SURVEILLANCE DE MASSE

ET CONTRÔLE DE LA DISSIDENCE EUROPÉENNE

FRANCE

En France, la surveillance rogne sur les libertés publiques

Comment le Covid-19 a accéléré la surveillance de l'espace public et es citoyens

ENCO EUROPEAN NETWORK OF CORPORATE OBSERVATORIES

Observatoire des multinationales SOCIAL, ÉCOLOGIQUE, POLITIQUE

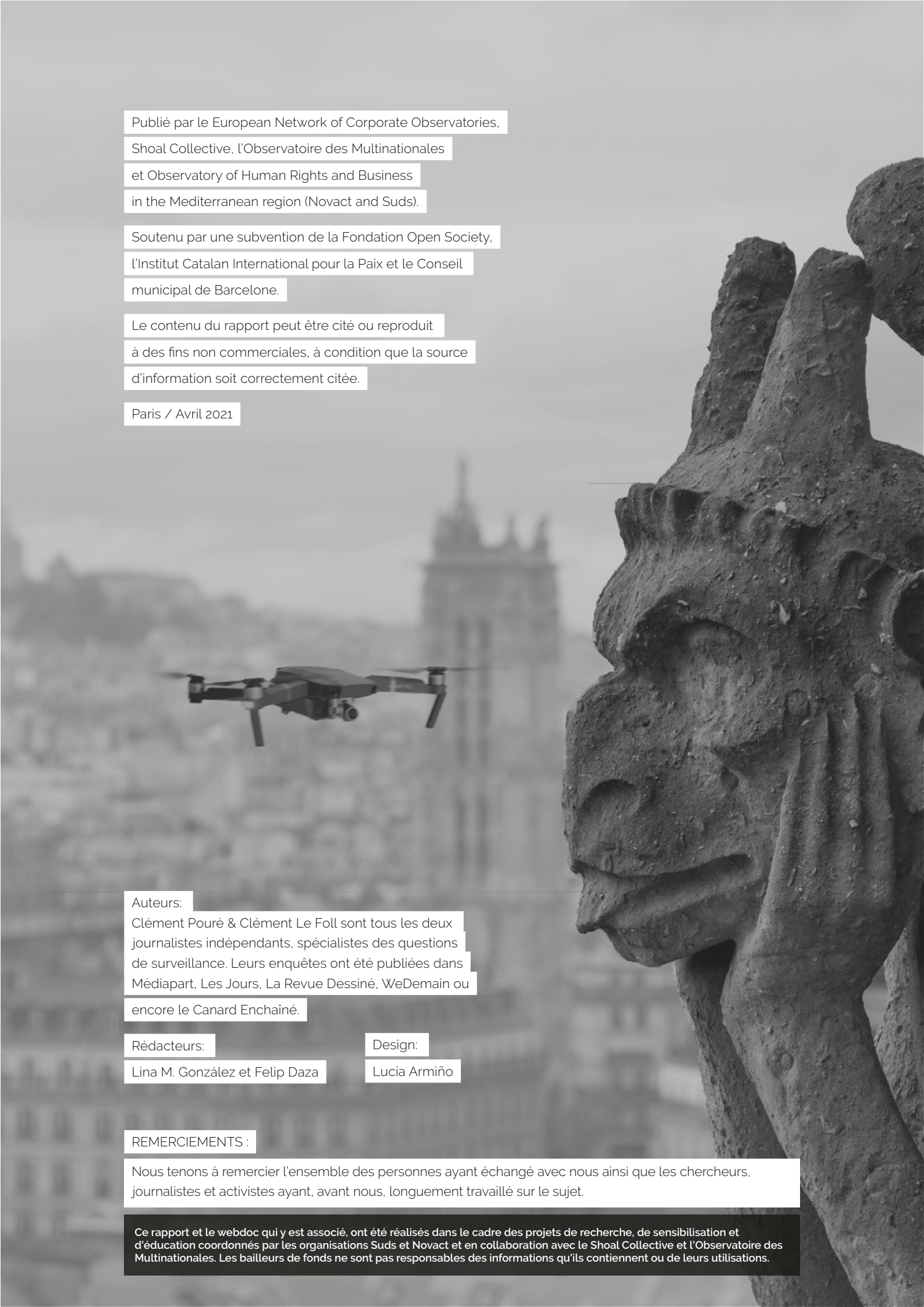
ODHE Observatori de Drets Humans i Empreses a la Mediterrània

shoal radical writing for a world beyond capitalism

Publié par le European Network of Corporate Observatories,
Shoal Collective, l'Observatoire des Multinationales
et Observatory of Human Rights and Business
in the Mediterranean region (Novact and Suds).

Soutenu par une subvention de la Fondation Open Society,
l'Institut Catalan International pour la Paix et le Conseil
municipal de Barcelone.

Paris / Avril 2021



Auteurs:
Clément Pouré & Clément Le Foll sont tous les deux
journalistes indépendants, spécialistes des questions
de surveillance. Leurs enquêtes ont été publiées dans
Médiapart, Les Jours, La Revue Dessiné, WeDemain ou
encore le Canard Enchaîné.

Rédacteurs:
Lina M. González et Felip Daza

Design:
Lucía Armiño

REMERCIEMENTS :

Nous tenons à remercier l'ensemble des personnes ayant échangé avec nous ainsi que les chercheurs, journalistes et activistes ayant, avant nous, longuement travaillé sur le sujet.

Ce rapport et le webdoc qui y est associé, ont été réalisés dans le cadre des projets de recherche, de sensibilisation et d'éducation coordonnés par les organisations Suds et Novact et en collaboration avec le Shoal Collective et l'Observatoire des Multinationales. Les bailleurs de fonds ne sont pas responsables des informations qu'ils contiennent ou de leurs utilisations.

SOMMAIRE

MÉTHODOLOGIE

Sans être exhaustif, ce rapport a pour objectif de donner un aperçu global des technologies de surveillance déployées en France durant la pandémie, en insistant particulièrement sur leurs impacts concrets sur les libertés individuelles.

Nous avons pour cela :

- compilé des informations issues des documents officielles des entreprises et des associations représentants les organisations du secteur ;
- Utilisé des documents officiels, récupérés par nos soins lors de différentes enquêtes réalisées tout au long de l'année 2020, issus des administrations, des collectivités ou des entreprises ainsi que ceux mis en ligne par les différentes associations de défense des libertés publiques, en particulier la Quadrature du Net et leur plateforme Technopolice;
- Travaillé avec des articles de presse issu de la presse francophone.
- Echangé avec des acteurs de l'industrie, des chercheurs et des activistes spécialistes des questions de surveillance et de sécurité.

INTRODUCTION

C'était au milieu du premier confinement. Two-I, entreprise spécialiste des logiciels d'hypervision, annonce en grande pompe la sortie de Vigilance, un logiciel de traitement d'images et d'analyse de données, initialement pensé pour la gestion de la ville mais « rebrandé» pour la crise du Covid.

Sur un fond de cartographie d'une ville jaillissent en temps réel des alertes : « accident de voiture », « embouteillage », mais aussi « fièvre », « station surpeuplée », « absence de masque » ou « distanciation sociale ». En cliquant sur ces points, le contrôleur du logiciel accède au contenu vidéo en live. Des filtres lui permettent de vérifier la température corporelle des citoyens ou de consulter une batterie de statistiques.

Datakalab, qui a pu expérimenter des logiciels de reconnaissance de masques dans plusieurs communes françaises, MyConnect, dont les caméras thermiques se sont vendues comme des petits pains lors des premiers mois de la pandémie, ou Thales qui a signé de nouveaux contrats pour déployer ses solutions de reconnaissance faciale dans les aéroports. Depuis le début du confinement, de nombreuses entreprises françaises du secteur de la surveillance ont transformé leurs technologies pour les adapter aux conditions de la pandémie.

Prenons de la hauteur. Si ces entreprises ont pu profiter d'un nouveau marché, l'État, autant que les collectivités territoriales, a multiplié les gadgets technologiques pour lutter contre la pandémie. Drones utilisés pour rappeler aux passants les gestes barrières ou traquer ceux qui ne respectent pas le confinement, caméras thermiques destinées à contrôler l'accès à certains bâtiments, application de *tracking* pour endiguer la pandémie… autant d'outils mobilisés pour résorber la crise mettant en risque les libertés individuelles.

Des plus petites entreprises aux grandes institutions policières de l'État, l'année 2020 marque un tournant pour la surveillance en France. L'ouverture d'un nouveau marché pour la surveillance, l'émergence d'enjeux de sécurité publique liés au respect du confinement et une volonté politique affichée de faire des nouvelles technologies un outil central de lutte contre la pandémie ont conduit aux déploiements massifs de nouveaux outils de contrôle de l'espace public tout en crédibilisant des technologies encore à la marge comme la vidéosurveillance intelligente. Une tendance large, sur fond de virage sécuritaire et de crise sociale et politique.

C'est au début des années 2000 que les questions de surveillance commencent à s'inscrire durablement dans le paysage politique Français. En 1993, le maire de Levallois-Perret, Patrick Balkany, installe le premier système de vidéosurveillance municipale. Le modèle fait des émules et se popularise au début des

années 2000. « *Les élections municipales de 2001 jouent un rôle majeur,* confie Laurent Mucchielli, sociologue spécialiste de la vidéosurveillance. *L'argument sécurité a été pour la première fois un thème récurrent des campagnes aux élections municipales.* »

Si le nombre de villes à s'équiper augmente, le boom de la vidéosurveillance va être insufflé par un homme, Nicolas Sarkozy. Proche de Patrick Balkany, il est tout aussi convaincu par l'efficacité de la vidéosurveillance, impressionné par le système mis en place au Royaume-Uni, qui aurait joué un rôle clé dans l'arrestation des suspects après les tentatives d'attentat de Londres en 2005.

Alors ministre de l'Intérieur, il confie en 2005 à l'inspecteur général de l'administration Philippe Melchior un rapport intitulé « La vidéosurveillance et la lutte contre le terrorisme. » Un rapport qui s'interroge sur les buts recherchés du dispositif : Lutter contre la délinquance ? Le banditisme ? Rassurer les commerçants et les citoyens ? Sans répondre à ces questions, Nicolas Sarkozy fait voter la loi du 23 janvier 2006 relative à la lutte contre le terrorisme, qui assouplit les conditions d'utilisation de la vidéosurveillance dans l'espace public. Ce penchant s'accentue lors de son arrivée à la présidence de la République en 2007 et la création du Fonds interministériel de prévention de la délinquance (FIPD) qui, entre 2007 et 2013, dédiera 150 millions d'euros au financement de la vidéosurveillance par les collectivités locales. En 2012, alors que le mandat de Nicolas Sarkozy s'achève, la Commission Nationale de l'Informatique et des Libertés (CNIL) dresse un bilan équivoque[1]. 935000 caméras de surveillance sont en place en France. 827 749 dans des lieux ouverts au public, comme les commerces et 70 003 dans l'espace public : routes, places et ruelles.

Si le FIPD a consacré une part moins importante de son budget à la vidéosurveillance sous sa présidence, l'élection de François Hollande n'inverse pas la tendance. Durant son mandat, l'État structure les acteurs de la sécurité en créant le Conseil des industries de la confiance et de la sécurité, CICS, interlocuteur industriel de l'État qui regroupe les plus gros acteurs du secteur « *Ces rassemblements d'industriels ont de l'influence car ils représentent de milliers d'emplois. Ils jouent un rôle clé dans le développement de la surveillance en tentant d'influencer les processus législatifs* », pointe Martin Drago, juriste à la Quadrature du Net.

1 Communiqué de presse de la CNIL, 21 juin 2012, "Vidéosurveillance/vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée" https://www.cnil.fr/sites/default/files/typo/document/CNIL-DP_Video.pdf

Les attentats de Charlie Hebdo et les attaques du 13 novembre 2015 marquent un nouveau tournant dans la politique sécuritaire française. Au lendemain de l'attentat du Bataclan, François Hollande décrète l'état d'urgence pour une dizaine de jours. Il sera finalement prolongé jusqu'au premier novembre 2017. L'utilisation de ce régime d'exception, qui étend les pouvoirs de police et réduit les libertés des citoyens, est largement critiquée par les associations de défense des libertés publiques. Facilitant les perquisitions et permettant l'assignation à résidence - et donc la restriction de la liberté d'un citoyen avant même qu'il ait commis un crime - il est notamment utilisé pour cibler des militants écologistes et issus de la gauche alternative à quelques jours de la COP-21[2].

Plusieurs textes de loi vont ensuite étendre le pouvoir de la police. La loi « renforçant la lutte contre la criminalité organisée, son financement, l'efficacité et les garanties de la procédure pénale », adoptée le 8 mars 2016, permet l'instauration de premières mesures sécuritaires. Le 30 octobre 2017 est voté la loi SILT (sécurité intérieure et la lutte contre le terrorisme) qui fait entre autres entrer l'assignation à résidence dans le droit commun.

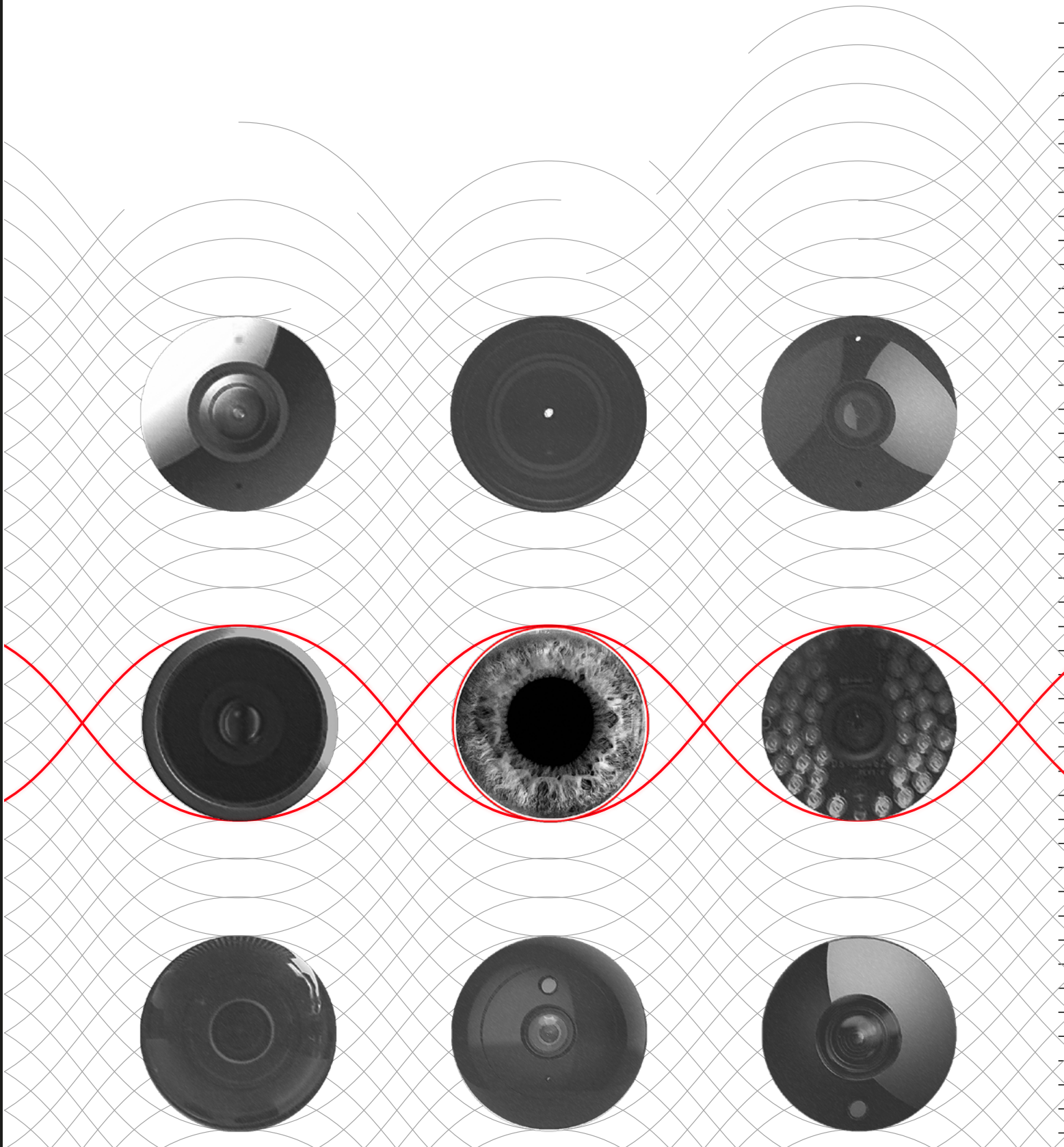
Hérité de ce contexte, le mandat d'Emmanuel Macron est lui aussi marqué par une série de réformes sécuritaires. Le mouvement des gilets jaunes, largement réprimé et marqué par d'importantes violences policières, donne lieu à un texte portant sur la liberté de manifester dit « loi anti-casseur » qui permet notamment d'interdire, de manière préventive, à une personne suspectée de pouvoir représenter un trouble à l'ordre public de participer à une manifestation.

Au-delà de la pandémie, l'année passée a elle aussi été marquée par d'importants mouvements sociaux contre les violences policières mais aussi, fin 2020, contre le projet de loi sécurité globale. Réforme majeure du gouvernement d'Emmanuel Macron, cette proposition de loi, est critiquée de toute part pour les menaces qu'elle fait peser sur les libertés publiques. Elle prévoit, entre autres, l'interdiction de filmer la police, la généralisation de la vidéosurveillance par drones ou encore des caméras-piétons. Dénoncé par la défenseure des droits parce que présentant *« des risques considérables d'atteinte à plusieurs droits fondamentaux »*, le projet de loi, qui pour l'ONU porte *« une atteinte disproportionnée aux libertés fondamentales »* et est *« susceptible de porter préjudice à l'État de droit »*, a été adopté par le Parlement le 15 avril dernier. Un tournant pour les libertés publiques en France.

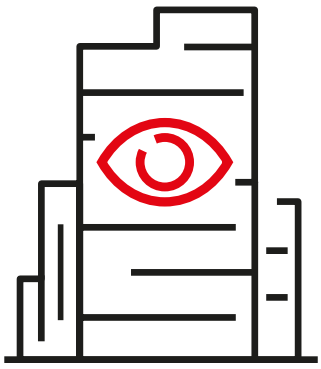
2 Human Rights League press release, 26 November 2015, "Home Secretary loses his nerves, confuses and equates associative movement with terrorism"
https://www.ldh-france.org/ministre-linterieur-perd-ses-nerfs-confond-assimile-mouvement-associatif-au-terrorisme/

En France, la surveillance rogne sur les libertés publiques

TENDANCES



TENDANCE 1:



SAFE CITY,
UNE VILLE NUMÉRISÉE AU SERVICE DE LA SÉCURITÉ

Au cœur des discours des professionnels de la sécurité, la Safe City s'inspire directement de la Smart City, ville intelligente au sein de laquelle les nouvelles technologies pensent un service public – gestion de l'eau, des déchets, transports en commun… – plus efficace et moins coûteux. Cette façon de voir la ville naît au début des années 2000 aux Etats-Unis, portée par les sociétés IBM et Cisco. *« Safe City » et « Smart City » sont les deux faces d'un même projet technosolutionniste qui prétend pouvoir gouverner un peuple comme on gère un système informatique »*. écrivent Yaël Benayoun et Irénée Régnauld dans leur ouvrage *« Technologies partout, démocratie nulle part. »* Dans une *« Safe City »*, les capacités numériques se mettent au service de la sécurité. Stationnement gênant, vol, trafic de drogue, crime, terrorisme… Qu'importe la gravité des faits, la technologie est censée répondre à ce *« sentiment d'insécurité »*, élément de langage dont abusent certains politiques.

En France, la Safe City se rattache à une métropole du sud-est de la France, Nice. Avec 3 800 caméras de vidéosurveillance, la ville dirigée par Christian Estrosi est aujourd'hui la plus surveillée de France. Sur fond de menace terroriste, le maire multiplie les initiatives pour tenter de renforcer la sécurité de sa ville.

Les technologies de surveillance ont pourtant déjà montré leurs limites à Nice. Le 14 juillet 2016, jour de la fête nationale française, en début de soirée, un terroriste fonce sur la promenade des Anglais, avenue la plus célèbre et touristique de la ville, à bord d'un camion et tue 86 personnes. La veille, il avait commis plusieurs

infractions dans la ville, sans que les nombreuses caméras ne sonnent l'alerte.

Un échec réfuté par Christian Estrosi qui, plutôt que de désavouer son système, considère les dispositifs en place insuffisants. Décision est prise. Sa « ville martyre » deviendra la première « Safe City » française, dans le cadre d'un partenariat avec l'entreprise Thales, noué en 2018[3]. Pendant 3 ans, l'entreprise a carte blanche pour y déployer ses technologies sécuritaires. Une ville transformée en terrain d'expérimentation, avec un objectif : construire un territoire numérique et surveillé, où la technologie se met au service de la sécurité.

Les milliers d'heures d'enregistrements de vidéosurveillance sont compilées au sein du Centre de supervision urbain (CSU), poumon du système de surveillance niçois. Répartis dans trois salles, les opérateurs vidéo scrutent en temps réel 90 écrans. La première pièce tente de constater les infractions en flagrance. La seconde retranscrit les images des écoles – Nice a fait installer une caméra devant chaque établissement – et celles des 900 caméras du réseau de bus et de tramways. Dans la dernière, les agents verbalisent en temps réel et s'occupent de la gestion du trafic routier. La ville s'est également dotée d'un « hyperviseur de sécurité », à savoir un écran tactile qui centralise caméras, boutons d'alerte, feux de circulation, contrôles d'accès des bâtiments.

Dans le cadre du projet Safe City mené en partenariat avec Thales, la ville a d'abord expérimenté le 27 juin 2019 un scénario de gestion d'inondation, qui a mobilisé une technologie de patrouille connectée et s'est concentré sur la sécurisation des routes et des écoles. Le 19 décembre 2019, ce sont les visiteurs du marché de Noël qui ont servi de cobaye. La prochaine expérimentation, initialement programmée pour novembre 2020, prévoyait un énigmatique scénario de gestion de crise, alliant algorithmes prédictifs, système vidéo d'analyse des comportements, système de surveillance des réseaux sociaux et, surtout, une nouvelle expérimentation autour de la reconnaissance faciale[4].

Dès 2017, un autre projet de Safe City s'esquissait en France, dans la quartier des affaires de La Défense, à l'ouest de Paris. Thales prévoyait alors la construction d'un centre de supervision urbaine, auquel seraient directement connectés les pompiers et les policiers pour aiguiller leur intervention. Les 1200 caméras de vidéosurveillance de l'espace public du quartier des affaires auraient été reliées à un logiciel permettant de *« detecter les comportements anormaux. »* Sans que Thales ou La Défense en donne les raisons, le projet a finalement avorté avant même d'être lancé[5].

3 Thales group website, "Nice: security at the cutting edge of technology". https://www.thalesgroup.com/fr/monde/defence-and-security/news/nice-securite-pointe-technologie

4 Clément Pouré et Clément le Foll (2020), Les Jours, "Nice, le « little brother » de Thales" https://lesjours.fr/obsessions/thales-surveillance/ep1-nice-safe-city/

5 David Livois (2017), le Parisien, "For its safety, La Défense will soon be full of sensors" https://www.leparisien.fr/hauts-de-seine-92/pour-sa-securite-la-defense-bientot-truffee-de-capteurs-20-03-2017-6780270.php

D'autres collectivités développent un modèle similaire à celui de la ville de Christian Estrosi. En décembre 2017, la ville de Marseille annonçait ainsi le lancement de son « Observatoire Big Data de la tranquillité publique» destiné à « analyser ce qui s'est passé » (en matière de criminalité et de délinquance) pour « anticiper la situation future ou probable ». Le projet, qui utilise des données issues des collectivités territoriales et des forces de l'ordre, s'articule autour d'un dispositif plus large : un réseau de plus de 2000 caméras de vidéosurveillance « intelligentes », l'utilisation de données issues des hôpitaux publics ou encore la surveillance des réseaux sociaux.

ENTREPRISES IMPLIQUÉES

Les projets de Safe City sont menés par Thales, entreprise spécialisée dans l'aéronautique, la défense et la sécurité. Avant de déployer sa Safe City en France, Thales l'a testée à partir de 2009, à Mexico[6]. Doté d'un pharaonique budget de 460 millions de dollars, le dispositif a permis l'installation de 15 000 caméras de vidéosurveillance, 10 000 boutons d'appel d'urgence, 850 systèmes capables de scanner les plaques d'immatriculation des véhicules et 6 centres de supervision qui analysent les images 24/24.

A Nice, Thales est à la tête d'un consortium de 15 entreprises. Le projet se chiffre à 25 millions d'euros, dont 10,9 millions d'euros directement extraits des caisses de la Banque publique d'investissement[7], un organisme français de financement et de développement des entreprises créé en 2012.

Idemia est une entreprise française née en 2017 de la fusion de Morpho, la branche identité et sécurité de la société spéicalisée dans l'aéronautique et spatial Safran, et de l'entreprise Oberthur Technologies. L'entreprise est aujourd'hui spécialisée dans l'identité biométrique. Dans le cadre du projet Safe City niçois, Idemia a mis au point deux logiciels. Le premier est capable de detecter automatiquement les plaques d'immatriculations et les images permettant d'identifier la couleur, la marque du véhicule, ainsi qu'un écriteau annonçant le transport de matières dangereuses. Le second système est lui chargé de détecter des comportements définis comme suspects ou dangereux. « *Ce type de système signale notamment les accidents, les véhicules empruntant les mauvaises files, les poids lourds non autorisés, et alerte un opérateur dans une salle de contrôle ou exécute une procédure prédéfinie*[8].»

6 Thales group website « Mexico : une ville plus sûre »
https://www.thalesgroup.com/fr/monde/securite/news/mexico-une-ville-plus-sure

7 Press release from the public investment bank, "The innovative SafeCity project, to strengthen the security of smart cities in the region, obtains funding from the Future Investments Program (PIA)"
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/

8 Quadrature du Net website, "Experimentation, provision and demonstration agreement: SafeCity 'experimentation project'"
https://data.technopolice.fr/api/files/1565879613407ce0u67yomk.pdf

Créé en 2003, Deveryware est une société française spécialisée dans la cybersécurité. Elle développe des plateformes de géolocalisation en temps réel, de lutte contre la fraude ou de gestion de crise et des communications d'urgence. Aujourd'hui, l'entreprise compte 140 collaborateurs et un chiffre d'affaires de 37 millions d'euros. Parmi ses clients : les Ministères français de l'Intérieur, de la Justice, de l'Économie et des Finances, mais aussi des entreprises comme Total, Axa, Veolia, SNCF, RTE[9]. Le projet Safe City utilise le logiciel «Notico-Safe» de Deveryware, développé grâce à des projets de recherche et développement européen, dont le but est d'alerter simultanément des citoyens sur leur smartphone en cas de danger ou de catastrophe naturelle. En plus de cette fonctionnalité, Deveryware a pensé un appel d'urgence 112 nouvelle génération, permettant aux citoyens d'être mis en relation avec le centre de secours (CTA) le plus proche. Deux systèmes qui, pour fonctionner, doivent géolocaliser les citoyens à partir de leur smartphone.

A Marseille, c'est l'entreprise Engie Ineo devenue depuis Engie Solution, qui est à la manœuvre pour le projet d'« observatoire big data de la tranquilité publique ». Le leader du marché de la vidéosurveillance, filiale du groupe Engie, est aussi partie prenante du projet de Safe City niçoise.

IMPACT SUR LES LIBERTÉS PUBLIQUES

Le développement de la Safe City niçoise pose plusieurs problèmes pour l'opposition politique et les militants associatifs de la ville. Ils dénoncent l'opacité du projet alors même qu'il impacte directement les citoyens niçois. Dans la convention de partenariat signée entre la ville de Nice et le consortium d'entreprises, ces dernières s'inquiètent d'un potentiel « *changement de paradigme et des politiques qui placeraient la sécurité sur un second plan.* » Pour que le projet fonctionne, il faut que le maire continue de mettre la sécurité à l'ordre de ses priorités. Ils jouent ainsi sur les « peurs » inconscientes de sa population, en définissant sa ville « *sous le prisme de l'insécurité, comme lieux de désorganisation sociale* », comme le définit Myrtille Picaud,[10] chercheuse associée à la chaire « Villes et numérique » de l'Ecole urbaine de Sciences Po et au Centre d'études européennes et de politique comparée (CEE).

Certains membres de l'opposition niçoise s'inquiètent de ce discours sécuritaire, comme l'ancien conseiller municipal socialiste Paul Cuturello, qui a tenté de questionner la municipalité lors de l'adoption de la convention de partenariat.

9 Site web de Deveryware, "Deveryware : Qui sommes-nous ?" https://www.gicat.com/membre/deveryware/

10 Myrtille Picaud (2020), The Conversation France, "Fear of the city: the 'safe cities' market" https://theconversation.com/peur-sur-la-ville-le-marche-des-safe-cities-138313

« C'est très dérangeant. La sécurité publique passe au second plan derrière les ambitions commerciales des sociétés du consortium[11]*. »*

D'autres hommes politiques s'inquiètent que ce projet aboutisse à de la surveillance de masse des citoyens et qu'il puisse être détourné pour espionner les militants, activistes et opposants politiques. Dès 2018, quelques mois avant la mise en place du Règlement général de protection des données, texte européen qui renforce les contraintes de collecte et de traitement, la Commission nationale de l'informatique et des libertés, chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, s'inquiétait du développement des Smarts Cities, dont la Safe City est le penchant sécuritaire. *« La possibilité de l'anonymat dans la ville est en train de s'évanouir »*, écrivait-elle[12].

L'antenne locale de la Ligue des droits de l'Homme, association de défense des libertés individuelles française fondée en 1898, partage ce constat et s'inquiète du fait que la ville de Nice conserve les données collectées et se substitue ainsi aux services de la police nationale. *« Le rôle d'une commune n'est pas de développer un service des renseignements généraux bis, lequel, fatalement, finirait par servir les intérêts partisans de la petite équipe au pouvoir*[13]*. »* Dans une Safe City, la détection des « comportements anormaux » est définie par des algorithmes et donc biaisée par ceux qui les ont créés, soulevant le risque que certaines populations ou personnes soient stigmatisées.

L'association La Quadrature du Net parle elle de « militarisation de l'espace public », avec des sociétés privées comme Thales, dont l'activité historique est de construire des systèmes qui sont ensuite utilisés sur des champs de bataille et théâtres de guerre, qui ont au fil du temps adapté leurs technologies et les déploient désormais dans l'espace public. Avec la Safe City, c'est l'ensemble des mouvements et des données personnelles d'un citoyen qui pourraient être collectées, analysées par des algorithmes, dans le simple but de pouvoir ensuite anticiper ses comportements futurs : déplacements, rencontres, achats. Dans cette vision sécuritaire de la ville développée à Nice, la sécurité de la population, compétence de la municipalité elle-même, est sous-traitée à une entreprise privée. *« Se retrouvent dans l'administration de nos espaces publics des logiques de marché, de concurrence, de normalisation qui y sont totalement étrangères et qui ne peuvent conduire qu'à des dérives, la première étant d'en faire des terrains d'expérimentations pour ces start-ups qui peuvent développer en toute impunité leurs outils de surveillance »*, développe la chercheuse Myrtille Picaud[14].

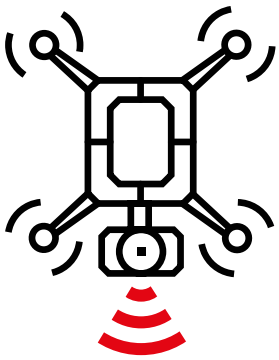
11 Clément Pouré et Clément le Foll (2020), Les Jours, "Nice, le « little brother » de Thales" https://lesjours.fr/obsessions/thales-surveillance/ep1-nice-safe-city/

12 Guénaël Pépin (2017), NextImpact, "Smart city: the CNIL paints a grim picture for individual freedoms". https://www.nextinpact.com/article/27434/105426-smart-city-cnil-dresse-tableau-sombre-pour-libertes-individuelles

13 Website of the Human Rights League of Nice (2018), "Observation n° 7, Response to the mayor of nice: 'safe city' or 'allo mairie'?" https://site.ldh-france.org/nice/2018/08/27/safe-city-criminogene/

14 Clément Pouré & Clément le Foll (2020), Lesjours.fr, "The security thought colonizes the management of the city" https://lesjours.fr/obsessions/thales-surveillance/ep4-interview-picaud-castagnino-surveillance/

TENDANCE 2:



UTILISATION DE **DRONES** DANS L'ESPACE PUBLIC

C'est à Istres, ville de 43 000 habitants située dans le sud-est, à quelques dizaines de kilomètres de Marseille, que des drones policiers ont pour la première fois volé dans le ciel français. Seules la police nationale et la gendarmerie les avaient utilisées jusqu'à présent dans le cadre de l'expulsion de la zone à défendre de Notre-Dame-Des-Landes[15].

En avril 2018, le maire François Bernardini (divers gauche) annonce qu'il équipe sa police municipale (composée de 80 personnes) de deux drones. Munis de caméras Ultra HD enregistrant 30 images par seconde, ces drones diffusent avec quelques millisecondes de décalage les images filmées sur les écrans du centre de supervision urbain de la ville. « *Ils offrent un moyen supplémentaire au service de la sécurité quotidienne, mais aussi pour la surveillance des massifs forestiers l'été ou des nombreuses fêtes ou festivals que nous organisons en extérieur. C'est une technologie*

15 Pascal Simon (2018), Ouest France, "Notre-Dame-des-Landes: How the Gendarmes used drones" https://www.ouest-france.fr/pays-de-la-loire/notre-dame-des-landes-44130/notre-dame-des-landes-comment-les-gendarmes-ont-utilise-les-drones-5894651

d'avenir, tout le monde y viendra », prédit alors François Bernardini[16].

Force est de constater que le maire d'Istres à vu juste. L'épidémie de COVID-19 a servi de justification aux maires des quatre coins de la France pour équiper leur police municipale de drones. Le ministère de l'Intérieur s'est lui chargé de fournir ceux utilisés par la gendarmerie et la police nationale. L'objectif de cette surveillance par drone : s'assurer du respect du confinement. A Lyon[17], la police nationale et la direction départementale de la sécurité publique ont utilisé des engins volants pour faire respecter les mesures de confinement. « *Police nationale. Tout déplacement est interdit. Rentrez chez vous* », prononce l'aéronef à la vue de livreurs de nourritures, qui ont eux continué à travailler et discutaient en attendant la préparation des commandes de nourritures.

Des hélicoptères et des drones ont également survolé les littoraux, pour surveiller les promeneurs qui se baladaient le long des plages ou pour accéder à des zones que les policiers ne peuvent pas atteindre en marchant. Près de Montpellier, deux drones ont été utilisés pour surveiller les plages de Palavas et de Carnon. Mais ils permettent également aux forces de l'ordre de surveiller les quartiers populaires. « *Le but des drones c'est de faire une reconnaissance pour savoir si on a des points de fixation dans les quartiers et éviter d'envoyer une équipe pour qu'elle se retrouve dans une embuscade. Il y a des poches de résistance. Les individus qui sont toujours au même endroit et qui vont être verbalisés à quatre ou cinq reprises seront sanctionnés pour mise en danger délibérée de la vie d'autrui, ils pourront être placés en garde à vue* », explique Yannick Blouin, le directeur départemental de la sécurité publique de l'Hérault[18].

A Cannes, également dans le sud-est de la France, le maire David Lisnard, qui a déployé toutes sortes de gadgets en espérant qu'ils permettraient de freiner l'épidémie, a vaporisé de l'eau de javel avec un drone pour tenter de désinfecter un des marchés de la ville[19]. Paris n'a pas été épargné. De nombreux drones ont surveillé la capitale française pendant le premier confinement. Au total, plusieurs dizaines de villes ont été scrutées par des drones durant le premier confinement français du 17 mars au 10 mai 2020.

16 Marc Leras (2018), Le Parisien, "Istres: the municipal police acquire surveillance drones, a first" https://www.leparisien.fr/faits-divers/istres-la-police-municipale-se-dote-de-drones-de-surveillance-une-premiere-11-04-2018-7659057.php

17 Catherine Lagrange (2020), Le Parisien, "National Police. Go home: in Lyon, drones enforce confinement" https://www.leparisien.fr/societe/police-nationale-rentrez-chez-vous-a-lyon-les-drones-font-respecter-le-confinement-10-04-2020-8297343.php

18 Joane Mériot (2020), France 3 Occitanie, "Coronavirus: helicopters and drones to enforce confinement in Hérault" https://france3-regions.francetvinfo.fr/occitanie/herault/coronavirus-helicopteres-drones-faire-respecter-confinement-herault-1804528.html

19 Alexandre Carini (2020), Nice Matin, "Cannes is experimenting with a drone to disinfect the Bocca market" https://www.nicematin.com/vie-locale/cannes-experimente-un-drone-pour-desinfecter-le-marche-de-la-bocca-493890

Le COVID-19 n'est pas l'unique raison invoquée pour généraliser les drones : la crise migratoire en est une autre. Depuis plusieurs années, la surveillance des frontières françaises se fait parfois à l'aide de drones, notamment celles avec la Belgique[20]. Plus récemment, l'armée britannique a utilisé un drone pour survoler la Manche, qui sépare le Royaume-Uni de la France[21]. En ligne de mire, la cité frontalière de Calais, ville française où la pression migratoire est la plus forte et où les réfugiés sont harcelés et vivent dans des conditions inhumaines. En avril 2020, le ministère de l'Intérieur a lancé un appel d'offres portant sur l'acquisition de 650 drones[22] pour la gendarmerie nationale, police nationale et sécurité civile, soit le double du nombre de drones qui seraient actuellement entre les mains des forces de l'ordre.

ENTREPRISES IMPLIQUÉES

DJI est une entreprise chinoise, leader mondial dans la fabrication de drones de loisir, professionnels et pour entreprise, créée en 2006 par Frank Wang. La société fondée à Shenzhen a récemment été interdite aux Etats-Unis, le gouvernement estimant que leur utilisation faisait courir un risque d'espionnage de la part du régime chinois[23]. Par le biais du distributeur français Flying Eyes, une quinzaine de modèles DJI Mavic Enterprise[24] ont été utilisés par la préfecture de police de Paris pendant le confinement, acquis le 18 mars 2020, dans le cadre d'un marché public de type accord-cadre. Le 2 mars, Mediapart révélait que le ministère de l'Intérieur avait à nouveau commandé 600 drones de ce modèle pour agrandir sa flotte d'aéronefs.

Parrot, entreprise française créée en 1994 et spécialisée dans le numérique et les objets connectés a été sélectionnée le 12 janvier 2021 par le ministère des Armées pour fournir 300 micro-drones, qui devraient être livrés à partir de juin 2021. Ils seront utilisés pour des missions de reconnaissance et de renseignement. Capable de voler pendant trente minutes, ils pèsent moins de 500 grammes et peuvent voler de jour comme de nuit. « *En mesure de détecter des cibles de taille humaine avec une grande précision jusqu'à deux kilomètres de distance, particulièrement discret et même inaudible à plus de 130 mètres, il peut être mis en œuvre*

20 Bruno Susset (2018), Est Républicain, "Belgian drones to monitor the border between France and Belgium" https://www.estrepublicain.fr/le-mag/2018/12/07/des-drones-douaniers

21 George Allison, 2020, UK Defense Journal, "Watchkeeper drone carries out border patrol over the English Channel" https://ukdefencejournal.org.uk/watchkeeper-drone-carries-out-border-patrol-over-the-english-channel/

22 Fabien Leboucq (2020), Liberation, "Why has the Interior Ministry just ordered drones?" https://www.liberation.fr/checknews/2020/04/15/pourquoi-le-ministere-de-l-interieur-vient-il-de-commander-des-drones_1785166/

23 BBC (2020), "Chinese drone and chip makers added to US banned list" https://www.bbc.com/news/technology-55367163

24 DJI website, " Mavic 2 Enterprise series" https://www.dji.com/fr/mavic-2-enterprisehttps://www.dji.com/fr/mavic-2-enterpris

en moins d'une minute », explique le ministère des Armées[25].

Le géant de la défense et de l'aérospatial Thales, dont l'État français et l'entreprise Dassault Aviation sont les actionnaires majoritaires, est lui impliqué dans la construction du drone Watchkeeper WK 450,26 utilisé en septembre 2020 par l'armée britannique pour une opération de surveillance des frontières britanniques et françaises. Pour concevoir ce drone, initialement déployé en Afghanistan sur les terrains militaires par l'armée britannique, Thales s'est associé à l'entreprise israélienne Elbit.

Fondée en 1953, cette dernière entreprise s'est fait connaître en développant le modèle de drones Hermes. Il y a quelques mois, le Canada a déboursé plus de 36 millions de dollars pour obtenir un Hermes 900 StarlLiner[27], qui sera chargé de faire de la surveillance maritime. Elbit est également à l'origine de nombreuses controverses. En 2018, le média d'investigation américain *The Intercept* révélait qu'un drone Hermes 450 avait été utilisé en 2014 par l'armée israélienne pour bombarder la bande de Gaza en Palestine, tuant quatre enfants[28].

Drone Watchkeeper WK 450, coproduit par Thales et Elbit.

25 Site du minisitère de la défense, "Le ministère des Armées commande de nouveaux micro-drones de reconnaissance et de renseignement" https://www.defense.gouv.fr/actualites/articles/le-ministere-des-armees-commande-de-nouveaux-micro-drones-de-reconnaissance-et-de-renseignement

26 Site du groupe Thalès, " Système de drone tactique Watchkeeper" https://www.thalesgroup.com/fr/worldwide/defense/drone-tactique-watchkeeper

27 Levon Sevunts (2020), RCINET, "Canada buys Israeli drone for Arctic maritime surveillance" https://www.rcinet.ca/eye-on-the-arctic/2020/12/22/canada-buys-israeli-drone-for-arctic-maritime-surveillance/

28 Secret Israeli Report Reveals Armed Drone Killed Four Boys Playing on Gaza Beach in 2014 https://theintercept.com/2018/08/11/israel-palestine-drone-strike-operation-protective-edge/

IMPACT SUR LES LIBERTÉS PUBLIQUES

Depuis le début de la pandémie, des drones ont été utilisés pour surveiller au moins cinq manifestations parisiennes et ont permis d'interpeller plusieurs militants du syndicat de la santé qui ont mené une action non-violente le 14 juillet 2020[29]. L'extension de plusieurs fichiers de renseignement (voir partie V), le projet de légalisation de la surveillance par drone via le projet de loi sur la sécurité globale et la prolifération des outils de reconnaissance faciale inquiètent particulièrement les associations de défense des libertés publiques, qui y voient un outil pouvant être détourné pour surveiller les militants.

L'utilisation de drones par les forces de l'ordre a immédiatement suscité une rébellion des groupes de défense des libertés civiles et des avocats. Le flou juridique qui accompagne leur utilisation était en cause.

Le cadre juridique de l'utilisation des drones est particulièrement instable. Il est défini par l'arrêté du 17 décembre 2015[30], qui fixe les conditions d'utilisation « *de l'espace aérien par les aéronefs qui circulent sans personne à bord* », et qui prévoit que chaque vol de drone soit déclaré en préfecture au moins cinq jours ouvrés avant le vol. Cependant, cet arrêté exempte de toute déclaration de vol la police nationale et la gendarmerie à partir du moment où « *les circonstances de la mission et les exigences de l'ordre et de la sécurité publics le justifient.* »

Dans le cas de cet usage, les forces de l'ordre peuvent utiliser leur drone sans que les citoyens sachent s'ils sont filmés, si les images sont transmises ou enregistrées et les données conservées. Une opacité qui fait craindre des atteintes à la vie privée et au respect des données personnelles. Surtout qu'initialement déployés pour survoler les principaux axes routiers, les drones sont depuis plusieurs mois utilisés pour surveiller les manifestations.

Avocat au barreau de Paris, Thierry Vallat, spécialiste du droit numérique, pointe une utilisation de plus en plus invasive des drones au fur et à mesure que ces technologies ont gagné en maturité. « *De la surveillance de massifs forestiers, leur utilisation s'est étendue aux manifestations de gilets jaunes et aux événements sportifs*[31]*.* »

Face à cette absence de cadre juridique, le Conseil D'État, plus haute juridiction administrative française, qui avait été saisi par les associations de défense des libertés publiques La Quadrature du Net et la Ligue des droits de l'Homme, a enjoint le 18 mai 2020 à l'État de cesser « *sans délai* » d'utiliser des drones à Pa-

29 Clément Pouré & Clément le Foll (2020), Médiapart, "Taking advantage of legal vagueness, police drones are still buzzing" https://www.mediapart.fr/journal/france/261020/profitant-du-flou-juridique-les-drones-policiers-bourdonnent-toujours

30 Légifrance, "Order of 17 December 2015 relating to the use of airspace by aircraft traveling without anyone on board" https://www.legifrance.gouv.fr/loda/id/JORFTEXT000031679868/

31 Clément Pouré & Clément Le Foll (2020), Médiapart, "With containment, drones are intruding into public space" https://www.mediapart.fr/journal/france/250420/avec-le-confinement-les-drones-s-immiscent-dans-l-espace-public

ris pour surveiller le respect des règles du déconfinement.[32] Le Conseil d'État a estimé que les drones pouvaient évoluer à des distances permettant une identification des individus. « *Dans ces conditions,* note le Conseil d'État, *les données susceptibles d'être collectées par le traitement litigieux doivent être regardées comme revêtant un caractère personnel* ». La juridiction exige que l'État cesse « *sans délai, de procéder aux mesures de surveillance par drone* » tant qu'un texte réglementaire, pris après avis de la Commission nationale de l'informatique et des libertés, le gendarme français du numérique, n'aura pas clarifié leur usage.

Malgré cette décision, dont le champ d'action devait concerner toute la France, les forces de l'ordre ont continué à déployer des drones pour filmer les différentes manifestations, faisant craindre une atteinte à la liberté de manifester. « *La collecte d'informations [par le biais de drones – ndlr] sur les participants à une action de la CGT ou une manifestation organisée par un mouvement religieux relève pour nous d'un traitement de données sensibles injustifié* », rappelle Martin Drago, juriste à La Quadrature du Net[33].

Alors que la préfecture de police de Paris justifiait l'usage des drones par le recours à un logiciel capable de flouter les silhouettes captées par les images des drones, et ainsi anonymiser les données, une enquête de Mediapart expliquait en novembre que ce logiciel n'était efficace que dans 70% des cas[34].

Fin décembre, le Conseil d'État a ordonné cette fois-ci au préfet de police de Paris Didier Lallement de cesser d'utiliser des drones pour surveiller les manifestations, une seconde victoire pour les défenseurs des libertés publiques, particulièrement La Quadrature du Net, à l'origine du recours[35]. Un camouflet pour le gouvernement français, qui prévoit un élargissement de l'utilisation des drones à travers l'article 22 de la proposition de loi sécurité globale.

Dès le début de l'année 2018, les drones ont été utilisés dans le cadre de l'expulsion et de la surveillance de la ZAD de Notre-Dame-Des-Landes[36]. Sur certaines journées, 6 à 7 drones ont survolé la zone, tout comme des hélicoptères des forces de l'ordre. « *Il facilite l'appui tactique des unités au sol. Cela nous permet d'observer de très près, et en discrétion, ce qui se passe derrière une haie, de repérer des individus préparant des munitions…* », expliquait à *Ouest-France*[37],

32 Council of State (2020), "Decision on drone surveillance in the context of deconfinement" https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones

33 Clément Pouré & Clément le Foll (2020), Médiapart, "Taking advantage of legal vagueness, police drones are still buzzing" https://www.mediapart.fr/journal/france/261020/profitant-du-flou-juridique-les-drones-policiers-bourdonnent-toujours

34 Clément Pouré & Clément le Foll (2020), Médiapart, "Drones: when it comes to blurring the demonstrators, the police are less careful" https://www.mediapart.fr/journal/france/181120/drones-quand-il-s-agit-de-flouter-les-manifestants-la-police-moins-regardante

35 La Quadrature du Net (2020), "Interdiction des drones victoire totale contre le gouvernement" https://www.laquadrature.net/2020/12/22/interdiction-des-drones-victoire-totale-contre-le-gouvernement/

36 Pascal Simon (2018), Ouest France, "Notre-Dame-des-Landes: How the Gendarmes used drones" https://www.ouest-france.fr/pays-de-la-loire/notre-dame-des-landes-44130/notre-dame-des-landes-comment-les-gendarmes-ont-utilise-les-drones-5894651

37 Idem

le lieutenant-colonel Henri Dulong de Rosnay, commandant du groupement des forces aériennes de gendarmerie Ouest.

Les drones de la police et la gendarmerie nationale ont également été régulièrement utilisés pour surveiller des manifestations, notamment du mouvement des gilets jaunes. Dans un article publié par Mediapart, trois militants du collectif Inter-Urgences participant à une marche organisée à l'appel de syndicats de soignants et soutenue par les gilets jaunes, ont témoigné avoir été identifiés grâce à des drones après avoir déployé une banderole accusant le président français Emmanuel Macron « d'asphyxier l'hôpital. » comment les drones peuvent permettre à la police de surveiller des activistes dans des lieux où ils ne peuvent pas aller, mais également d'interpeller des militants en exploitant les images filmées.

Depuis le début de la pandémie, et ce malgré un premier arrêt du Conseil d'État pointant l'absence de cadre légale entourant l'utilisation de drones dans le cadre du déconfinement, les drones ont été utilisés pour surveiller au moins cinq manifestations parisiennes et ont été utilisés pour arrêter plusieurs militants syndicaux du domaine de la santé ayant réalisé une action coup de poing non violente le 14 juillet 2020[38].

Début janvier, la Commission nationale informatique et libertés a sanctionné l'usage des drones par le gouvernement français. Dans son avis, l'autorité explique que le mécanisme de floutage développé par le ministère de l'Intérieur n'a été mis en place qu'au mois d'août, alors que de nombreux vols avaient été déjà réalisés. « *De plus, ce mécanisme ne peut pas être exécuté directement par le drone. Des images contenant des données personnelles sont donc collectées, transmises et traitées par le ministère de l'Intérieur avant que ce système de floutage ne soit appliqué* », s'insurge la CNIL.

38 Clément Pouré & Clément le Foll (2020), Médiapart, "Taking advantage of legal vagueness, police drones are still buzzing" https://www.mediapart.fr/journal/france/261020/profitant-du-flou-juridique-les-drones-policiers-bourdonnent-toujours

TENDANCE 3:

RECONNAISSANCE FACIALE ET BIOMÉTRIE

Le recours à la reconnaissance faciale en temps réel dans l'espace public est indissociable d'une ville du sud de la France, à la pointe des technologies de surveillance : Nice. En février 2019, le carnaval de la ville, qui s'étale sur deux jours, a été le théâtre de la première expérimentation de reconnaissance faciale dans l'espace public en France. Plusieurs caméras placées à l'une des entrées de l'événement étaient chargées d'identifier 50 personnes volontaires. Suite à cette expérimentation, la ville de Nice s'est réjouit que l'algorithme ait pu reconnaître ces 50 individus. La CNIL est plus réservée, estimant , dans un rapport rédigée à l'issu de l'expérimentation , que le bilan d'expérimentation transmis par Nice était incomplet et ne permettait pas de tirer de conclusions sur sa réussite[39].

En décembre 2018, toujours dans le sud de la France, le conseil de la région Sud (anciennement PACA) a autorisé une expérimentation pour installer des por-

39 Le Journal du Net (2019), "Facial recognition experimentation: Nice delighted, Cnil skeptical" https://www.journaldunet.com/economie/services/1443319-reconnaissance-faciale-nice-ravie-la-cnil-sceptique/

tiques de reconnaissance faciale dans deux lycées : le lycée des Eucalyptus à Nice et le lycée Ampère à Marseille[40].

Depuis plusieurs années, les aéroports parisiens de Roissy Charles de Gaulle et Orly, respectivement fréquentés par 76,2 millions et 31,9 millions de voyageurs en 2019, sont équipés de portiques de reconnaissance faciales, appelés SAS PARAFE[41] (pour passage automatisé rapide des frontières extérieures). Ces dispositifs sont également installés aux aéroports de Marseille-Provence, Lyon Saint-Exupéry, Nice, ainsi qu'à la Gare du Nord de Paris et de Saint-Pancras à Londres. Ils sont aussi déployés au départ d'Eurotunnel pour les autocars.

Il y a quelques mois, l'État Français a également voulu amener la reconnaissance faciale dans le quotidien des Français, en lançant ALICEM, une application pour smartphone développée par le ministère de l'Intérieur et l'Agence nationale des titres sécurisés (ANTS). Son but: permettre à tout particulier de prouver son identité sur Internet à l'aide de son smartphone et de son passeport ou de son titre de séjour et d'accéder à différentes démarches administratives.

La proposition d'un texte de loi réglementant l'usage de la reconnaissance faciale dans l'espace public fait débat au niveau politique. Parmi ceux qui sont favorables à son application, le maire de Nice, Christian Estrosi, à l'origine de la première expérimentation sur le sol français. Du côté des parlementaires, les Jeux Olympiques 2024 qui se dérouleront à Paris, apparaissent comme l'événement parfait pour légiférer ou lancer une expérimentation grandeur nature de la reconnaissance faciale[42].

Si la reconnaissance faciale en temps réel est encore interdite en France, elle est déjà une réalité pour les forces de l'ordre. Celles-ci disposent, depuis 2011, d'un logiciel permettant de mettre en regard des images issues de vidéosurveillance ou des réseaux sociaux avec celles contenues dans le fichier TAJ (Traitement d'antécédents judiciaires) qui regroupe plus de 8 millions de photographies de résidentes français. Au premier semestre 2020, plus de 200 000 requêtes avaient été faites concernant ce fichier, selon le site Next Impact[43].

40 Quadrature du Net website (2019), "Facial recognition in high schools: an impossible debate?" https://www.laquadrature.net/2019/10/15/reconnaissance-faciale-dans-les-lycees-debat-impossible/

41 Website of the Ministry of the Interior, "PARAFE: passing border controls faster" https://www.interieur.gouv.fr/Actualites/Infos-pratiques/PARAFE-passer-les-controles-aux-frontieres-plus-rapidement

42 Clément Pouré and Clément Le Foll (2020), Lesjours.fr, "Thales is involved in your face" https://lesjours.fr/obsessions/thales-surveillance/ep5-reconnaissance-faciale/

43 Pierre Januel (2020), NextImpact, "Police: the massive use of facial recognition is confirmed" https://www.nextinpact.com/article/44242/police-emploi-massive-reconnaissance-faciale-se-confirme

ENTREPRISES IMPLIQUÉES

Thales Digital Identity and Security est la filiale de l'entreprise Thales, dédiée à la biométrie. Cette entité est née en 2019, lorsque Thales a conclu le rachat du spécialiste de la biométrie franco-hollandais Gemalto[44]. Avec cet achat, Thales a mis la main sur un large panel de technologies de pointe et fait son retour sur un marché qu'elle avait quitté en 2017 en cédant à IN Groupe – l'Imprimerie nationale – son activité de gestion d'identité[45] (données d'état civil, production des documents sécurisés, etc.). Deux ans plus tard, avec le rachat de Gemalto, Thales s'affirme comme l'un des leaders mondiaux de la biométrie.

A travers Gemalto, Thales a récupéré la gestion des SAS PARAFE (pour passer les contrôles aux frontières plus rapidement). A l'origine basé sur la correspondance de l'empreinte biométrique, le nouveau système PARAFE, mis en place en 2018, utilise de portiques de sécurité. Placés dans les aéroports, ils exploitent les données des passeports biométriques et la reconnaissance faciale. Lors de son passage à l'aéroport, un ressortissant de l'Union européenne scanne une première fois son passeport sur un lecteur, qui ouvre un sas dans lequel l'individu s'arrête. Son visage est soumis à la reconnaissance faciale et la seconde porte s'ouvre après un délai de 10 à 15 secondes. En 2017, Gemalto a annoncé le lancement d'une solution baptisée « Fly to Gate»[46], où un individu pourrait être suivi de chez lui jusqu'à la porte d'embarquement de son vol, grâce à la reconnaissance faciale.

Thales est également impliqué dans ALICEM, un système de reconnaissance faciale développé par le ministère de l'Intérieur français en 2019. Ce dispositif d'Authentification en ligne certifié sur mobile, est en phase de test depuis juin 2019 à l'Agence nationale des titres sécurités (ANTS). Il se présente sous la forme d'une application mobile Android, qui permettra de se connecter à des services publics comme les impôts, l'assurance maladie ou la sécurité sociale grâce à une authentification par reconnaissance faciale des traits du visage. Prévu pour 2019, le lancement d'ALICEM a été retardé et devrait débuter en 2022.

Début novembre 2020, Thales annonçait son « Identity Verification Suite »[47], un projet encore au stade pilote, s'adressant aux fournisseurs de services qui souhaitent vérifier l'identité de leurs clients à distance. Il s'appuie sur la vérification biométrique via un selfie pris avec un smartphone.

44 Thales group website, "Thales and Gemalto create a world leader in digital security" https://www.thalesgroup.com/fr/thales-et-gemalto-creent-un-leader-mondial-de-la-securite-digitale

45 Ingroup website (2017), "Thales signs an agreement with the Imprimerie Nationale Group on the sale of its identity management activity" https://www.ingroupe.com/newsroom/thales-signe-un-accord-avec-le-groupe-imprimerie-nationale-sur-la-cession-de-son-activite-de-gestion-d-identite

46 Thales group website, "Border control" https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/controle-aux-frontieres

47 Thales group website, "Thales launches its new identity verification offer, a secure biometrics-based solution for remote customer enrollment" https://www.thalesgroup.com/fr/group/journaliste/press-release/thales-lance-sa-nouvelle-offre-verification-didentite-une-solution

Anyvision est une société israélienne fondée en 2015 et spécialisée dans le secteur des technologies de cybersécurité et de reconnaissance faciale. Ses fondateurs comprenaient du personnel académique et des experts en cybersécurité. Son logiciel de reconnaissance faciale "Better tomorrow » - qui revendique moins de 0,1% d'erreurs - a été couplé à des caméras de surveillance de Nice lors du carnaval, pour la première expérimentation de reconnaissance faciale dans l'espace public en France.

Cisco est une entreprise informatique américaine basée en Californie. Fondée en 1984, elle est à l'origine spécialisée dans le matériel réseau avant de s'orienter progressivement vers l'intelligence artificielle. L'entreprise avait été sélectionnée en 2019 pour coupler un logiciel de reconnaissance faciale aux caméras de deux lycées de Marseille et Nice. Un fichier numérique contenant le nom et la photo de l'élève aurait été créé par l'établissement pour générer un QR code affichable sur le téléphone. A chaque entrée dans le lycée, les élèves auraient dû scanner ce QR code sur un portique dédié, équipé d'une caméra qui aurait scanné leur visage et l'aurait comparé avec celui détenu dans le fichier[48]. Le projet a finalement été abandonné.

Idemia est une entreprise française née en 2017 de la fusion de Morpho, la branche identité et sécurité de la société spécialisée dans l'aéronautique et spatial Safran, et de l'entreprise Oberthur Technologies. L'entreprise est aujourd'hui spécialisée dans l'identité biométrique et collabore avec Thales et In Groupe sur le développement des SAS Parafe. Idemia travaille également sur la construction des bases de données indispensables au bon fonctionnement de la reconnaissance faciale.

Il y a quelques mois, la société a remporté avec une autre entreprise française, Sopra Steria, le contrat attribué par l'Union européenne pour créer une base de données biométriques pour les contrôles aux frontières de l'espace Schengen[49]. Prévue pour 2022, elle intégrera les empreintes digitales et les portraits de plus de 400 millions de ressortissants de pays tiers. Idemia planche actuellement sur un nouveau logiciel de reconnaissance faciale, appelé Augmented vision. «*Ce logiciel scrute des images de vidéosurveillance en temps réel et en post-événement. Après un attentat dans le métro, par exemple, il peut retrouver sur les images un visage figurant dans une liste d'intérêt préétablie, reconstituer des trajectoires et des interactions entre personnes*», explique Vincent Bouatou, le directeur innovation de la direction identité et sécurité publique d'Idemia[50].

48 Romain Baheux (2019), Le Parisien, "Facial recognition tested in high schools" https://www.leparisien.fr/societe/video-dans-les-lycees-et-maintenant-place-a-la-reconnaissance-faciale-04-02-2019-8004192.php

49 Sopra Steria website, "IDEMIA and Sopra Steria chosen by the French Ministry of the Interior for the development of a centralized border control system" https://www.soprasteria.fr/media/communiques/details/idemia-et-sopra-steria-choisis-par-le-ministere-de-l-interieur-fran%C3%A7ais

50 Marion Garreau (2020), L'Usine Nouvelle, "How the French Idemia exploits the biometric vein" https://www.usinenouvelle.com/editorial/comment-le-francais-idemia-exploite-le-filon-biometrique.N1026034

Le traitement du fichier TAJ se fait à l'aide d'outils développés en interne par les forces de l'ordre françaises, mais comprend également des partenariats privés. Depuis 2011[51] la police utilise le logiciel de reconnaissance faciale "Facevacs Dbscan", commercialisé par la société allemande Cognitec, qui travaille avec de nombreux intégrateurs comme Indemia et Atos.

IMPACT SUR LES LIBERTÉS PUBLIQUES

Nous sommes à Montreuil[52] le 27 février 2021. Le Marbré, un squat de la ville, organise une soirée de soutien à des militants incarcérés à Meaux suite à l'incendie d'un centre de rétention administratif. Les policiers viennent pour les expulser. Les militants résistent mais sont finalement arrêtés. Plusieurs d'entre eux refusent de donner leurs identités. Les forces de l'ordre les prennent en photo et les identifient à l'aide d'un logiciel de reconnaissance faciale. *« Certaines personnes ont été identifiées après avoir refusé de décliner leur identité,* écrivent les militants, *et que les keufs les ont photographié et comparé leurs photos via un système de reconnaissance faciale. Deux personnes parmi celles qui étaient à l'intérieur initialement ont été placées en garde à vue ».*

La multiplication des dispositifs impliquant la reconnaissance faciale inquiète de nombreux observateurs qui y voient une stratégie pour faire mieux accepter ces technologies. *« C'est en déployant de la biométrie présentée comme inoffensive que l'on crée du consentement »*, explique le journaliste spécialisé dans les sujets liés à la surveillance Olivier Tesquet[53].

Il y a quelques mois, l'association La Quadrature du Net a attaqué devant le Conseil d'État, la plus haute juridiction administrative française, les dispositions du code de procédure pénale qui autorisent la police à utiliser la reconnaissance faciale pour identifier les personnes fichées dans le TAJ (pour « Traitement des Antécédents Judiciaires »). Ce fichier contient les photographies des visages de toute personne « mise en cause » lors d'une enquête de police, qu'elles aient été condamnées ou innocentées. Le TAJ contient aujourd'hui, selon un rapport parlementaire et la CNIL, 19 millions de fiches et 8 millions de photographies de visage. *« La surveillance biométrique est exceptionnellement invasive et déshumanisante. Elle permet un contrôle invisible, permanent et généralisé de l'espace public. Elle fait de nous une société de suspects. Elle attribue à notre corps une fonction de traceur constant, le réduisant à un objet technique d'identification. Elle*

51 Gabriel Thierry (2019), l'Essor, "Why the legal challenge of facial recognition could make pschitt" https://lessor.org/a-la-une/pourquoi-contestation-judiciaire-reconnaissance-faciale-pourrait-faire-pschittt/

52 Indymedia Nantes, "Montreuil (93): expulsion from Marbré" https://nantes.indymedia.org/articles/54990

53 Clément Pouré & Clément Le Foll (2020), Lesjours.fr, "Thales is involved in your face" https://lesjours.fr/obsessions/thales-surveillance/ep5-reconnaissance-faciale/

abolit l'anonymat », explique le communiqué[54].

Comme l'explique l'association, l'un des risques qui planent autour de l'usage de la reconnaissance faciale, au-delà du fait que tout individu ne pourra plus être « anonyme » lorsque des caméras l'identifierons, est celui sur la liberté de manifester. La multiplication des fichiers de police « *sont suffisamment graves pour dissuader une large partie de la population d'exercer son droit de manifester.* » Le recours à la reconnaissance faciale dans les manifestations aurait un effet pervers sur les manifestants, qui se sentiraient surveillés dans l'exercice de ce droit. « *La possibilité de faire partie d'une foule anonyme est ce qui permet à de nombreuses personnes de participer à des manifestations pacifiques en se sentant en sécurité* », estime Amnesty International[55].

54 Quadrature du Net website (2020), "We are attacking facial recognition in TAJ" https://www.laquadrature.net/2020/08/07/nous-attaquons-la-reconnaissance-faciale-dans-le-taj/

55 Amnesty International website (2020), "As protests continue around the world, facial recognition technologies must be banned" https://www.amnesty.org/fr/latest/news/2020/06/usa-facial-recognition-ban/

TENDANCE 4:

LES LOGICIELS DE **VIDÉOSURVEILLANCE INTELLIGENTE** À L'ASSAUT DES COMMUNES

Dans son ouvrage *L'oeil sécuritaire: Mythes et réalités de la vidéosurveillance,* la sociologue Elodie Lemaire raconte notamment le quotidien de vidéo-opérateurs, en poste dans un centre de supervision urbaine et chargés de scruter les caméras et parfois d'en prendre le contrôle. Elle dépeint un métier atypique, tant par son statut que par le rôle des opérateurs, dont certains chassent la moindre infraction, alors que d'autres se contentent de regarder et communiquer sur la fluidité du trafic routier. « *En outre, si les pratiques des agents en poste derrière les caméras diffèrent, ils ont en commun de ne pas connaître l'impact réel de la vidéo-surveillance, tant sur la plan de la prévention (dissuader le passage à l'acte) que sur celui de la répression (élucider les affaires judiciaires)* », détaille la sociologue[56].

Après avoir installé des caméras dans des milliers de communes françaises, les industriels du secteur misent désormais sur ces potentielles failles des vi-

56 CNIL website (2019), Elodie Lemaire: "Video surveillance is not ideal proof" https://linc.cnil.fr/fr/elodie-lemaire-la-vidéosurveillance-nest-pas-une-test-ideale

déo-opérateurs pour tenter de vendre des logiciels d'intelligence artificielle. Couplés aux caméras déjà installées, ils permettent de se focaliser sur certains éléments : des voitures, des couleurs, une silhouette ou même de condenser plusieurs heures de vidéos en quelques secondes. Un traitement assisté par ordinateur, proche de la reconnaissance faciale mais qui n'utilise pas de données biométriques.

Un choix fait par la ville de Roubaix, dans le nord de la France. En juin 2020, la ville a inauguré son nouvel hôtel de police. Il réunit police municipale et centre de supervision urbain, qui centralise toutes les images des 123 caméras de vidéosurveillance de la ville. Le logiciel d'intelligence artificielle permet de faire de la vidéoverbalisation, de zoomer sur les individus et de surveiller en temps réel les rues, les sorties de métro ou les parkings[57]. Certaines des plus grandes villes de France, comme Lyon ou Marseille (même si le projet fait l'objet d'un audit de la municipalité) ont aussi choisi de développer la vidéosurveillance intelligente. Cette technologie est également utilisée depuis 2014 par la police nationale dans le cadre d'enquêtes criminelles[58].

ENTREPRISES IMPLIQUÉES

Briefcam est une entreprise israélienne, spécialisée dans la production de logiciels d'analyse d'images de vidéosurveillance. Elle a été fondée en 2008 sur la base de la technologie VIDEO SYNOPSIS, développée par Shmuel Peleg, chercheur à l'Université hébraïque de Jérusalem. Briefcam est une filiale de l'entreprise japonaise Canon, qui détient d'autres entreprises du secteur de la vidéosurveillance comme Axis ou Milestones.

Couplé à une caméra, le logiciel VIDEO SYNOPSIS permet à l'opérateur vidéo d'appliquer de nombreux filtres aux images filmées. Il est possible de se focaliser sur les véhicules à deux roues, les camionnettes, trains ou bus, mais aussi de repérer certains types de vêtements par couleur ou selon la longueur de leur manche. Le logiciel permet également de repérer des objets et personnes selon leur taille, trajectoire et d'effectuer des recherches par plaque d'immatriculation. En 2020, l'entreprise affirme être présente dans 30 villes françaises, Roubaix, Vannes, Nice ou Nîmes.

57 Anne-Sophie Hourdeaux (2020), Actu.fr, "Video surveillance in Roubaix: cutting-edge technologies to keep an eye on the city" https://actu.fr/hauts-de-france/roubaix_59512/video-surveillance-roubaix-technologies-pointe-garder-loeil-sur-ville_30822291.html

58 Biometric Update (2016), "French National Police using Safran's Morpho Video Investigator solution" https://www.biometricupdate.com/201612/french-national-police-using-safrans-morpho-video-investigator-solution

Hikvision est une entreprise chinoise spécialisée dans la conception de vidéo-surveillance et de logiciel intelligent fondée en 2001. L'entreprise est l'une des leaders mondiales du marché avec un chiffre d'affaires de 41,9 milliards de yuans en 2017, soit environ 5 milliards d'euros. En plus d'une dizaine de caméras différentes, Hikvision commercialise une série de produits basés sur le *deep learning*, permettant de se focaliser sur certains éléments des images de vidéosurveillance[59].

L'entreprise affirme équiper 300 communes françaises. « *Nous sommes capables de reconnaître de nuit l'approche d'un individu à 200 m, en la distinguant d'un animal errant ou d'une chute de branche par exemple* », expliquait son P-DG, Jean-Baptiste Ducatez[60].

Huawei est une entreprise chinoise créée en 1987 par Ren Zhengfei, spécialisée dans le secteur des technologies de l'information et de la communication. En février 2017, Huawei a offert à la ville de Valenciennes 217 caméras nouvelle génération et un centre de surveillance. En plus de pouvoir faire de la reconnaissance faciale que la municipalité affirme ne pas utiliser, elles sont dotées des nouvelles technologies développées par Huawei : zoom HD, vision nocturne et sous la pluie, traitement intelligent de l'image avec détection des mouvements de foules, objets abandonnés, situations inhabituelles[61].

La société française EVITECH a été fondée à la fin de l'année 2002 suite à un projet du ministère de la Défense, visant à prévenir des événements tel que la prise d'otages du théâtre de Moscou le 26 octobre 2002. Elle est spécialisée dans les logiciels de vidéosurveillance intelligente. Sa solution «Jaguar» est installée depuis 2010 sur 70 caméras du port de Lyon. Elle permet le comptage des véhicules, la détection des véhicules à l'arrêt, à contre-sens ou en survitesse[62]. Plus récémment, le logiciel «Lynx» a permis à la ville de Lyon de compter l'évolution du nombre de personnes présentes sur la place des Terreaux lors de la fête des Lumières[63]. Un dispositif similaire est dépoyé dans la commune d'Hurepoix[64].

59 Hikvision Website, "Hikvision CCTV systems for perimeter protection"
https://www.hikvision.com/en/solutions/solutions-by-application/perimeter-protection/

60 Jordan Pouille (2020), La Vie, "How" intelligent "video surveillance is needed in French cities"
https://www.lavie.fr/actualite/comment-la-vidéosurveillance-intelligente-simpose-dans-les-villes-francaises-2816.php

61 Huawei website (2017), "Valenciennes inaugurates a new video protection system and is part of a" smart city "approach with Huawei"
https://e.huawei.com/fr/news/fr/2017/170213_valenciennes_safe_city

62 Evitech website (2011), "EVITECH experience feedback in urban video surveillance"
https://www.evitech.com/fr/component/content/article/20-blog/references/31-retour-experience-evitech-video-surveillance-urbaine

63 Evitech website (2018), "Counting at the festival of lights in Lyon"
https://www.evitech.com/fr/component/content/article/20-blog/references/326-comptage-a-la-fete-des-lumieres-a-lyon?Itemid=136

64 Evitech website (2019), "Revitalization of a city center"
https://www.evitech.com/fr/component/content/article/20-blog/references/349-revitalisation-d-un-centre-ville?Itemid=136

IMPACT SUR LES LIBERTÉS PUBLIQUES

Ces logiciels qui viennent se coupler à la vidéosurveillance ont un impact concret sur les opérateurs vidéos, mais également sur les individus qui sont observés dans l'espace public par ces caméras.

Au Carnet, en Loire-Atlantique, des militants écologistes qui luttent contre le bétonnage d'un site naturel ont découvert que des caméras avaient été camouflées pour pouvoir les espionner[65]. Camouflées dans des souches d'arbres ou des faux cailloux, ces 4 caméras filmaient en continu et étaient reliées, via des câbles enterrés, à des grosses batteries et modems, également dissimulés, permettant d'envoyer directement les images à un poste à distance. « *La mention « Allwan », visible sur une partie des images retrouvées, ou encore sur une étiquette sur une caméra, fait fortement penser qu'il s'agit d'équipements fournis par la société Allwan Security, située près d'Angers (Maine-et-Loire), spécialisée dans le matériel vidéo. Cette entreprise ne traite qu'avec des professionnels, et compte les forces de l'ordre parmi ses clients importants* », explique l'article.

En mai 2020, la police de Millau, dans l'Aveyron, a exploité les caméras de vidéosurveillance de la ville pour confirmer l'identité de manifestants ayant participé à deux manifestations non déclarées en préfecture pour dénoncer la gestion de la crise du Covid-19, et soutenir les services publics et le système de santé. Une dizaine de jours plus tard, certains militants ont confié avoir reçu une amende de 135€ pour « rassemblement interdit sur la voie publique dans une circonscription territoriale où l'état d'urgence sanitaire est déclaré». Une verbalisation rendue possible par l'exploitation par la police des images de vidéosurveillance. « *Les vidéos ne sont pas censées servir à verbaliser ce type d'infraction*», signale Julien Brel, l'avocat au barreau de Toulouse[66].

Enseignant-chercheur au sein de l'école d'ingénieur IMT Atlantique, Florent Castagnino a consacré sa thèse aux dispositifs de surveillance au sein de la SNCF. Dans un document publié en 2019, il décrit la manière dont la vidéosurveillance intelligente déplace le travail des opérateurs de vidéosurveillance et redéfinit le soupçon. « *L'automatisation supposément induite par l'intelligence artificielle ne supprime pas le travail des opérateurs, mais le déplace. Ce déplacement de l'objet doit ainsi conduire au déplacement de l'enquête empirique vers l'étude du travail des informaticiens. Le papier montre alors comment ces derniers doivent formaliser mathématiquement une partie du travail des opérateurs afin de le stabiliser dans des règles algorithmiques. Dans cette tâche d'abstraction, ils opèrent alors des choix plus ou moins implicites de ce qui est « suspect », et ainsi de ce qu'il « faut surveiller [67]».*

65 Héloïse Leussier (2020), Reporterre, "In Carnet, hidden and illegal cameras to monitor environmentalists https://beta.reporterre.net/Au-Carnet-des-cameras-cachees-et-illegales-pour-surveiller-des-ecologistes

66 Mélenn Gautier (2020), Liberation, "Can we be fined by video surveillance?" https://www.liberation.fr/checknews/2020/08/03/peut-on-etre-verbalise-par-vidéosurveillance_1791447

67 Florent Castagnino (2019), Science Po, "Making cameras 'smart': shifting the work of video surveillance operators and redefining suspicion" https://www.sciencespo.fr/ecole-urbaine/sites/sciencespo.fr.ecole-urbaine/files/2019_05%20-%20Castagnino.pdf

En janvier 2020, deux associations de défense des libertés individuelles, la Quadrature du Net et la Ligue des droits de l'homme ont déposé un recours devant le tribunal administratif de Marseille contre un nouveau système de vidéosurveillance intelligente mis en place par la mairie se.

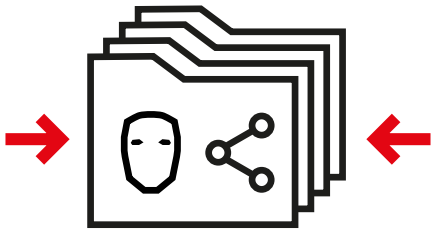
Les associations estimaient que les caméras intelligentes captaient des données biométriques, particulièrement sensibles et donc protégées, alors que la loi ne l'autorise pas. « *De part le fonctionnement même du traitement qui conduit à l'alerte, mais aussi probablement de part les informations transmises par l'alerte, la décision attaquée autorise un traitement de données biométriques - un traitement de caractéristiques comportementales, et aussi probablement de caractéristiques physiques et physiologiques, permettant d'identifier une personne de façon unique.* »[68]

La Quadrature du net et la Ligue des droits de l'homme s'inquiétaient également d'une délégation des pouvoirs de police à la société chargée du projet, SNEF, expliquant qu'il était indiqué dans des documents techniques que le paramétrage des algorithmes serait réalisé par SNEF. « *Il reviendra ainsi à la solution logicielle de l'entreprise privée d'identifier, de catégoriser et de générer des alertes sur certaines évènements ayant lieu sur la voie publique* », s'inquiétaient-ils.

L'un des autres impacts que pourrait avoir la vidéosurveillance intelligente est la possibilité de suivre les déplacements d'un opposant politique ou un militant à travers un réseau de caméras. La solution déployée par Briefcam permet de filtrer des véhicules ou individus selon la couleur de leur vêtement. Un individu pourrait ainsi être identifié puis suivi par l'ensemble des caméras. Dans une vidéo accessible sur Youtube, un officier de la police de Hartford, aux États-Unis, montre comment le logiciel Briefcam lui a permis d'identifier les mouvements d'individus pendant plusieurs heures et ainsi se rendre compte qu'ils prenaient tous la même direction, celle du point de deal qu'il cherchait à démanteler.

68 Olivier Tesquet (2020), Télérama, "Intelligent video surveillance is coming to Marseille, two associations are trying to have it suspended" https://www.telerama.fr/medias/deux-associations-attaquent-la-vidéosurveillance-intelligente-a-marseille

TENDANCE 5:



UN FICHAGE POLICIER ÉTENDU

16 mars 2020. Le gouvernement français annonce un confinement sur l'ensemble du territoire national. Celles et ceux qui ne le respecteront pas écoperont de 135 euros d'amendes. En cas de récidive dans les quinze jours, le contrevenant peut être verbalisé avec une amende de 1 500 euros (ramenée à 200 euros fin mars). Le 15 avril, la police et la gendarmerie nationale ont réalisé plus de 12 millions de contrôles et 762 106 verbalisations[69].

Ces infractions sont dans l'urgence consignées dans le SCA (système de contrôle automatisé). Aussi appelé ADOC (accès au dossier des contraventions), ce fichier de police est initialement destiné aux infractions routières. Y inscrire les sanctions relatives au non-respect du confinement est illégal. Le 9 avril, l'avocat rennais Rémi Casette se rend compte de la faille juridique et obtient la relaxe d'un de ses clients poursuivi pour non-respect répété du confinement. L'ensemble des

69 France Info (2020), "Coronavirus: 1,733 police custody for repeated containment violations since March 17"

procédures en cours pour non-respect du confinement se trouvent fragilisées. Il faut agir en urgence. Le gouvernement publie un décret le 16 avril pour rectifier la situation. Et étend, au passage, le fichier SCA a une trentaine de nouvelles infractions.

« *Non seulement les infractions visées sont peu graves*[70], pointe la Quadrature du Net dans un article publié en novembre 2020, *mais elles sont aussi très nombreuses. Vous pourrez donc vous retrouver dans ce fichier de police pour avoir vendu une Tour Eiffel à la sauvette, pour avoir du cannabis sur vous, pour le dépôt d'ordures…* »

L'utilisation illégale de fichiers de police en France a plus d'une fois été documentée. Dans un raport parlementaire daté de 2009[71], Delphine Batho et Jacques Alain Bénisti recensent 58 fichiers de police dont 27 % n'ayant fait l'objet d'aucune autorisation légale ou réglementaire ou d'une déclaration à la Commission Nationale de l'Informatique et des Libertés (CNIL), les gendarmes du numérique français. Un rapport parlementaire, cette fois-ci daté d'octobre 2018[72], fait état d'un vaste mouvement de mise en conformité et pointe que la CNIL estime aujourd'hui qu'il n'y a plus de mise en œuvre irrégulière d'importants traitements nationaux. Autre constat dressé par les parlementaires : la multiplication du nombre de fichiers de traitement de données puisqu'ils recensent 106 fichiers mis à disposition des forces de sécurité.

Les fichiers de police français incluent d'abord des fichiers administratifs. Ceux-ci regroupent des informations sur l'ensemble de la population française, indépendamment du fait qu'ils aient ou non commis des actes répréhensibles. Fichier des cartes d'identité, des permis de conduire : ils sont avant tout destinés à l'identification.

Depuis plusieurs années, un fichier inquiète particulièrement les associations de défense des libertés publiques : le fichier des titres électroniques sécurisés, qui regroupe, dans une base de données centralisée, l'image numérisée du visage et des empreintes digitales de l'ensemble des demandeurs de carte nationale d'identité et de passeport. Ces données biométriques sont conservées entre 15 et 20 ans. Si le décret qui a permis sa création précise bien que les forces de l'ordre ne peuvent accéder aux empreintes digitales conservées dans le fichier TES, aucune limite juridique formelle n'empêche son utilisation à des fins de reconnaissance faciale et les forces de l'ordre peuvent, via « une application », accéder à toutes les données à l'exception des empreintes digitales - selon le

70 Quadrature du Net website (2020), "Police registration: recourse against the misappropriation of the" automated control system file" https://www.laquadrature.net/2020/11/09/fichage-policier-recours-contre-le-detournement-du-fichier-du-systeme-de-controle-automatise/

71 Delphine Batho and Alain Bénisti (2009), "Information report on police files" https://www.assemblee-nationale.fr/13/rap-info/i1548.asp

72 Didier Paris and Pierre Morel-à-L'Huissier (2018), "Information report on the files made available to the security forces" https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information#_Toc256000053

Centre Français de Recherche sur le Renseignement[73].

D'autres fichiers de police, dit fichiers judiciaires, concernent les personnes ayant eu affaire aux forces de l'ordre. Ayant pour objet « la collecte et la centralisation de renseignements destinés à lutter contre les infractions bien déterminées [74]», ces fichiers s'intéressent autant aux objets et véhicules volés (FOVeS), au faux monnayage (FNFM) ou encore à l'authentification judiciaire (comme le fichier automatisé des empreintes digitales (FAED) ou le fichier national des empreintes génétiques (FNAEG).

Parmi eux, le fichier TAJ (traitement d'antécédents Judiciaires), commun à la police et la gendarmerie, résulte de la fusion de deux fichiers plus anciens et comporte plus de 19 millions de fiches dont 8 millions de photos (soit plus de 10 % de la population française).

Il ne se borne pas aux personnes condamnées par la justice, mais centralise des informations sur l'ensemble des personnes ayant été mises en cause dans une affaire judiciaire, mais aussi les victimes d'infractions ou les personnes faisant l'objet d'une enquête pour cause de disparition. Un rapport du Centre Français de Recherche sur le Renseignement fait état des avantages de ce nouveau fichier par rapport à ces prédécesseurs[75]. « *Le TAJ présente en outre des évolutions par rapport aux fichiers qu'il remplace : plus de catégories de personnes concernées et nouvelles fonctionnalités, comme des outils d'analyse et de rapprochement des données permettant de faire des recherches d'éléments communs dans des procédures différentes ou reconnaissance faciales à partir de photographies des personnes ».*

Le fichier des personnes recherchées (FPR) a aussi été largement pointé du doigt. Créé en 1969 et actualisé en 2017, ce fichier de police, commun à la police et la gendarmerie nationale et consultable sur tablette ou sur terminal embarqué, recense toutes les personnes « faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique » pour « faciliter les recherches, les surveillances et les contrôles effectués par les services de police et de gendarmerie à la demande des autorités judiciaires, militaires ou administratives [76]». Un fichier d'identification, destiné à l'identification des personnes et la collecte des renseignements, qui regroupe notamment les fiches "S", pour sûreté de l'état, soit « les personnes qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'État et à la sécurité publique par le recours ou le soutien actif apporté à la violence, ainsi que celles entretenant ou ayant des relations directes et non fortuites avec ces personnes [77]» Une définition large, qui regroupe autant des personnes susceptibles d'appartenir à des mouvances

73 Jean Marie-Cotteret (2017), "Police and intelligence files in France" https://www.cf2r.org/wp-content/uploads/2017/10/RR-21-Fichiers-Police.pdf

74 Didier Paris and Pierre Morel-à-L'Huissier (2018), "Information report on the files made available to the security forces" https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information#_Toc256000053

75 Jean Marie-Cotteret (2017), "Police and intelligence files in France" https://www.cf2r.org/wp-content/uploads/2017/10/RR-21-Fichiers-Police.pdf

76 CNIL website, "Wanted persons file" https://www.cnil.fr/fr/fpr-fichier-des-personnes-recherchees

77 Didier Paris and Pierre Morel-à-L'Huissier (2018), "Information report on the files made available to the security forces" https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/

terroristes islamistes que des militants et activistes voire des journalistes[78].

En décembre 2020, une réforme des fichiers PASP (Prévention des atteintes à la sécurité publique), GIPASP (gestion de l'information et prévention des atteintes à la sécurité publique) et EASP (Enquêtes administratives liées à la sécurité publique), tous trois des fichiers de renseignement liés à la direction générale de la police nationale et la direction générale de la gendarmerie nationale, a fait bondir les représentants des libertés publiques. Regroupant des informations extrêmement précises (profession, adresses physiques, email, photographies, activités publiques, comportement, déplacements…), ces fichiers recensant des individus pour de nombreux motifs liés au maintien de l'ordre (manifestations illégales, violences et dégradations liées à des contestations idéologiques, discours de haine, violences et vandalisme lors de manifestations sportives…) ont d'abord été étendus aux personnes morales et aux « groupements ».

Autrement dit, ces fichiers pourront maintenant concerner les entreprises, les associations, mais aussi des groupes Facebook, des espaces militants ou simplement des manifestations publiques (tous assimilables à des groupements). Cette réforme autorise aussi le PASP et GIPASP à ficher les personnes « entretenant ou ayant entretenu des relations directes et non fortuites » avec le dit « groupement ». Si la police le juge nécessaire, la police pourra largement ficher les personnes ayant participé à ces groupements (par exemple, un journaliste présent sur place). Alors que ces fichiers excluaient jusqu'à maintenant le fichage des enfants, le PASP et le GIPASP pourraient théoriquement être utilisés sans limite d'âge.

La même réforme étend aussi le périmètre des informations collectées : habitudes de vie, activités en ligne, posts publiés sur les réseaux sociaux… Une porte ouverte à la collecte généralisée de données que le gouvernement a refusé de formellement exclure malgré la demande de la CNIL. Plus grave : les décrets autorisent aussi la collecte d'informations sur « les opinions politiques », les « convictions philosophiques, religieuses » ou « l'appartenance syndicale » des personnes fichées ainsi que certaines données de santé.

78 Marie-Pierre Hadad (2016), "How a journalist discovered that he was on file" https://www.rtl.fr/actu/politique/comment-un-journaliste-a-decouvert-qu-il-etait-file-s-7786291210

ENTREPRISES IMPLIQUÉES

Bien que les fichiers de polices constituent une brique essentielle de la politique de maintien de l'ordre et de la surveillance en France, peu d'informations sont aujourd'hui disponibles concernant les entreprises impliquées dans la conception de ces bases de données ou leur stockage. Le même flou entoure les logiciels utilisés par les policiers, les gendarmes et les services de renseignements pour traiter les données collectées et essentiel de l'appareil de surveillance des pouvoirs publics en France.

Le traitement du fichier TAJ se fait à partir d'outils développés en interne par les forces de l'ordre françaises mais inclut aussi des partenariats privés. Depuis 2011[79], les forces de l'ordre utilisent, d'abord à titre expérimental, le logiciel de reconnaissance faciale "Facevacs Dbscan », commercialisé par la société allemande Cognitec, qui collabore avec de nombreux intégrateurs comme Indemia ou Atos.

79 Gabriel Thierry (2019), l'Essor, "Why the legal challenge of facial recognition could make pschitt" https://lessor.org/a-la-une/pourquoi-contestation-judiciaire-reconnaissance-faciale-pourrait-faire-pschittt/

IMPACT SUR LES LIBERTÉS PUBLIQUES

Pour les défenseurs des libertés publiques, la multiplication des différents fichiers de police et leur élargissement pourraient avoir des conséquences directes sur les militants. *« Le droit actuel permet déjà la généralisation de la reconnaissance faciale des manifestants »*, pointe ainsi la Quadrature du Net. Le TAJ, depuis 2012, permet techniquement la reconnaissance faciale des manifestants - il suffit, pour y être inscrit, d'avoir été en contact avec la police dans le cadre d'une affaire judiciaire.

L'extension des fichiers TASP, GIPASP et EASP fait, pour de nombreux observateurs, peser un véritable risque sur les libertés individuelles puisque permettant de ficher des citoyens sur la seule base de leurs idées politiques -, en particulier dans un contexte de généralisation de la surveillance par drone. *« Si,* pointe la Quadrature du Net, *via la loi sécurité globale, tous les manifestants pourront être filmés en manifestation et que, via le fichier TAJ, une grande partie d'entre eux pourra être identifiée par reconnaissance faciale, le PASP et le GIPASP leur a déjà préparé une fiche complète où centraliser toutes les informations les concernant, sans que cette surveillance ne soit autorisée ni même contrôlée par un juge*[80]*».* Une réforme qui selon eux ouvre la porte *« au fichage massif de militantes et militants politiques, de leur entourage (notamment de leurs enfants mineurs), de leur santé ou de leurs activités sur les réseaux sociaux ».*

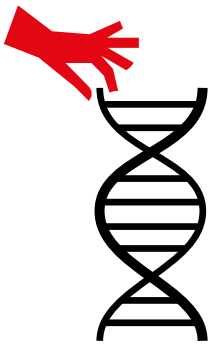
En août 2020, la Quadrature du Net a attaqué devant le Conseil d'État plusieurs dispositions du code de procédure pénale autorisant la police à utiliser la reconnaissance faciale pour identifier les personnes fichées dans le TAJ[81]. Le 9 novembre, l'association a aussi déposé un recours devant le Conseil d'État contre l'extension du fichier du Système de contrôle automatisé (SCA). Elle conteste de la même manière l'extension des fichiers TASP, GIPASP et EASP[82].

80 Quadrature du Net website, "We are attacking facial recognition in the TAJ" https://www.laquadrature.net/2020/08/07/nous-attaquons-la-reconnaissance-faciale-dans-le-taj/

81 Quadrature du net website "Massive filing of political demonstrators" https://www.laquadrature.net/2020/12/08/decrets-pasp-fichage-massif-des-militants-politiques/

82 Quadrature du Net website "PASP decrees: first battle lost against the massive registration of political activists" https://www.laquadrature.net/2021/01/07/decrets-pasp-premiere-bataille-perdue-contre-the-massive-filing-of-political-activists/

TENDANCE 6:



VERS LA CENTRALISATION DES DONNÉES DE SANTÉE

Une application pour les sauver toutes, et dans la technologie les lier. Comme des dizaines de pays dans le monde, la France s'est dotée, durant les premiers mois de la pandémie, d'une application de *contact tracing* destiné à lutter contre le Covid-19.

Annoncée en avril 2020 et lancée en juin de la même année, l'application, appelée Stop-Covid puis TousAntiCovid, peine à prendre. Alors qu'elle ne présente un intérêt qu'à partir de 14 % d'utilisateurs sur l'ensemble de la population[83], elle enregistre 1,6 millions d'utilisateurs (2,4 % de la population française). En janvier 2021, le gouvernement revendique près de 12 millions d'utilisateurs[84]. Des chiffres que plusieurs médias jugent peu fiables[85]... l'exécutif communiquant sur le nombre de

83 Clément Pouré & Clément le Foll (2020), Médiapart, "'StopCovid', a French fiasco" https://www.mediapart.fr/journal/france/290920/stopcovid-un-fiasco-la-francaise?onglet=full

84 Xavier Demagny (2021), France Inter, "After seven months of existence, TousAntiCovid still does not have its 15 million users" https://www.franceinter.fr/societe/apres-sept-mois-d-existence-tousanticovid-still-does-not-have-15-million-users

85 Sylvain Rolland (2021), La Tribune, "How the government manipulates the figures of Tous Anti-Covid" https://www.latribune.fr/technos-medias/comment-le-gouvernement-manipule-les-chiffres-de-tous-anti-covid-863808.html#:~:text=Manipulation%20des%20chiffres&text=%5BTweet%20du%20Premier%20ministre%2C%20Jean,'est%20pas%20le%20cas.%5D

comptes créés sur la plateforme et non le nombre d'utilisateurs quotidiens réel.

La Quadrature du Net, des spécialistes du numérique mais aussi plusieurs parlementaires se disent rapidement inquiets de la nature du projet et de sa mise en œuvre technique. « *On parle quand même d'une application dont le principe est de savoir qui est où en permanence* », notait, par exemple, une des figures françaises de la cybersécurité Baptiste Robert dès avril. Si le gouvernement insiste sur la mise en place d'un système de pseudonymat, la condition sine qua non pour protéger la vie des malades et les informations médicales sensibles collectées par l'application, Stop Covid ne permet pas de réel anonymat. « *C'est juste totalement impossible",* explique Martin Drago, juriste à la Quadrature du Net qui pointe que « *Stop-Covid est une application de surveillance et les citoyens sont suivis dans leurs déplacements* ».

Autre problème : le modèle de stockage des données. En avril, alors Google et Apple travaillent sur une interface de programmation applicative basée sur un système décentralisé à destination des pays souhaitant lancer leur outil de contact tracing - qui sera finalement adopté par la majorité des pays du monde -, le gouvernement français s'oriente vers un outil souverain basée sur une infrastructure centralisée - critiqué car moins sécurisé qu'un modèle décentralisé.

TousAntiCovid, surtout, facilite pour les experts la popularisation d'autres outils numérique de surveillance. « *L'application incite à soumettre son corps à une surveillance constante,* pointe la Quadrature du Net[86], *ce qui renforcera l'acceptabilité sociale d'autres technologies, comme la reconnaissance faciale ou la vidéo surveillance automatisée, qui sont actuellement largement rejetées* ». Un risque qui inquiète d'autant plus que la France entend aujourd'hui réformer la gestion de ses données de santé.

Lancé à l'issue de la mission parlementaire sur l'IA du député Cédric Villani[87], le projet Heath Data Hub vise la création d'une base nationale de données de santé, à l'importance stratégique certaine et classées comme sensibles au regard du RGPD.

Ces données existent déjà. Elles sont éparpillées entre les services de santé (chaque grand hôpital, par exemple, accumule des informations sur ses patients) et de multiples bases de données nationales (celle de la caisse nationale de l'assurance maladie, l'une des plus importantes au monde, a accumulé près de 100 téraoctets de données). Le projet, qui vise à centraliser ces informations pour, comme le mentionne la loi santé du 24 juillet 2019 qui entérine la réforme, « favoriser l'utilisation et de multiplier les possibilités d'exploitation des données, aussi bien en recherche clinique qu'en termes de nouveaux usages, notamment ceux liés au développement des méthodes d'intelligence artificielle », inquiète autant les acteurs du monde médicale que les associations de défense des libertés publiques.

86 Quadrature du Net website (2020), "Our arguments for rejecting StopCovid" https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid/

87 Cédric Villani (2018), "Giving meaning to artificial intelligence: for a national and European strategy" https://hal.inria.fr/hal-01967551/document

Jérôme Hourdeaux,[88] journaliste en charge des libertés publiques à Mediapart, s'en fait le relais dès novembre 2019. Il y rapporte les interrogations de la CNIL, inquiète de l'architecture technique du projet et de possibilités de fuites mais aussi de l'ouverture des données de santé à une utilisation beaucoup plus large - jusqu'alors, elles ne pouvaient être utilisées que dans le cadre de « l'accomplissement des missions des services de l'État, ou à des fins de recherche, d'étude ou d'évaluation » répondant à un motif d'intérêt public ; la loi santé ouvre leur utilisation à tout « motif d'intérêt public ».

« *Outre la Cnil,* poursuit le journaliste dans un long papier consacré au sujet, *le projet de Health Data Hub inquiète de nombreux observateurs pour plusieurs raisons. Il y a tout d'abord la vision extrêmement libérale de la mission à l'origine du Health Data Hub, qui souhaite favoriser avant tout l'innovation et les start-up au risque d'offrir les données des Français aux GAFAM ».*

Le 21 avril 2020, un arrêté gouvernementale est par ailleurs venu jeter de l'huile sur le feu: en raison de la crise sanitaire, le gouvernement décide d'accélérer le lancement de la plateforme à collecter, « aux seules fins de faciliter l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le virus Covid-19 » un grand nombres de données de santé. Avec, comme véritable point d'achoppement, l'hébergement de ces données de santé par le géant Microsoft .

ENTREPRISES IMPLIQUÉES

Le projet Stop-Covid, devenu TousAntiCovid, est porté par une multitude d'acteurs[89] et est coordonné par l'Institut national de recherche en sciences et technologies du numérique (INRIA). L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a à sa charge les questions de cybersécurité. Plusieurs institutions françaises du secteur médical participent aussi au projet.

Capgemini, l'un des plus importants cabinets de conseil en numérique, classé parmi les dix plus puissants du monde, a travaillé sur l'architecture logiciel de l'application. Atos, Thales ou encore Sopra Steria ont aussi été associé au projet auquel elles contribuent ponctuellement.

La maintenance et l'hébergement de l'application sont facturés à l'État par la société Outscale, filiale de Dassault Systèmes. Premier éditeur de logiciel français et deuxième éditeur européen, Dassault Systèmes est en majeure partie déte-

88 Jérôme Hourdeau (2019), Médiapart, "Health Data Hub: the mega file that wants to make our health data profitable" https://www.mediapart.fr/journal/france/221119/health-data-hub-le-mega-fichier-qui-veut-rentabiliser-nos-donnees-de-sante?onglet=full

89 Written question from the deputy of Philippe Latombe (2020) relating to the anonymity of the developers of the StopCovid project https://questions.assemblee-nationale.fr/q15/15-28687QE.htm

nue par le Groupe industriel Marcel Dassault, notamment connu pour fabriquer des avions de chasse.

L'attribution du marché d'hébergement n'est pas passé par une procédure de marché public. L'association de lutte contre la corruption Anticor a à ce titre saisi le parquet national financier en juin 2020.

Le Health Data Hub est un groupement d'intérêt public mais c'est l'entreprise Microsoft qui a été retenue pour gérer l'hébergement des données de la plateforme via son service de cloud Azure. Une décision contestée car remettant en cause la souveraineté des données françaises.

IMPACT SUR LES LIBERTÉS PUBLIQUES

TousAntiCovid et le projet de Health Data Hub ne sont pas perçus comme des mesures ciblant spécifiquement les militants ou les manifestations mais impactent potentiellement tous les citoyens. L'une des principales inquiétudes pour les libertés publiques, dénoncée par plusieurs chercheurs dans la presse dans le cas de Stop-Covid,[90] est l'hypothétique croisement entre ces données de santé et d'autres informations.

Début juin, une quinzaine d'associations et de personnalités ont par ailleurs saisi le Conseil d'État pour tenter d'empêcher le déploiement du Health Data Hub. La procédure a fait pchit mais le combat commence à porter ces fruits : le 19 novembre, comme le révèle Jérôme Hourdeaux dans un article pour Mediapart, le ministre de la santé Olivier Véran s'est engagé auprès de la CNIL à mettre fin à l'hébergement des données de santé par le géant américain d'ici deux ans.

90 Antonio Casilli, Paul-Olivier Dehaye and Jean-Baptiste Soufron (2020), "Stop Covid is a disastrous project piloted by apprentice sorcerers" https://www.lemonde.fr/idees/article/2020/04/25/stopcovid-is-a-disastrous-pilot-project-by-sorcerer's-apprentice_6037721_3232.html

CONCLUSION

COVID-19, EXTENSION DU DOMAINE DE LA SURVEILLANCE

A l'instar de la vague d'attentats qui a frappé la France lors de l'année 2015, l'épidémie de COVID-19 a fourni une nouvelle excuse aux forces de l'ordre et institutions françaises pour déployer dans l'espace public des technologies sécuritaires. Alors que la France regardait début 2020 avec incrédulité des policiers chinois utiliser des drones pour demander aux citoyens de respecter le confinement, elle a fait de même quelques mois plus tard. Les drones ont servi à surveiller les grandes villes, mais aussi les littoraux et coins réculés où des policiers ne peuvent s'aventurer à pied ou en véhicule.

De nombreuses entreprises se sont engouffrées dans la brèche sanitaire, adaptant leur technologie pour commercialiser des caméras permettant de détecter la température des individus, le respect de la distanciation sociale ou le port du masque. Des technologies auxquelles les institutions françaises, à l'image du Conseil d'État à propos des caméras thermiques dans la commune de Lisses, se sont d'abord opposées. Mais les entreprises du secteur de la sécurité ont fini par remporter le bras de fer, les libertés individuelles passant au second plan pour un gouvernement éreinté par plus d'un an de crise sanitaire.

Le 11 mars 2021, un décret publié au Journal officiel a autorisé les transporteurs à utiliser des caméras intelligentes pour observer le respect du port du masque dans les bus, métros ou trains. La Commission nationale de l'informatique et des libertés, qui avait en mai 2020 interrompu une première expérimentation dans le métro parisien, car elle présentait le risque de généraliser un sentiment de surveillance chez les citoyens, a changé d'avis, estimant début mars que leur usage permettrait à la RATP de « *produire des évaluations statistiques sur le respect de l'obligation de port du masque* » et « *adapter leurs actions d'information et de sensibilisation du public* ».

Un revirement symptomatique. Le Covid-19 a fourni des prétextes pour déployer dans l'espace public des technologies intrusives, dont l'utilisation s'inscrit dans un tournant sécuritaire plus large, d'autant plus inquiétant que le gouvernement français entend durcir la répression des manifestations. La loi dite « sécurité globale », adoptée par le Parlement le 15 avril 2021, va renforcer entre autres, l'interdiction de filmer la police, la généralisation adoptée par l'Assemblée Nationale le 15 avril dernier, de la vidéosurveillance par drones ou encore les caméras-piétons.

Une perte sans précédent pour les libertés individuelles de la population française, alors que le gouvernement ne cesse de prolonger l'État d'urgence sanitaire, comme il a pu prolonger l'État d'urgence après les attentats ayant frappé le pays, avant de l'inscrire dans le droit commun. Les élus, nationaux comme locaux, espèrent eux y gagner en image, s'affirmant comme des défenseurs de leurs concitoyens et utilisant l'argumentaire sécuritaire comme argument électoral.

Un autre combat s'annonce pour les associations de défense des libertés publiques : celui de la reconnaissance faciale que le gouvernement voudrait déployer, lors d'une expérimentation à grande échelle, lors des JO de 2024, qui se dérouleront à Paris. Un point de non retour, puisque qu'il amènerait, comme ce fut le cas lors des JO de 2008 à Pékin ou de 2012 à Londres avec la vidéosurveillance, à une extension sans précédent de cette technologie dans l'espace public.

Images:

Page de Couverture:
Jeanne Menjoulet_ Manifestation contre la loi sécurité globale_30/01/2020

Couverture intérieure: Photomontage
El primer paso blog Flickr
+ Pxfuel.com

Page 6:
Photomontage.
Images originales Pxfuel.com

Page réelle:
Jeanne Menjoulet_ Manifestation contre la loi sécurité globale_30/01/2020

A PROPOS DES ORGANISATIONS

ENCO (European Network of Corporate Observatories) est un réseau d'organisations civiques et médiatiques européennes qui se consacre à l'investigation des entreprises et de leur pouvoir.

https://corpwatchers.eu

Observatoire des Multinationales, basé à Paris, est une plateforme en ligne qui fournit des ressources et des enquêtes approfondies sur l'impact social, écologique et politique des entreprises transnationales françaises.

https://multinationales.org

Observatory of Business and Human Rights in the Mediterranean (ODHE), basée à Barcelone, est un projet de Suds et Novact qui vise à dénoncer l'impact et les complicités des entreprises en matière de droits de l'homme dans les contextes d'occupation et de conflit armé.

www.odhe.cat

Shoal est une coopérative radicale et indépendante d'écrivains et de chercheurs. Nous produisons des articles d'actualité, des enquêtes, des analyses et des écrits théoriques afin de contribuer et de servir de ressource aux mouvements qui tentent d'apporter des changements sociaux et politiques.

www.shoalcollective.org

En association avec:

NOVACT suds Internacionalisme Solidaritat Feminismes

Avec le soutien de:

Ajuntament de Barcelona ICIP Institut Català Internacional per la Pau OPEN SOCIETY FOUNDATIONS