillance, reconnaissance faciale, détection de sons et de mouvements, logiciels de police prédictive, etc. Si ces nouvelles technologies sont parfois présentées comme des outils prometteurs qui permettent de faciliter le travail des forces de l'ordre et d'en renforcer l'efficacité, elles sont également dénoncées comme autant de menaces pour la vie privée et les libertés des citoyens, leur foisonnement dans l'espace urbain se faisant souvent hors de tout réel contrôle démocratique.

2 De nombreux évènements récents - le mouvement des Gilets jaunes, la crise sanitaire du Covid-19, les manifestations contre les violences policières et contre la Proposition de loi sur la sécurité Globale, entre autres - ont mis ces questions au centre du débat public en 2020.

3 Nous avons souhaité discuter de ces sujets avec Félix Tréguer, chercheur en Sciences politiques et activiste de La Quadrature du Net, une association de lutte pour les libertés numériques, afin d'approfondir les enjeux de cette technologisation du maintien de l'ordre.

MARION LECOQUIERRE : BONJOUR FÉLIX !

Félix Tréguer : Bonjour !

TU ES CHERCHEUR, ACTUELLEMENT POST-DOCTORANT À SCIENCES PO EN SCIENCES POLITIQUES, SPÉCIALISTE DES QUESTIONS DE COMMUNICATION ET NOTAMMENT D'INTERNET, ET TU T'INTÉRESSES PLUS PARTICULIÈREMENT AUX QUESTIONS DE SURVEILLANCE DU PUBLIC ET DE L'ESPACE PUBLIC PAR LES INSTITUTIONS ÉTATIQUES. DE QUELLE MANIÈRE LA DIMENSION SPATIALE DU MAINTIEN DE L'ORDRE APPARAÎT-ELLE DANS TON TRAVAIL ?

Depuis 2013-2014, suite aux révélations du lanceur d'alerte Edward Snowden[1], j'ai travaillé sur les controverses associées à la surveillance d'Internet par les services de renseignement. Cela m'a amené à m'intéresser plus généralement à la question de la surveillance, à son histoire comme pratique d'État et à son rôle dans la régulation de l'espace public. Dans le cadre de ma thèse, j'ai essayé de réinscrire ces enjeux dans une histoire du temps long pour voir comment l'espace public médiatique a été contrôlé par l'État depuis l'apparition de l'imprimerie, en identifiant différentes époques et les évolutions dans les stratégies de contrôle de l'espace public – qu'elles passent par le recours à la surveillance, à la censure, à la propagande, au secret ou par la centralisation des moyens de communication. L'espace public médiatique peut être pensé comme un dispositif de pouvoir, où la distribution des rôles, du droit à s'exprimer et à être reconnu comme légitime, est déterminé par la topologie de l'espace public – son caractère plus ou moins concentré, plus ou moins distribué, plus ou moins démocratique –, topologie qui est elle-même conditionnée par le droit, les propriétés techniques associées aux moyens de communication, et bien d'autres paramètres. L'espace public médiatique a sa géographie propre. Mais son histoire est aussi intimement liée à celle de l'espace public urbain.

C'est ce que montre Dominique Reynié dans son livre intitulé *Le triomphe de l'opinion publique* (1998). Il y rappelle que la consécration de l'espace public médiatique à travers le droit libéral et la protection de la liberté d'expression est aussi une manière de confiner le conflit politique au débat d'idées, et donc de désamorcer la puissance subversive potentielle de l'espace public urbain. Du point de vue du pouvoir, ce dernier est toujours apparu comme plus dangereux parce que c'est l'espace du peuple et pas simplement de l'opinion publique abstraite, des idées : c'est l'espace où les corps assemblés créent un rapport de force direct. En libéralisant l'espace public médiatique, le pouvoir se serait ainsi offert la latitude de corseter l'espace public urbain pour tenter de le neutraliser en tant que terrain d'affrontement politique, afin d'éviter que le peuple rassemblé ne devienne une force politique à même de le menacer dans un corps à corps direct.

Les exemples abondent mais les débats autour de la loi de 1881 sur la liberté de la presse offrent une bonne illustration de ce processus : lors des débats législatifs autour de cette loi, la question de la frontière entre le dire et le faire est centrale. On va par exemple réprimer beaucoup plus durement des discours dont on estime qu'ils peuvent inciter à l'action directe. Typiquement, les chants populaires – dont les parlementaires estiment qu'ils pourraient exciter le peuple et l'amener à des formes de violence politique – sont plus sévèrement réprimés que les infractions commises par voie de presse. C'est l'une des nombreuses illustrations de cet impératif que constitue, pour les autorités, la pacification et la domestication des formes d'expression politique dans l'espace public urbain. L'histoire du droit de manifestation et de son encadrement relève de logiques similaires.

Ces dernières années, c'est d'abord par le militantisme que j'en suis venu à m'intéresser à la surveillance de l'espace urbain. Depuis 2009, je suis engagé dans *La Quadrature du Net*, une association de défense des libertés publiques dans l'environnement numérique – et historiquement principalement sur Internet. Depuis 2015, on a beaucoup travaillé sur toutes les législations antiterroristes, les lois de surveillance comme la loi renseignement, ou encore le recul des libertés publiques liées à l'état d'urgence et la manière dont celui-ci a pu être utilisé aussi pour museler la liberté d'expression et de manifestation, notamment au travers des assignations à résidence, lesquelles ont aussi visé des militants écologistes[2]. C'est dans ce contexte que l'on s'est progressivement rendu compte que les technologies de surveillance informatiques utilisées par les États ou les grandes entreprises sur Internet étaient en train d'être appropriées à des fins de police urbaine.

CE DÉPLOIEMENT CROISSANT DE TECHNOLOGIES DE SURVEILLANCE DANS L'ESPACE PUBLIC URBAIN EST SOUVENT DIRECTEMENT LIÉ À (ET JUSTIFIÉ PAR) UNE MODIFICATION DES MODALITÉS ET DES CAPACITÉS DU MAINTIEN DE L'ORDRE. PEUX-TU NOUS FAIRE UN RAPIDE HISTORIQUE DES TECHNOLOGIES ACTUELLEMENT EMPLOYÉES ET DÉVELOPPÉES EN FRANCE ET DE LEUR UTILISATION ?

L'informatisation de la police date des années 1960-1970 – c'est-à-dire au début du mouvement d'informatisation des bureaucraties d'État. Elle se traduit notamment par l'informatisation des bases de données et des fichiers de police, mais aussi, déjà, par l'expérimentation, aux États-Unis, d'algorithmes censés prédire le crime en fonction des zones géographiques[3]. Dans les années 1990, ce processus de « mise en données » de l'activité policière évolue en réponse aux thèses du « nouveau management public » (Eterno, Silverman, 2012). Le logiciel CompStat, déployé par la police new-yorkaise en 1994 pour collecter et comparer systématiquement les statistiques à la fois sur la criminalité et sur la réponse policière apportée, va devenir un symbole de cette « politique du chiffre ». C'est aussi l'époque où « l'intelligence-led policing » devient à la mode, principalement aux États-Unis. L'idée sous-jacente, c'est que la police ne doit plus simplement réagir à la criminalité, mais qu'elle doit l'anticiper et la préempter dans une démarche de gestion des risques.

À partir des années 1990, on voir aussi s'engager une multiplication des capteurs vidéo dans l'espace public. En France, la vidéosurveillance commence à se développer à partir de 1993, sous l'impulsion de responsables politiques de droite comme Charles Pasqua, et dans un premier temps souvent à l'initiative d'élus locaux, comme Patrick Balkany à Levallois-Perret. Comme aujourd'hui avec les nouvelles technologies de surveillance urbaine, l'arrivée de la vidéosurveillance suscite la controverse, et des résistances d'organismes comme la Commission nationale de l'informatique et des libertés (CNIL). Mais petit à petit, son usage fait tache d'huile. Dès 1995, on procède à quelques aménagements législatifs pour sécuriser ces déploiements sur le plan juridique. Ce n'est que des années plus tard, en particulier sous le quinquennat de Nicolas Sarkozy, qu'on verra la mise en place d'un véritable plan national concernant la vidéosurveillance, avec des financements publics très importants. Entre temps, les peurs initiales qui émergeaient dans l'opinion semblent pour l'essentiel avoir été résorbées.

Ce qui est remarquable avec la vidéosurveillance, c'est à quel point il s'agit d'une politique publique qui n'est pas évaluée. Depuis vingt ans que des dizaines et des dizaines de milliers de caméras sont installées sur le territoire par les pouvoirs

publics, l'investissement doit se chiffrer en milliards d'euros en équipement et en maintenance, mais on ne dispose d'aucun chiffre précis sur l'argent public dépensé pour ces technologies. Pour donner un exemple, les cinq cents dernières caméras de surveillance en cours d'installation à Marseille ont coûté plus de 46 millions d'euros, soit trois fois le montant annoncé au départ[4]. En aval, la capacité de la vidéosurveillance à atteindre les objectifs que lui assignent ses promoteurs n'est pas non plus évaluée. À travers des enquêtes indépendantes mais forcément partielles, le sociologue Laurent Mucchielli (2018) parle de résultats dérisoires, évoquant notamment le chiffre de 3 % d'enquêtes sur des faits de délinquance « ordinaire » où les images de vidéosurveillance joueraient un rôle « important » (mais pas forcément décisif), ce qui est très faible. Dans son rapport sur les polices municipales, publié en novembre 2020, la Cour des Comptes rappelle d'ailleurs le manque d'études statistiques et d'évaluations indépendantes sur le sujet, tout en affirmant qu'« aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation » (Cour des Comptes, 2020 : 70).

ET OÙ EN EST-ON ACTUELLEMENT ?

Ces dernières années, ces différentes approches technopolicières ont été réactualisées à l'aune des évolutions technologiques, notamment en matière de stockage et d'analyse de grandes masses de données (ce qu'on appelle le Big Data) et des techniques dites d'intelligence artificielle.

Une partie de ces nouvelles technologies vise à automatiser certaines fonctions via « l'apprentissage machine » – par exemple pour apprendre aux programmes informatiques à reconnaître certaines catégories d'événements à partir par exemple de flux de vidéosurveillance. On voit aujourd'hui se structurer un marché autour de ces nouvelles technologies à grand renfort de projets de recherche publique, de partenariats publics-privés et d'expérimentations locales. Par exemple, les programmes de vidéosurveillance automatisée (VSA) se multiplient, avec pour objectif d'analyser automatiquement les images de vidéosurveillance afin de repérer des événements « suspects » (par exemple à Marseille, le système envisagé permettrait de repérer automatiquement des individus qui réaliseraient des graffitis[5]) ou d'identifier des individus. Le principal lobby du secteur, l'Association nationale de vidéoprotection[6], explique aujourd'hui que l'automatisation doit permettre de faire face à l'ampleur des flux créés par ces dizaines de milliers de capteurs : puisque l'on ne dispose pas de suffisamment d'opérateurs humains pour scruter les écrans dans les centres de supervision urbains, il faudrait automatiser ce travail d'analyse en s'appuyant sur des algorithmes. On voit aussi se développer des capteurs sonores destinés à déclencher, selon la même logique, des alertes pour les forces de l'ordre en cas de bruit suspect.

Les solutions de police prédictives se développent également. On en est encore au stade de prototypes, mais il y a des entreprises comme Engie Ineo à Marseille qui travaille à un « Observatoire Big Data de la Tranquillité publique » pour croiser tout un tas de données issues de jeux de données des villes, de l'État mais aussi de partenaires privés comme les opérateurs télécoms ou les réseaux sociaux[7]. L'objectif est de produire des cartographies dynamiques et de faire des recommandations sur les tactiques, les stratégies de maintien de l'ordre, notamment en cas d'événement sur la voie publique. L'une des applications de cet outil consiste par exemple à

indiquer le parcours d'une manifestation revendicative dans le système pour que, après analyse de la couverture du parcours par les caméras de vidéosurveillance, l'algorithme déduise les endroits où des déploiements policiers seront le plus pertinents. Une autre société très présente sur le marché français est Sûreté Globale[8] qui travaille avec des villes comme Montpellier ou la Préfecture de police de Paris. Son produit phare, « Map Revelation »[9], est un logiciel qui, d'après son site web, « fournit des analyses prédictives, graphiques et géographiques, de semis de points » en fonction des données fournies (faits de délinquance, signalements à la police, mises en fourrière, vie associative, etc.). Dans le Livre blanc de la sécurité intérieure, publié le 16 novembre 2020, le Ministère de l'Intérieur appelle à généraliser ces outils d'analyse et de visualisation – qu'il baptise « infocentres » – dans le but d'« analyser les phénomènes rencontrés et ainsi orienter les actions futures ou mieux allouer les moyens » (Ministère de l'Intérieur, 2020 : 246).

ON ASSISTE AUSSI À L'EMPLOI DE PLUS EN PLUS FRÉQUENT DE DRONES.

En effet, les drones font aussi partie de ces nouvelles technologies qui sont en train de transformer le maintien de l'ordre. Ils ont été souvent utilisés par la police depuis 2014 dans le cadre des manifestations pour filmer les cortèges, repérer des gens dans la foule. Depuis quelques mois, notamment à l'occasion de la crise sanitaire, on assiste à la prolifération de ces outils. Ce fut par exemple le cas pour imposer les mesures de « distanciation sociale » entre mars et mai 2020. On peut analyser les drones comme une extension mobile et aéroportée de la vidéosurveillance, à l'image des caméras-piétons intégrées aux uniformes des policiers.

C'est l'ensemble de ces nouvelles technologies policières de surveillance qu'on essaye de documenter dans le cadre de la campagne « Technopolice » lancée en 2019 par *La Quadrature du Net*, en lien avec la *Ligue des Droits de l'Homme*. L'enjeu, c'est aussi de se donner les moyens de résister à cette fuite en avant techno-policière : après la mobilisation des Gilets Jaunes et la loi anti-manifestation du 10 avril 2019, l'État poursuit une stratégie de mise sous surveillance de l'espace public, et plus largement de toutes les formes d'expression politique – en particulier les manifestations.

La proposition de loi sur « la sécurité globale » relève de cette logique. Outre l'interdiction de la diffusion d'images qui permettraient l'identification de membres des forces de l'ordre, cette loi vise à légaliser l'emploi des drones ou des caméras-piétons, dont les flux pourront être croisés en temps réel avec les fichiers de police pour faire de la reconnaissance faciale et identifier les personnes, participe d'un grand chantier technologique et législatif qui va s'étaler sur plusieurs années. Le *Livre blanc de la sécurité intérieure* prévoit d'ailleurs une augmentation de 30 % du budget dévolu aux politiques de sécurité d'ici 2030, avec comme priorité de mobiliser ces financements pour « porter le Ministère de l'Intérieur à la frontière technologique » (Ministère de l'Intérieur, 2020 : 9).

TU ÉVOQUES LA « CAMPAGNE TECHNOPOLICE » : QUEL EST LE SENS QUE VOUS METTEZ DERRIÈRE CE TERME ET QUEL EST LE BUT DE CETTE INITIATIVE ?

Ce néologisme de « Technopolice » sert avant tout à pointer ce phénomène d'une technologisation croissante du travail policier en lien avec le développement des technologies informatiques - intelligence artificielle, Big Data, etc. Le terme de « Technopolice » renvoie à ce phénomène, et joue aussi avec l'homophonie du mot « police » pour renvoyer à la « polis », à la ville, parce que cette campagne s'intéresse

en premier lieu à la police urbaine. C'était donc aussi une manière de jouer sur l'étymologie commune de ces deux termes et de souligner la porosité entre le contrôle social policier et la ville, qui occupe une place particulière dans l'imaginaire politique et dans l'histoire de la démocratie, mais qui est aussi un lieu privilégié pour le déploiement de ces logiques technocratiques et déshumanisantes, liée à la dérive libérale-autoritaire du pouvoir.

Pour la petite histoire, le soir où on a réfléchi à ce nom de campagne, un ami de *La Quadrature du Net* propose le terme de Technopolice. Le lendemain, on regarde sur Internet s'il est déjà utilisé, et là le moteur de recherche nous renvoie vers des « rencontres technico-opérationnelles » organisées par le Ministère de l'Intérieur deux fois par an, et qui visent justement à débattre des usages des nouvelles technologies policières entre industriels et praticiens, policiers, gendarmes et responsables du Ministère de l'Intérieur. Mais pas grand-chose ne filtrait sur le contenu de ces journées. On trouvait que c'était un joli pied de nez que de reprendre ce terme et sa connotation angoissante pour notre campagne. Mais ce qui est encore plus drôle, c'est qu'en mai 2019 – on était à quelques mois du lancement de la campagne, on venait de déposer le nom de domaine technopolice.fr et on travaillait à définir son univers graphique– on reçoit un message d'invitation aux prochaines rencontres « Technopolice » du Ministère de l'Intérieur, organisées en septembre 2019 sur le thème de « l'acceptabilité sociale de la reconnaissance faciale »[10] ! Nous y sommes allés, et ce fut un moment de débat assez tendu, même si assez important pour nous dans la mesure où ça nous a permis d'avoir accès à des informations très précieuses sur les projets en cours[11]. Car c'est bien là le premier objectif de cette campagne : combattre l'opacité qui entoure ces projets.

La campagne « Technopolice », que pour ma part j'aborde comme un projet de recherche-action, résulte d'une urgence qui nous a sauté aux yeux fin 2017. À l'époque, on prend connaissance dans la presse du projet d'Observatoire Big Data à Marseille. Mais très vite, au gré de nos recherches, on se rend compte que ces enjeux ne sont pas du tout abordés dans le débat public ou dans les médias dominants, alors même qu'il y a plein de projets de ce type en cours de déploiement sur le territoire. À l'époque, les médias parlent de la reconnaissance faciale en Chine, de la police prédictive aux États-Unis, mais éludent complètement le fait que ces technologies et ces usages sont en train de s'établir en France.

Du coup, l'enjeu de cette campagne, ça a été de mettre en place une suite d'outils et quelques méthodes facilement reproductibles pour documenter ces projets – à l'image des demandes d'accès aux documents administratifs, les « demandes CADA » – et de construire des analyses et des argumentaires pour tenter de souligner leur danger et tous les enjeux politiques et juridiques qu'ils soulèvent. On a donc rédigé un manifeste pour expliquer le sens de notre opposition à ces déploiements, on a mis en place plusieurs de ces outils, notamment un forum public qui permet à des citoyens, des chercheurs, des journalistes de collaborer, d'échanger, de faire de la veille, de partager le fruit de leurs recherches pour documenter ces projets. Outre la documentation, l'objectif était aussi de permettre à des collectifs locaux de s'organiser, d'agir localement tout en ayant un espace commun où échanger sur les stratégies, sur les arguments à mobiliser.

Il s'agissait aussi de voir comment articuler ces combats locaux à une stratégie plus générale puisqu'il y a évidemment beaucoup d'interlocuteurs et d'enjeux qui se structurent au niveau national et au niveau de l'Union européenne[12], ne serait-ce que du point de vue juridique ou du point de vue des projets de recherche qui président au déploiement de ces technologies.

TU PARLAIS DE LABORATOIRES ET D'EXPÉRIMENTATIONS, DE PROJETS QUI SE METTENT EN PLACE EN FONCTION DES ÉVÈNEMENTS, AVEC LA CRISE SANITAIRE PAR EXEMPLE, ON VOIT QU'IL Y A DES MOMENTS QUI PEUVENT ÊTRE DÉCLENCHEURS POUR L'INTRODUCTION DE NOUVELLES TECHNOLOGIES.

Les crises – qu'elles soient par exemple antiterroristes ou sanitaires – sont des moments clés pour légitimer ces technologies policières et leurs usages. Mais outre les penchants sécuritaires voire autoritaires d'une partie des élites au pouvoir, ces déploiements sont aussi surdéterminés par des enjeux industriels. Nous assistons en Europe aux premières applications « grandeur nature » de ces technologies, mais en réalité, cela fait plus de dix ans que la recherche publique travaille à mettre au point des systèmes automatisés de gestion et d'aide à la décision, notamment dans le cadre des politiques urbaines – correspondant au projet de « *Smart City* » – et leur déclinaison sécuritaire – ce que les industriels appellent la « *Safe City* ». Par exemple, dans le cadre des projets de recherche européens, on voit des consortiums où des grandes multinationales comme Thales ou Idemia, s'allient avec des centres de recherche publique comme l'INRIA et à la Préfecture de police de Paris pour travailler à la reconnaissance faciale, au contrôle des foules, et d'autres applications de ce type.

Face aux contraintes légales qui, pour l'heure, limitent encore le déploiement de ces technologies en France, l'État a encouragé ces entreprises à tester leurs solutions de surveillance dans des régimes où la protection du droit à la vie privée est très mal assurée, comme en Chine ou à Taïwan, ou dans plusieurs pays africains[13]. Il s'agit d'une logique néocoloniale, malheureusement assez fréquente dans l'histoire de la surveillance : il faut se rappeler par exemple que la carte d'identité a d'abord été mise en place pour les populations indochinoises avant d'être proposée en France et finalement généralisée sous le gouvernement de Vichy[14]. Mais l'enjeu pour une partie de l'industrie européenne, c'est de présenter leurs solutions comme étant tout à fait acceptables en démocratie, y compris dans des régions qui sont censées disposer d'un haut niveau de protection des « données personnelles ». C'est notamment pour cette raison qu'aujourd'hui en France, on assiste à une vague d'expérimentation grandeur nature à l'échelle locale – c'est le cas des projets que je mentionnais tout à l'heure.

La plupart des programmes que nous documentons dans le cadre de la campagne Technopolice visent en réalité à permettre un apprentissage mutuel où collectivités locales et forces de l'ordre qui travaillent sur le terrain apprennent à collaborer avec les industriels qui développent ces technologies. Ces derniers peuvent travailler au plus près des praticiens et mieux intégrer les « processus métiers » dans leurs outils. Dans le même temps, ces collaborations leur permettent d'affiner le fonctionnement de leurs algorithmes à partir des systèmes informatiques et de bases de données utilisés sur le terrain par les forces de l'ordre. Les technologies ne sont à vrai dire pas encore très abouties ; on est au début d'une phase de test et de déploiement continu. Mais les crises à répétition risquent d'amplifier ces logiques. De fait, beaucoup des acteurs sur lesquels on travaillait depuis plusieurs mois ont profité de la crise sanitaire du printemps 2020 pour transformer un peu le cadrage marketing sur leurs

outils[15]. On a ainsi vu fleurir des systèmes de vidéosurveillance automatisée permettant de détecter le port ou le non-port du masque dans le métro parisien ou à Cannes notamment…

UN AUTRE ÉVÈNEMENT QUI FAIT ÉMERGER DE NOUVEAUX PROJETS TECHNOPOLICIERS, C'EST L'ORGANISATION DES JEUX OLYMPIQUES À PARIS EN 2024.

L'échéance des Jeux Olympiques en 2024 risque en effet d'accélérer ces déploiements. Le secteur industriel français se positionne, encouragé par le Ministère de l'Intérieur, pour développer de nouvelles technologies de maintien de l'ordre et de gestion des foules, et faire de cet événement une « vitrine » du savoir-faire français en la matière. Et là encore on assiste à la mise en route d'un cycle de recherche-développement lancé à grand renfort d'argent public. En février 2020, l'Agence nationale de la recherche (ANR) a retenu six projets visant à développer - je cite - les « meilleures solutions technologiques » pour répondre aux problématiques de sécurité que posent des évènements du type des Jeux Olympiques[16].

Parmi les projets retenus, il y a par exemple le projet « Discret », qui vise à démontrer « qu'il est possible de détecter en temps réel les situations atypiques ou critiques à travers l'analyse de données des opérateurs de téléphonie mobile », croisées avec les réseaux sociaux (ibid.). Un autre projet vise à simuler et analyser le comportement des foules ou des groupes au moyen de systèmes de vidéosurveillance automatisés, un autre à développer des systèmes d'identification et de contrôles d'accès biométrique low-cost pour permettre « l'accès différencié des individus à certaines zones réservées selon le niveau d'accréditation et de détecter les individus non habilités à circuler dans ces zones » (ibid.). Les Jeux Olympiques risquent fort de constituer un moment clé dans la légalisation et la normalisation de ce type de technologies et de leurs usages dans le cadre des politiques de sécurité.

CONCRÈTEMENT, QUE CHANGENT TOUTES CES TECHNOLOGIES AU MAINTIEN DE L'ORDRE, ET EN PARTICULIER AU RAPPORT À L'ESPACE DES FORCES DE L'ORDRE ET DES CITOYENS ?

Cette campagne « Technopolice » est née d'une urgence, et pour l'heure, je n'ai pas eu la possibilité de mener des enquêtes de terrain ou d'entretiens auprès des policiers qui expérimentent et utilisent ces technologies. On ne dispose pas non plus de bilans d'expérimentation, ni même des études d'impact liées à ces projets alors qu'elles sont pourtant exigées par le droit européen des données personnelles.

À ce stade, il est donc assez difficile de savoir ce que ça change en pratique. Ce qu'on anticipe, c'est la remise en cause du droit à la ville et l'aggravation des logiques technocratiques de surveillance, d'optimisation, d'organisation de l'espace imposées par les autorités. Il y a bien sûr des parallèles à faire avec d'autres moments de transformation urbaine extrêmement importants – je pense aux travaux d'Haussmann à Paris où, comme avec la « *Smart City* » aujourd'hui, il y avait déjà à la fois cette idée d'optimisation, mêlée à des considérations hygiénistes, économiques, de gestion du foncier, etc. Du point de vue strictement policier, de la même manière qu'Haussmann a fait percer des grands boulevards aussi pour permettre l'arrivée des troupes au cœur de Paris et mater les insurrections populaires, il y a dans les projets de « *Safe City* » cette même logique d'une surveillance par en haut, où l'infrastructure urbaine tout entière est conçue en fonction d'impératifs de maintien de l'ordre.

ET QUELS SONT LES PRINCIPAUX DANGERS DE CES PROCESSUS ?

Les dangers que l'on pointe ce sont des choses qu'on observe déjà dans les pays et dans les zones où ces technologies sont les plus utilisées, les plus mûres. Par exemple, une sur-policiarisation des quartiers déjà en proie à des formes de racisme systémique ou de discrimination. L'exemple étatsunien montre que les outils de police prédictive tendent en effet à reproduire et aggraver les biais inscrits dans les pratiques policières. Comme les patrouilles se concentrent sur des quartiers où vivent des populations déjà soumises à ces discriminations, des populations marginalisées, la police collecte davantage de données sur ces quartiers, et très peu sur les quartiers riches. Ces données vont ensuite venir nourrir l'algorithme, qui sera dès lors plus enclin à faire des recommandations sur la nécessité de patrouiller dans ces quartiers.

La chercheuse Sarah Brayne (2017) a aussi montré comme les outils « Big Data » permettaient à la police de Los Angeles une augmentation largement quantitative de la surveillance : on surveille un bien plus grand nombre de personnes, souvent pour des faits moins graves que dans le passé. Même si les outils de police prédictive servent d'abord à faire de la surveillance macroscopique, globale, agrégée, du comportement des foules et d'optimisation du travail de police, il y a aussi une dimension d'identification et de profilage qui se développe : on va chercher à cibler des populations, à anticiper quels sont les profils sociodémographiques qui sont facteurs de risque du point de vue de la prévention de la délinquance. Ce qu'on observe à l'étranger, c'est que ce sont très souvent des populations racisées, et que ces technologies de surveillance – loin d'être « indolores » et de mettre simplement en cause le droit à la vie privée – fonctionnent main dans la main avec les politiques carcérales[17].

Nous refusons ces technologies parce qu'elles participent à la mise en place d'un État policier qui ne dit pas son nom, en démultipliant la capacité d'action des bureaucraties policières à travers l'automatisation. On sait qu'elles ne seront d'aucun secours pour enrayer les formes de violence qui traversent nos sociétés, bien au contraire. Et au passage, en installant ces infrastructures de surveillance, on sape les conditions même de la vie démocratique. Je prends souvent cet exemple : si des technologies de reconnaissance faciale avaient été déployées à grande échelle au début des années 1940, nos grand-mères et nos grands-pères qui ont rejoint les réseaux de la résistance n'auraient pas tenu plus de trois semaines en clandestinité. Ce parallèle historique a le mérite de rappeler à quel point l'anonymat dans l'espace public urbain est quelque chose de vital en démocratie.

Et puis, à travers la dénonciation de ces technologies et de ces déploiements, l'enjeu est aussi de faire accepter l'idée qu'il faut arriver à trouver des réponses qui ne soient pas « technopolicières » aux problèmes qui se présentent à la ville. À notre modeste mesure, on essaie de contrer un peu ce double « solutionnisme », à la fois sécuritaire et technologique, qui s'est imposé dans les discours et qui nous fait penser que la technologie et les approches policières sont la bonne réponse à des problèmes fondamentalement politiques, comme la délinquance ou le sentiment d'insécurité. Trouver des réponses non policières à ces problèmes, c'est aussi une manière de contrer cette « pensée magique » qui restreint nos imaginaires et nous empêche d'envisager d'autres solutions. C'est aussi une manière de résister à une modification assez profonde du travail policier. Car dans les grands traités qui théorisent la police

moderne aux xvii[e] et xviii[e] siècles, il y avait cette idée d'un ordre public qu'il fallait tenter d'assurer au travers de multiples interventions dans la vie de la cité, par exemple pour assurer l'approvisionnement des populations, et pas seulement au travers de la surveillance et de la répression (Tilly, 1992 : 201-202). Or ce qui est frappant à la lecture des documents associés aux projets de « *Safe City* » sur le territoire, c'est qu'ils décrivent une ville chaotique, apocalyptique presque, soumise à tout un tas de risques environnementaux et sociaux. Dans ce contexte, les promoteurs de la « *Safe City* » ne cherchent plus à traiter les causes de ces différents problèmes, mais simplement à les mesurer et à les visualiser pour « optimiser » leur gestion. En somme, le but n'est plus tant de « garantir l'ordre public » que de « gérer le désordre ». Et ce faisant on s'empêche de poser toutes ces problématiques politiques extrêmement complexes et de les traiter de manière à la fois politique et radicale, au sens littéral, en les traitant à la racine. Je pense que c'est aussi ça l'enjeu de la résistance à ces déploiements : engager une désescalade techno-sécuritaire.

Les technologies de sécurité : un marché économique en explosion

TU AS PARLÉ DU SECTEUR INDUSTRIEL FRANÇAIS TOUT À L'HEURE, PAR EXEMPLE POUR LES JEUX OLYMPIQUES. TOUTES CES TECHNOLOGIES DE SURVEILLANCE SOULÈVENT BEAUCOUP DE QUESTION PAR RAPPORT À L'INTERVENTION D'ACTEURS PRIVÉS, NOTAMMENT DES GRANDES MULTINATIONALES, DANS CE SECTEUR. ÇA POSE ÉGALEMENT LA QUESTION DE LA PRIVATISATION DU MAINTIEN DE L'ORDRE ET DES ESPACES, NOTAMMENT URBAINS. DE QUELLE MANIÈRE LES ACTEURS PRIVÉS INTERVIENNENT-ILS DANS CE DOMAINE DU MAINTIEN DE L'ORDRE TECHNOLOGISÉ ET QUEL IMPACT CE PROCESSUS A-T-IL SUR LES VILLES ?

L'autre enjeu de notre travail est en effet de rappeler à quel point la fabrique de cette ville technopoliciarisée est dictée par les politiques industrielles, et comment elle résulte de formes de collusion entre acteurs privés et publics. En pratique, la technopolice s'accompagne en effet d'une privatisation de l'expertise technologique et juridique autour de ces projets.

Pour donner un exemple, dans le projet d'Observatoire Big Data pour la tranquillité publique à Marseille, le marché public prévoit que le prestataire retenu – en l'occurrence Engie Ineo – constitue une équipe qui inclut outre les ingénieurs qui travailleront l'outil sur le plan technologique, des sociologues pour faire une analyse métier du travail des policiers dans le but d'adapter l'outil à leurs besoins, et ensuite un juriste qui devra être en mesure de rédiger toutes les analyses juridiques, s'agissant notamment du droit des données personnelles. Ce juriste sera également chargé de rédiger les conventions de partenariat avec d'autres acteurs amenés à nourrir l'algorithme de leurs jeux de données. Employée par un industriel directement intéressé par la construction d'un outil de surveillance le plus complet possible, cette personne ne risque pas de faire preuve d'un zèle excessif. Les policiers eux-mêmes critiquent cette privatisation : le syndicat de la police municipale s'est notamment opposé à la distribution par la ville de Nice d'une application smartphone de dénonciation citoyenne à la police. Ils estiment qu'« il n'est jamais bon, sur le plan moral, de déléguer le service public de la sécurité à des personnes privées »[18].

C'EST DEVENU UN MARCHÉ CENTRAL…

En effet. Ces projets s'inscrivent au croisement de deux marchés très porteurs. En 2020, le marché de la « *Smart City* » était estimé à 410 milliards de dollars. Des études de marché prévoient 15 % de croissance entre 2019 et 2025, ce qui représentera à l'horizon 2025 plus de 820 milliards de dollars à l'échelle mondiale. Et le marché de la sécurité tous secteurs confondus, cela représente 629 milliards d'euros en 2018, en augmentation de 7 % par an soit deux fois la croissance mondiale[19]. Il s'agit clairement de marchés prometteurs et réputés stratégiques, tant pour les industriels français ou européens que les pouvoirs publics.

L'enjeu est de positionner un certain nombre d'acteurs face à la concurrence chinoise, étasunienne, israélienne. Le député LREM de la Loire Jean-Michel Mis le dit sans ambages : « il faut se positionner par rapport aux Américains ou Chinois, notamment sur les questions d'identification ou de reconnaissance biométrique »[20]. Quant au secrétaire d'État au numérique Cédric O, il est sur la même ligne lorsqu'il affirme qu'« expérimenter la reconnaissance faciale est nécessaire pour que nos industriels progressent »[21]. Le fait qu'en France l'État détienne encore des parts importantes dans les fleurons du secteur comme Thales ou Idemia contribue à expliquer pourquoi il y a des déploiements aussi nourris en comparaison d'autres pays européens. Ce n'est évidemment pas le seul facteur, mais il explique par exemple qu'un acteur comme la Banque Publique d'Investissement apporte des avances et des subventions pour ces projets[22]. Au final, on peut aussi voir dans les progrès de la Technopolice une forme de corruption de la décision politique, où l'État et les collectivités servent les stratégies industrielles de quelques acteurs privés.

QUEL EST LE RÔLE DES GAFAM[23] LÀ-DEDANS, INVESTISSENT-ILS AUSSI EN FRANCE ?

Aux États-Unis, les grandes multinationales qui dominent l'économie numérique jouent un rôle important dans les déploiements technopoliciers, venant concurrencer des acteurs historiques comme IBM. Un acteur comme Amazon propose par exemple une solution de reconnaissance faciale aux forces de l'ordre avec son logiciel Rekognition. Sa sonnette connectée Ring est aussi largement répandue aux États-Unis et permet dans certains cas de transmettre des flux vidéo à la police. Microsoft intervient également dans le marché de la reconnaissance faciale. Quant à Google, ils ont l'air de se tenir à distance, et interviennent plutôt dans des projets de « *Smart City* » ou la composante policière est moins évidente, et ce à travers une société spécialisée du nom de Sidewalk Labs. D'autres acteurs sont également très bien positionnés. Une entreprise qui revient souvent est Palantir, un des fers de lance de l'analyse « Big Data » qui travaille beaucoup avec les milieux du renseignement et qui est depuis peu côté en bourse. Il y a aussi des acteurs beaucoup moins connus.

Pour l'heure, ces entreprises étasuniennes semblent se tenir un peu à distance des marchés technopoliciers en France. Il y a quand même quelques exceptions notables : Palantir a par exemple un contrat avec les services de renseignement intérieur ; IBM propose une solution de vidéosurveillance automatisée à la ville de Toulouse ; Cisco était aussi à la tête d'une expérimentation de la reconnaissance faciale pour gérer les entrées et sorties dans des lycées de la région PACA – un projet qu'on a réussi à faire interdire à travers un recours contentieux[24].

Outre ces acteurs étatsuniens encore relativement marginaux, on voit aussi des entreprises israéliennes ou chinoises intervenir, par exemple Huawei, qui a conclu à

partir de 2016 un partenariat avec la ville de Valenciennes. Il se trouve qu'à Valenciennes, la politique municipale a longtemps été chapeautée par Jean-Louis Borloo, lequel a été conseiller de Huawei France et a même été pressenti pour en devenir président à l'été 2019 avant semble-t-il de reculer face aux controverses que cela risquait de susciter – un exemple qui illustre là encore les formes de collusion public-privé qui accompagnent la mise en place de ces technologies. En tout cas, on a des technologies chinoises, israéliennes ou japonaises qui sont déployées dans des villes françaises, et si ce n'est pas directement par les entreprises mères, c'est au travers d'intégrateurs français de technologies qui se chargent de candidater aux marchés publics pour revendre leur matériel.

Subir ou résister ?

QUAND ON PARLE DES POSSIBILITÉS D'ENCADRER, DE FREINER OU DE S'OPPOSER À CES TECHNOLOGIES DE SURVEILLANCE, ON SE HEURTE À L'IDÉE QUE CE SERAIT INÉLUCTABLE : LES GENS ONT L'IMPRESSION QUE QUOI QU'ON FASSE CES TECHNOLOGIES VONT EXISTER PARCE QU'ELLES SONT NÉCESSAIREMENT LIÉES AU FUTUR.

Cela pose effectivement la question du rôle de l'imaginaire et du discours dans la fabrique de la Technopolice. Est-ce que la science-fiction participe à former un déjà-là, en banalisant par anticipation ces nouvelles technologies ? Dans les discours des cadres, des services marketing, voire même des élus, on retrouve des éléments qui semblent tout droit tirés de romans de science-fiction. D'ailleurs, l'armée française a récemment lancé une initiative visant à recruter des auteurs de science-fiction, avec l'objectif, je cite, « d'imaginer et de créer des scénarios futuristes et disruptifs au profit de l'innovation de défense »[25].

En tant que genre littéraire et artistique, la science-fiction reste ambivalente : certaines œuvres sont là pour « faire rêver » et rendre désirable un futur hyper-technologique, tandis que d'autres œuvres tâchent de mettre en garde et agissent comme outils de conscientisation ou comme armes de résistance. On le mesure par exemple à la susceptibilité qu'on sent dans la population à l'endroit de technologies comme la reconnaissance faciale, qui évoque d'emblée l'imaginaire de la science-fiction et de la dystopie. De nombreuses œuvres comme *1984* ou *Minority Report* restent des garde-fous puissants contre l'idée que les technologies de surveillance représentent nécessairement un progrès. En tous cas, il faut battre en brèche cette idée d'inéluctabilité. La technologie est politique. Elle est produite par notre société, et nous pouvons collectivement infléchir son cours.

JUSTEMENT, EN TERMES DE RÉSISTANCE, AVANT LA RÉSISTANCE MÊME, QUELS TYPES DE GARDE-FOUS OFFICIELS, FORMELS, EXISTENT FACE À LA MISE EN PLACE DE CES TECHNOLOGIES QUI PEUT ÊTRE EXPÉRIMENTALE, LOCALE, ETC. ? QUELS TYPES DE MOBILISATION OU D'ALTERNATIVES SONT PROPOSÉES, TESTÉES OU MISES EN PLACE EN FRANCE OU AILLEURS ?

Dans le cadre de cette campagne Technopolice, on mobilise d'abord le droit : le droit des libertés publiques, des droits humains, le droit des données personnelles. Ça nous permet de remporter des petites victoires. Je l'ai évoqué rapidement : on a par exemple obtenu une jurisprudence qui interdit l'utilisation de systèmes biométriques comme la reconnaissance faciale pour gérer les entrées et sorties des lycées dans la région PACA. Ce n'était pas gagné : la CNIL avait d'abord semblé trouver que ce type d'application serait acceptable sous certaines conditions. Quelques mois plus tard, en

mai 2020, on a obtenu l'interdiction de l'usage policier des drones, faute d'un cadre juridique suffisamment détaillé[26]. Ce premier cas d'espèce concernait spécifiquement l'utilisation des drones à Paris pour faire appliquer les mesures de restrictions sanitaires. Or, durant l'été, le préfet de police de Paris a décidé d'ignorer cette décision, ce qui a motivé un second recours là encore victorieux[27].

Mais il s'agit-là de victoires temporaires. Le droit peut être un outil et je pense qu'il est important de continuer à le mobiliser, mais il ne permet pas de rendre compte de l'ensemble des enjeux que soulèvent ces déploiements technopoliciers. Beaucoup des garde-fous juridiques qui ont été mis en place depuis quarante ans pour juguler les aspects le plus problématiques des technologies informatiques s'avèrent en pratique inefficaces pour enrayer la fuite en avant des systèmes de surveillance. La CNIL est une institution assez paradigmatique à cet égard. Elle a été créée en 1978 suite aux premières grandes controverses autour de la surveillance informatique et du fichage d'État, et même si au cours de son histoire elle a parfois tenté de résister et de freiner le développement de la surveillance, elle reste structurellement enfermée dans une forme d'impuissance. Très souvent, elle se cantonne à l'application du droit existant et se refuse à faire valoir des positions proprement politiques, par exemple pour condamner une technologie telle que la reconnaissance faciale. En fait, elle se pense comme institution chargée d'accompagner le progrès technologique. Elle va donc se retrancher dans une position où elle appelle à l'adoption de garde-fous destinés à en encadrer l'usage, mais s'avérera incapable de les faire respecter en pratique. Et si jamais elle le fait – ce qui reste assez exceptionnel – le gouvernement passera outre son avis ou instrumentalisera la prochaine crise sécuritaire pour changer la loi et surmonter son opposition.

De fait, la CNIL a vu ses pouvoirs reculer depuis près de vingt ans. Dans les années 1990, elle s'était par exemple opposée de manière assez frontale au déploiement de la vidéosurveillance et à la création de vastes fichiers de police, et en 2004 une réforme est venue lui ôter son pouvoir de bloquer la création par le gouvernement de nouveaux programmes de surveillance – son avis est devenu simplement consultatif[28]. Le règlement européen dédié à la protection des données personnelles (RGPD), entré en vigueur en mai 2018 à l'échelle de l'Union Européenne, lui a aussi retiré certains pouvoirs, notamment ceux qui lui permettaient d'autoriser – et donc de bloquer – des dispositifs de surveillance à l'échelon local.

DONC QU'EST CE QUI EXISTE, QUELS MOYENS OU TYPES D'ACTIONS DIRECTS SONT MIS EN PLACE AU NIVEAU DES CITOYENS ?

Ce qu'on observe, ce sont des actions de brouillage ou de sabotage qu'on a pu voir par exemple à Hong-Kong à l'occasion des manifestations pour la démocratie et contre la mise sous tutelle de la région autonome par la Chine. On a ainsi vu des manifestants utiliser massivement des parapluies (figure 1), pointer des lasers vers l'optique des caméras ou couvrir les dômes des caméras de vidéosurveillance à l'aide de peinture aérosol pour « aveugler » les systèmes de reconnaissance faciale. On voit aussi aux États-Unis des municipalités qui vont interdire l'utilisation de la reconnaissance faciale par leur police municipale. C'est le cas à Oakland, à San Francisco, à Cambridge et dans d'autres villes étasuniennes. Dans ces mêmes villes, on assiste aussi fréquemment à la mise en place de comités citoyens pour auditer et contrôler de manière permanente les achats de technologies de surveillance. Cela crée un

contrôle citoyen à double tranchant, puisque cela risque aussi de rendre ces instances complices des politiques technopolicières et carcérales.

Figure 1. Installation « Les parapluies de Hong-Kong »

Source : photographie à droite de Thaddé Comar, « How was your dream », exposition « Technopolice » dans le cadre de l'exposition Mutalab, Ardenome – ancien grenier à sel, Avignon, juillet 2020[29].

CELA SE PASSE EN LIEN AVEC LES MUNICIPALITÉS DU COUP ?

Oui, c'est institutionnalisé à l'échelle locale, sachant qu'il y a aussi des propositions de loi à l'échelle fédérale qui ont été présentées ces derniers mois. Ces avancées au plan juridique sont liées à toutes les mobilisations anti-racistes et au mouvement Black Lives Matter, qui a très bien fait le lien entre le racisme policier et l'usage de ces technologies de contrôle.

Cette vague de mobilisation a conduit des entreprises comme IBM, Microsoft ou Amazon à annoncer au mois de juin dernier un moratoire sur la vente aux forces de police de leurs outils de reconnaissance faciale, dans l'attente d'un cadre juridique plus précis et adéquat. Comme en France, ces déploiements se font au mépris total des règles de droit. Cela dit, les annonces de ces multinationales constituent surtout une stratégie de relations publiques, et elles continuent de vendre bien d'autres technologies également très dangereuses, et notamment les autres applications de la vidéosurveillance automatisée qui permettent également de procéder à l'identification de sujets – pas forcément à partir d'un visage mais d'une démarche ou d'un attribut vestimentaire. Sur ces technologies, rien n'a été dit et il faut aussi voir dans les annonces de ces entreprises une forme assez choquante d'instrumentalisation des combats antiracistes.

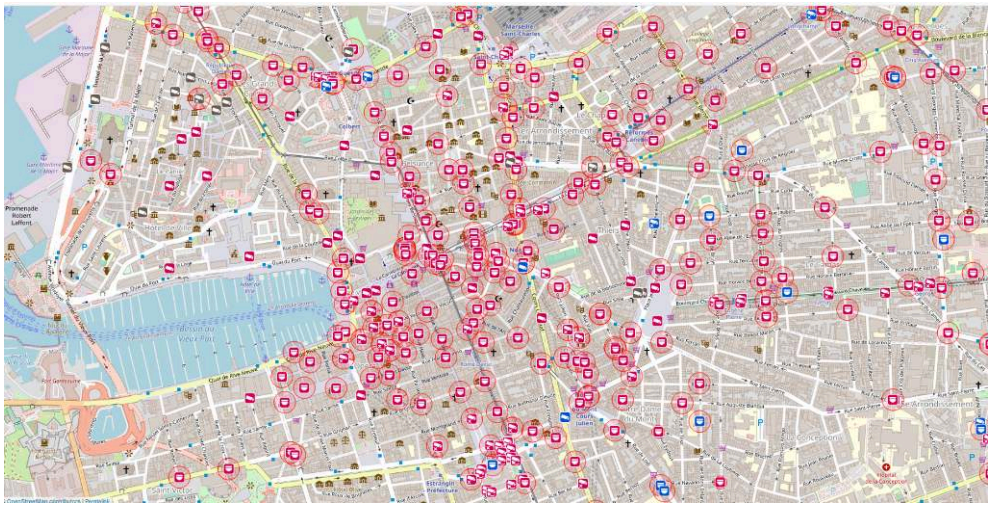
IL Y A AUSSI UNE MULTIPLICATION DES APPROCHES ARTISTIQUES SUR CES SUJETS.

Les interventions artistiques permettent de rendre sensible des technologies de surveillance souvent invisibles et impalpables. C'est aussi un moyen de créer des dispositifs originaux et parfois provocateurs. Je pense notamment au projet de

l'artiste italien Paolo Cirio qui en octobre 2020 a publié des photographies de visages de policiers prises en mage de manifestations, et proposait aux internautes de les identifier via le site *capture-police.com*. En fait, le dispositif n'enregistrait aucun patronyme, et n'identifiait personne. Mais ce qui est intéressant, c'est qu'en pleine polémique sur le floutage des visages de policiers, cette proposition artistique a tout de suite été dénoncée par le Ministère de l'Intérieur, qui sans aucune décision judiciaire a quand même réussi à faire annuler une exposition de l'artiste.

Or, cette œuvre relève de la liberté d'expression et de la liberté artistique. Elle permettait de rendre palpable le travail d'enrichissement d'une base de données à des fins d'identification, tout en retournant symboliquement la surveillance contre le pouvoir – en l'occurrence, contre l'institution policière – sur le mode de « l'arroseur arrosé ». Au-delà, il faut aussi se dire que l'art c'est parfois presque tout ce qu'il reste pour résister, notamment dans les contextes les plus franchement autoritaires. En Chine, c'est principalement par l'art que se manifestent des dénonciations publiques du système de surveillance mis en place par le régime[30].

Figure 2. Répartition des caméras de vidéosurveillance dans le centre de Marseille



Source : capture d'écran (14 janvier 2021), Surveillance under Surveillance, https://sunders.uber.space/.

Une posture de « recherche adversiale »

POUR FINIR, UNE QUESTION UN PEU PLUS MÉTHODOLOGIQUE. ON COMPREND DANS TON DISCOURS - ET TU L'AS DIT DÈS LE DÉPART - QUE TU AS FAIT TA THÈSE AUSSI POUR DONNER DU SENS À TON ENGAGEMENT MILITANT DONC IL Y A UN LIEN FORT POUR TOI ENTRE RECHERCHE ET ACTIVISME, OU ENGAGEMENT SOCIAL ET POLITIQUE. TU AS PARLÉ DE RECHERCHE-ACTION PAR RAPPORT À LA CAMPAGNE TECHNOPOLICE. TOUT ÇA RAMÈNE À LA VIEILLE QUESTION DE LA POSITIONNALITÉ DU CHERCHEUR. QU'EST-CE QUE ÇA VEUT DIRE POUR TOI ÊTRE CHERCHEUR ET ACTIVISTE EN MÊME TEMPS ? COMMENT EST-CE QUE TU CONCILIES CES DEUX ASPECTS ?

Pour moi, cela renvoie effectivement à la question de la neutralité axiologique, qui doit en même temps être nuancée parce que la sociologie des sciences a permis d'établir depuis pas mal d'années : la recherche est toujours, y compris dans les sciences dites « dures », le reflet de la position sociale d'un chercheur. En

l'occurrence, mon engagement contre ces technologies policières est le résultat d'une expérience militante mais aussi le fruit de mes lectures, de ma recherche. Dans le cadre de cette campagne Technopolice, mon problème par rapport à ces enjeux épistémologiques, c'est que j'ai aussi une parole publique critique vis-à-vis de ces déploiements, ce qui peut entraver l'accès à certains terrains sensibles. Alors je bricole avec d'autres moyens pour tenter de contourner ces obstacles.

De fait, à travers les demandes d'accès aux documents administratifs réalisés dans le cadre de la campagne Technopolice, à travers les recours aussi qui conduisent les collectivités locales mises en cause à produire tout un tas de documents et d'argumentations juridiques, à travers le fait par exemple d'aller dans des salons professionnels comme « Milipol » et d'autres événements liés aux technologies policières, on a accès à de nombreuses données qui peuvent être collectées et analysées. L'histoire est aussi d'une grande utilité, car en passer par d'autres épisodes historiques est une manière de mettre à distance l'actualité tout en produisant des outils critiques pour l'analyser. Et enfin, on peut envisager des techniques d'investigation journalistique, comme par exemple le fait de développer des relations avec des lanceurs d'alerte, voire même de conduire une enquête sous pseudonyme. Ça fait partie d'une boîte à outils qui reste à développer, et qui mériterait d'être formalisée au plan méthodologique. Ces choses-là ont été un peu abordées dans les années 1970 par certaines communautés de chercheurs, mais elles semblent depuis avoir été un peu délaissées au sein du champ universitaire.

TU EMPLOIES LE TERME DE « RECHERCHE ADVERSARIALE » POUR QUALIFIER CE TYPE DE RECHERCHE ENGAGÉE.

Je ne suis encore bien sûr du choix de l'adjectif, mais le terme « adversarial » dénote bien cette idée que dans la controverse, je peux parfois être identifié comme étant un adversaire par les interlocuteurs et les enquêtés auxquels j'aimerais avoir accès. Même si, parfois, cette posture peut contribuer à m'ouvrir des portes, il arrive en effet qu'on refuse de me rencontrer, ou que l'on me tienne un double discours. Le terme « adversarial » renvoie aussi au projet d'une recherche-action articulée à des mobilisations contre ces processus, dont elle se nourrit et qu'elle cherche à nourrir en retour en assumant une posture critique. Enfin, le terme est un clin d'œil à la recherche en sécurité informatique, où la « recherche adversariale » désigne ces cas où un chercheur en sécurité informatique essaye de trouver une faille dans un système informatique sans disposer d'informations préalables, et qui se met donc dans la position d'un « attaquant ».

En transposant ce type d'approche au sein des sciences sociales, l'enjeu est d'assumer la valeur à la fois éthique et heuristique du statut de ce statut de chercheur engagé, et en même temps de voir comment la recherche académique et la réflexivité qu'elle induit peuvent servir à la défense de la démocratie et des droits humains, par exemple en produisant une forme d'autocritique et en mettant à distance certains réflexes ou postulats propres au militantisme.

MERCI FÉLIX !

Un grand merci à toi Marion !

BIBLIOGRAPHIE

ABOUT I., DENIS V. (2010), *Histoire de l'identification des personnes*, La Découverte, Paris.

ABOUT I. (2011), « Surveillance des identités et régime colonial en Indochine, 1890-1912 », *Criminocorpus. Revue d'Histoire de la justice, des crimes et des peines*. En ligne : http://journals.openedition.org/criminocorpus/417

Anonyme (2020), « Community Defense : Sarah T. Hamid on Abolishing Carceral Technologies », *Logic Magazine*, no. 11. En ligne : https://logicmag.io/care/community-defense-sarah-t-hamid-on-abolishing-carceral-technologies/.

BRAYNE S. (2017), « Big Data Surveillance: The Case of Policing », *American Sociological Review*, vol. 82, no. 5.

Cour des comptes (2020), *Les polices municipales*. En ligne : https://www.ccomptes.fr/system/files/2020-11/20201020-rapport-polices-municipales_0.pdf [consulté le 8 mars 2021]

ETERNO J. A., Silverman E. B. (2012), *The Crime Numbers Game: Management by Manipulation*, Abingdon, CRC Press.

HOLSTON J. (2009), *Insurgent Citizenship: Disjunctions of Democracy and Modernity in Brazil*, Princeton, Princeton University Press.

MANACH J-M. (2018), « Défavorablement connus », *Pouvoirs*, no. 164, pp. 49-61.

Ministère de l'Intérieur (2020), *Livre blanc de la sécurité intérieure*. En ligne : https://www.interieur.gouv.fr/fr/content/download/125071/1001195/file/livre-blanc-de-la-securite-interieure.pdf (consulté le 8 mars 2021).

MCILWAIN C. (2019), *Black Software: The Internet & Racial Justice, From the AfroNet to Black Lives Matter*, Oxford University Press, Oxford.

MCILWAIN C. (2020), « Of course technology perpetuates racism. It was designed that way », *MIT Technology Review*, vol. 3. En ligne : https://www.technologyreview.com/2020/06/03/1002589/technology-perpetuates-racism-by-design-simulmatics-charlton-mcilwain/.

MUCCHIELLI L. (2018), *Vous êtes filmés !*, Paris, Armand Colin.

REYNIE D. (1998), *Le triomphe de l'opinion publique*, Paris, Odile Jacob.

TILLY C. (1992), *Contrainte et capital dans la formation de l'Europe, 990-1990*, Paris, Aubier.

NOTES

1. Edward Snowden a révélé, en 2013, l'ampleur des programmes d'écoute et de surveillance de la NSA, aux États-Unis et dans le monde. Voir par exemple le documentaire *Citizenfour* réalisé par Laura Poitras (2014).

2. « Les militants de la COP21, cibles de l'état d'urgence », Pécout, Adrien, Borredon Laurent, *Le Monde*, 27 novembre 2015, https://www.lemonde.fr/societe/article/2015/11/27/les-militants-de-la-cop21-cible-de-l-etat-d-urgence_4818885_3224.html (consulté le 8 mars 2021). La loi du 20 novembre 2015 relative à l'état d'urgence (Loi n° 2015-1501) autorisait l'assignation à résidence d'une personne s'il existait « des raisons sérieuses de penser que son comportement constitu[ait] une menace pour la sécurité et l'ordre publics » (art. 6). Depuis, l'article 3 de la loi du 30 octobre

2017 renforçant la sécurité intérieure et la lutte contre le terrorisme a inscrit ces mesures dans le droit commun, en les limitant au terrorisme. Le ministre de l'Intérieur peut ainsi, aux seules fins de prévention du terrorisme, ordonner des mesures individuelles de contrôle administratif et de surveillance à l'égard des personnes dont le « comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics », et qui soit entrent en relation avec des personnes ou organisations incitant à commettre des actes de terrorisme, soit adhèrent à des thèses incitant à commettre des actes de terrorisme. Codifiée au sein des articles L. 228-1 à L. 228-7 du code de la sécurité intérieure, ces mesures comprennent notamment l'interdiction de se déplacer à l'extérieur d'un certain périmètre géographique.

3. Voir McIlwain 2019, 2020.

4. « Vidéo-protection : Les 500 nouvelles caméras coûteront trois fois plus cher que prévu », Manach Jean-Marc, *Marsactu* , 11 avril 2018, https://marsactu.fr/video-protection-500-nouvelles-cameras-couteront-trois-plus-cher-prevu/ (consulté le 8 mars 2021).

5. Voir la fiche de présentation du projet, obtenue auprès de la mairie de Marseille via des demandes d'accès aux documents administratifs : https://data.technopolice.fr/fr/entity/77rqd2d8qn4 (consulté le 8 mars 2021).

6. Site internet de l'Association nationale de la vidéoprotection : http://www.an2v.org/ (consulté le 8 mars 2021).

7. Documents administratifs, Observatoire Big Data de la Tranquillité Publique, Marseille, en ligne sur https://data.technopolice.fr/fr/entity/2ba0kd98gg4 (consulté le 8 mars 2021).

8. Site internet de la société Sûreté Globale : https://www.sureteglobale.org (consulté le 8 mars 2021).

9. Présentation du logiciel Map Revelation : www.maprevelation.fr (consulté le 8 mars 2021).

10. Voir par exemple « Ce que nous avions à dire à ceux qui bâtissent la technopolice », La Quadrature du Net, 27 septembre 2019, https://www.laquadrature.net/2019/09/27/ce-que-nous-avions-a-dire-a-ceux-qui-batissent-la-technopolice/ (consulté le 8 mars 2021).

11. Voir une restitution de la prise de parole des représentants de La Quadrature du Net : https://www.laquadrature.net/2019/09/27/ce-que-nous-avions-a-dire-a-ceux-qui-batissent-la-technopolice/ (consulté le 8 mars 2021).

12. Voir notamment la campagne #ReclaimYourFace, lancée par des organisations de protection des droits pour faire interdire au niveau de l'Union européenne la surveillance biométrique de l'espace public. https://europa.eu/citizens-initiative/initiatives/details/2021/000001_fr (consulté le 8 mars 2021).

13. Voir par exemple « Au Mali, Niger et Sénégal, le marché de l'identité en plein essor », Andrea de Georgio et Giacomo Zandonini, *Médiapart*, 5 mars 2019, https://www.mediapart.fr/journal/international/050319/au-mali-niger-et-senegal-le-marche-de-l-identite-en-plein-essor?page_article=1 (consulté le 8 mars 2021) ; « Here's how a well connected security companies quietly build mass biometric databases in West Africa with EU aid funds », Privacy International, novembre 2020, https://www.privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric (consulté le 8 mars 2021). Voir aussi : About, Denis, 2010.

14. Voir About, Ilsen. (2011). Surveillance des identités et régime colonial en Indochine, 1890-1912. *Criminocorpus. Revue d'Histoire de la justice, des crimes et des peines*. http://journals.openedition.org/criminocorpus/417 (consulté le 8 mars 2021).

15. Voir Tesquet, Olivier, 2021, *Etat d'urgence technologique*, Premier Parallèle.

16. « Lancement des projets lauréats de l'appel à projets Flash JOP24 », Agence Nationale de la Recherche, 23 janvier 2020, https://anr.fr/fr/actualites-de-lanr/details/news/lancement-des-projets-laureats-de-lappel-a-projets-flash-jop24/ (consulté le 8 mars 2021).

17. « Community Defense : Sarah T. Hamid on Abolishing Carceral Technologies », *Logic Magazine,* n°11, août 2020, https://logicmag.io/care/community-defense-sarah-t-hamid-on-abolishing-carceral-technologies/ (consulté le 8 mars 2021).

18. « Smart Cities Market Report 2020 - Global Forecast to 2025: Market Size is Expected to Grow from $410.8 Billion in 2020 to $820.7 Billion », *ResearchAndMarkets.com*, octobre 2020, https://www.globenewswire.com/news-release/2020/10/05/2103315/0/en/Smart-Cities-Market-Report-2020-Global-Forecast-to-2025-Market-Size-is-Expected-to-Grow-from-410-8-Billion-in-2020-to-820-7-Billion.html (consulté le 8 mars 2021).

19. « Milipol 2019 : 'Développer une approche globale de la sécurité en agissant sur tous les continuums' (Yann Jounot) », Clément Giuliano, 18 novembre, *AEF Info*, https://www.aefinfo.fr/depeche/616430 (consulté le 8 mars 2021).

20. Cité dans Le Foll, Clément et Clément Pouré, « Citizen Caine veille sur Thales », *Les Jours*, 19 novembre 2020, https://lesjours.fr/obsessions/thales-surveillance/ep2-patrice-caine/ (consulté le 8 mars 2021).

21. « Cédric O : 'Expérimenter la reconnaissance faciale est nécessaire pour que nos industriels progressent », Untersinger, Martin, *Le Monde*, 14 octobre 2019.

22. Voir par exemple le communiqué de presse « Le projet innovant SafeCity, pour renforcer la sécurisation des villes intelligentes sur le territoire, obtient un financement du Programme d'Investissements d'Avenir (PIA) », 18 juillet 2018, https://data.technopolice.fr/fr/entity/ljlrtjb2b6?page=1 (consulté le 8 mars 2021).

23. Acronyme des multinationales du Web : Google, Apple, Facebook, Amazon et Microsoft.

24. « Lycées Nice Marseille : première victoire contre la reconnaissance faciale », La Quadrature du Net, 28 octobre 2019, https://www.laquadrature.net/2019/10/28/lycees-nice-marseille-premiere-victoire-contre-la-reconnaissance-faciale/ (consulté le 8 mars 2021).

25. « Lancement de l'appel public à la concurrence pour la constitution de la Red Team », Ministère des Armées, 16 décembre 2019, https://www.defense.gouv.fr/aid/actualites/lancement-red-team (consulté le 8 mars 2021). Voir aussi « Présentation de la stratégie innovation du ministère des Armées », Ministère des Armées, 9 septembre 2020, https://www.defense.gouv.fr/aid/actualites/presentation-de-la-strategie-innovation-du-ministere-des-armees (consulté le 8 mars 2021) ; « L'armée française dévoile le nom des auteurs de SF de sa "Red Team", chargée d'anticiper les menaces du futur », Marine Benoit, *Sciences et Avenir*, 4 décembre 2020, https://www.sciencesetavenir.fr/high-tech/le-ministere-de-la-defense-devoile-le-nom-des-auteurs-de-science-fiction-de-sa-red-team-chargee-d-anticiper-les-menaces-du-futur_149762 (consulté le 8 mars 2021) ; « Des auteurs de science-fiction recrutés par l'armée pour anticiper les futurs conflits », Franck Cognard, *France Info*, 4 décembre 2020, https://www.francetvinfo.fr/economie/emploi/metiers/armee-et-securite/des-auteurs-de-science-fiction-recrutes-par-l-armee-pour-anticiper-les-futurs-conflits_4206757.html (consulté le 8 mars 2021) ; « L'armée française en appelle à la science-fiction pour anticiper les menaces du futur », *Le Monde*, 18 juillet 2019, https://www.lemonde.fr/big-browser/article/2019/07/18/l-armee-francaise-en-appelle-a-la-science-fiction-pour-anticiper-les-menaces-du-futur_5490856_4832693.html (consulté le 8 mars 2021). Voir aussi la réaction de la maison d'édition La Volte, notamment éditrice d'Alain Damasio : « *Retour sur la nucléarisation et la militarisation des Utopiales 2019* », La Volte, novembre 2019, https://lavolte.net/militarisation-utopiales-2019/ (consulté le 8 mars 2021).

26. « Surveillance par drone », décision du Conseil d'État, 18 mai 2020, https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones (consulté le 8 mars 2021).

27. En décembre 2020 la Quadrature du Net a remporté un nouveau recours contre l'utilisation de drones pour surveiller les manifestations. Voir « Base de jurisprudence », Conseil d'Etat, 22 décembre 2020, https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-12-22/446155 (consulté le 8 mars 2021).

28. Voir Manach, 2018.

29. Exposition « Mutalab », 9 au 25 juillet 2020, Ardenome, Avignon, https://www.ardenome.fr/mutalab-archive-2020 (consulté le 8 mars 2021).

30. Voir par exemple Charlotte Gao, "One Man, One Road: A Funny Tale of Civic Protest in China", *The Diplomat*, 7 août 2017, https://thediplomat.com/2017/08/one-man-one-road-a-funny-tale-of-civic-protest-in-china/ (consulté le 8 mars 2021) ; Lu Mingjun, "Panorama: Visual Theater and the Politics of Surveillance", *Artlinkart*, 2018, http://cloudliste.artlinkart.com/en/article/overview/7cdesxuk (consulté le 8 mars 2021) ; Qianer Liu et al., "China, Coronavirus and Surveillance: The Messy Reality of Personal Data", 2 avril 2020, https://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca (consulté le 8 mars 2021) ; Jian Xiao et Shuwen Qu, "'Everybody's Donghu': Artistic Resistance and the Reclaiming of Public Space in China', *Space and Culture*, 6 février 2020.

INDEX

Thèmes : Carnets de débats

AUTEURS

MARION LECOQUIERRE

Docteure en géographie, post-doctorante à l'université d'Helsinki.

FÉLIX TRÉGUER

Chercheur en Sciences politiques, post-doctorant au CERI Sciences Po, membre de La Quadrature du Net