

NOTE RAPIDE

DE L'INSTITUT PARIS REGION N°899



PRÉVENTION-SÉCURITÉ

Juillet 2021 • www.institutparisregion.fr

QUELLE SURVEILLANCE DE LA POPULATION À L'ÈRE DE LA COVID-19 ?

DEPUIS LE DÉBUT DE LA CRISE SANITAIRE LIÉE À LA COVID-19, LES LIBERTÉS PUBLIQUES ET LA SURVEILLANCE DES DÉPLACEMENTS DE LA POPULATION SONT AU CŒUR DES PRÉOCCUPATIONS. DES EXPÉRIMENTATIONS ET DES ÉVOLUTIONS RÉGLEMENTAIRES ONT ACCOMPAGNÉ CETTE CRISE POUR FAIRE RESPECTER LES CONSIGNES SANITAIRES, LIMITER LA PROPAGATION DU VIRUS, ET ACCROÎTRE LA SURVEILLANCE ET LE CONTRÔLE DE LA POPULATION. SI CERTAINES TECHNOLOGIES NUMÉRIQUES SONT PROMUES À CE TITRE, LEURS USAGES SOULÈVENT CEPENDANT UN CERTAIN NOMBRE DE QUESTIONS.

Le recours aux technologies dans l'espace public n'est pas nouveau. En 2012, on estimait que près d'un million de caméras de vidéosurveillance avaient été installées en France dans le cadre de la lutte contre la délinquance¹. La lutte contre le terrorisme et, plus récemment, la lutte contre la Covid-19 ont accentué le recours à cette technologie, qui se dote désormais des innovations promises par l'intelligence artificielle. La surveillance de la population n'est pas un domaine réservé aux pouvoirs publics. L'espace médiatique est régulièrement traversé par des interrogations quant au rôle joué par les géants du web, qui proposent sans cesse de nouvelles fonctionnalités : la reconnaissance biométrique et la systématisation de la géolocalisation viennent, ainsi, brouiller les pistes d'une surveillance qui serait principalement régalienne.

UN FOISONNEMENT D'EXPÉRIMENTATIONS

Dès le début de la crise sanitaire, l'ensemble de l'arsenal sécuritaire a été mis au service de la lutte contre la propagation du virus. Dans un premier temps, pour assister les forces de l'ordre et faire respecter les mesures sanitaires, des dispositifs technologiques ont été déployés afin de contrôler et surveiller la population. À Paris, par exemple, la préfecture de police a fait voler des drones pour détecter les rassemblements sur la voie publique contraires aux nouvelles règles sanitaires. À Nice, la police municipale a été équipée de drones pour surveiller le port et la promenade des Anglais, et pour diffuser, par haut-parleurs, des messages aux habitants.

Comme la lutte antiterroriste, la crise sanitaire stimule les innovations dans le secteur des technologies de sécurité, en atteste l'intensification des expérimentations en matière de



LA COVID-19 DANS LE MONDE : QUELQUES EXEMPLES

En Chine

En Chine, berceau de l'épidémie, des applications fondées sur l'utilisation des données personnelles ont permis de suivre en temps réel le développement de la pandémie et la localisation des nouveaux foyers de contamination. À la sortie du premier confinement, les Chinois ont été largement incités à utiliser ces outils. Un QR code de couleur (vert, jaune ou rouge) correspondant à leur état de santé et de contagion détermine ainsi leur possibilité de déplacement (vert : circulation libre ; jaune : mise en quarantaine préventive de 7 jours ; rouge : confinement prolongé de 14 jours). Cette application a aussi permis de fournir aux services de police des informations sur la géolocalisation des smartphones, et ainsi de suivre les citoyens et les potentielles reprises d'un foyer d'infection. La couleur des QR codes est ainsi vérifiée à l'entrée du métro et des centres commerciaux, ou encore dans la rue, pour filtrer les accès et ne laisser passer que ceux dont le QR code est vert. Pour surveiller sa population, le pays dispose également d'un important parc de caméras de vidéosurveillance (200 millions de caméras ont été recensées), de caméras thermiques (prenant à distance la température des citoyens), ou encore de techniques de reconnaissance faciale.

vidéosurveillance dite « intelligente » : lors du premier déconfinement, à la station Châtelet - Les Halles, à Paris, comme dans le parc de bus à Cannes, des caméras ont été utilisées pour repérer et compter les personnes sans masque. Officiellement, il s'agissait d'établir des statistiques, et non d'identifier ou de verbaliser les individus. À titre expérimental, la Région Auvergne-Rhône-Alpes a équipé trois lycées de caméras thermiques, qui prennent la température sans contact : ils les ont testées pendant trois semaines après la rentrée scolaire 2020 pour repérer d'éventuels foyers épidémiques. Par ailleurs, depuis fin 2020, le Groupe ADP (anciennement Aéroports de Paris) teste des caméras thermiques à Roissy pour relever la température des voyageurs arrivant sur le sol français. Les aéroports figurent comme des espaces clés dans la lutte contre la propagation du virus. Des caméras 3D sémantiques sont aussi expérimentées à Roissy : elles ne génèrent pas d'images mais mesurent la distance, la forme et la taille des objets de manière précise, permettant ainsi de contrôler les flux de personnes et le respect de la distanciation sociale.

La « safe city » (ville sûre), pendant sécuritaire de la « smart city » (ville intelligente), séduit de plus en plus de collectivités, et ce, depuis déjà plusieurs années, dans un contexte de lutte antiterroriste. Des villes comme Marseille, Saint-Étienne, Nice et Suresnes, notamment, ont récemment expérimenté des algorithmes sur leur parc de caméras afin de repérer les « comportements jugés anormaux » ou de détecter des « bruits suspects ». Dans les Yvelines et les Hauts-de-Seine, le syndicat mixte Seine et Yvelines Numérique vise à développer les services numériques dans ces départements et à mettre à disposition des collectivités des algorithmes pour détecter des « comportements ou des situations anormaux » (mouvements de foule, individus statiques trop longtemps, objets abandonnés, etc.) dans les établissements accueillant du public et relevant de leur compétence (collèges, administrations, services publics...)². Avec la crise sanitaire, les villes se sont impliquées dans la gestion du virus. À ce titre, elles peuvent compter

sur un marché en pleine expansion qui leur propose, régulièrement, des innovations technologiques. La Commission nationale de l'informatique et des libertés (Cnil) a demandé l'interruption de certaines expérimentations, considérant qu'elles ne permettaient pas de garantir, en pratique, le droit d'opposition des personnes à la captation de leur image. Cependant, l'usage de la vidéosurveillance intelligente dans les transports publics pour mesurer le taux du port du masque a été finalement encadré par un décret le 10 mars 2021. Dans la délibération de la Cnil portant avis sur le projet de décret, il est à la fois rappelé que « la préservation de l'anonymat dans l'espace public est une dimension essentielle pour l'exercice de ces libertés », mais aussi que « la lutte contre l'épidémie de Covid-19 [...] constitue un impératif majeur de nature à justifier, dans certaines conditions, des atteintes transitoires au droit à la protection de la vie privée et des données à caractère personnel »³.

LES DONNÉES PERSONNELLES AU CŒUR DE LA GESTION DE L'ÉPIDÉMIE

La gestion de l'épidémie de Covid-19 s'est centrée dès le départ sur l'accès aux données à caractère personnel, pour mieux comprendre la transmission du virus et lutter contre sa propagation. En France, leurs usages sont encadrés par le Règlement général sur la protection des données (RGPD), le règlement le plus strict au monde en matière de protection des données à caractère personnel. Au lendemain du premier confinement, dans ce cadre d'exception que la Covid-19 entraîne, une coopération entre l'Institut national de la santé et de la recherche médicale (Inserm) et l'opérateur Orange a permis d'analyser l'ensemble des données de géolocalisation émises par les téléphones mobiles des abonnés. Anonymisées, ces données de géolocalisation ont été utilisées pour comprendre la diffusion du virus, ainsi que le respect des mesures de confinement et leur impact. Les analyses ont permis d'établir que près de 1,2 million d'habitants ont quitté la Métropole du Grand Paris (MGP) entre le 13 et le 20 mars 2020, soit 17 % de la population,



à la suite de l'annonce des mesures de confinement. Si les déplacements se sont répartis de façon plutôt homogène sur le territoire français, la population de l'Île de Ré, par exemple, a toutefois augmenté de 30 %.

Le traçage numérique est bien au centre de la gestion de crise liée à la Covid-19, et les technologies du numérique sont ainsi mises à son service.

À cet effet, en mai 2020, l'État a lancé une première application baptisée « StopCovid » pour gérer la sortie du confinement. Grâce à la technologie Bluetooth⁴, cette application enregistre les informations des téléphones dotés de la même application croisés pendant plus de 15 minutes à moins d'un mètre, permettant ainsi d'identifier la chaîne de transmission du virus lorsqu'une personne est déclarée malade. Elle a été remplacée en octobre 2020 par « TousAntiCovid », qui élargit le périmètre d'enregistrement des données et propose des statistiques locales sur l'évolution du virus. À la sortie du troisième confinement, en mai 2021, plus de 15 millions de Français l'ont téléchargée. L'application est aujourd'hui proposée lors de la vaccination : on attribue à chaque personne vaccinée un QR code qu'il est possible de scanner *via* l'application pour garder en mémoire l'ensemble des tests effectués et des vaccins reçus. Cette application préfigure l'instauration d'un « pass sanitaire ».

La gestion de la propagation du virus passe aussi par la création de fichiers regroupant les données des personnes contaminées. C'est le cas pour le suivi des cas contacts, qui a ainsi abouti à la création, en mai 2020, du fichier « Service intégré de dépistage et de prévention » (Sided). Renseigné par les laboratoires, il contient l'ensemble des résultats des tests PCR et antigéniques réalisés par chaque personne. Une seconde base de données gérée par l'Assurance maladie, « Contact Covid », contient les informations d'identité et de santé des individus qui ont contracté le virus et de ceux qui partagent leur foyer, mais aussi les identités et coordonnées de ceux avec qui le malade a eu une interaction rapprochée hors du foyer. Partout en France, des « brigades » de l'Assurance maladie

ont été constituées pour suivre ces cas contacts et collecter les informations nécessaires⁵.

« Vaccin Covid » est le dernier système d'information en date. Sa création, par décret, en décembre 2020, a suscité l'inquiétude dans l'opinion publique quant au respect du secret médical et au droit de tout un chacun de refuser la vaccination. Ce fichier regroupe les données d'identité et de santé des personnes vaccinées contre la Covid-19. Cogéré par la Direction générale de la santé et l'Assurance maladie, il a pour objectif d'assurer le bon suivi de la campagne de vaccination, l'identification des personnes prioritaires ou encore l'information des personnes vaccinées en cas d'effets indésirables persistants. La Cnil a émis un avis favorable lors de sa création, en précisant cependant qu'elle était sensible au « droit d'opposition » des personnes face au traitement de leurs données de santé. En l'occurrence, ce droit ne peut être pris en compte que lorsque la personne refuse la vaccination, car une personne qui consent à la vaccination est intégrée systématiquement au fichier « Vaccin Covid ». Pour autant, la Cnil a rappelé dans son avis qu'elle sera vigilante quant aux conditions de mise en œuvre du fichier et qu'elle exercera son pouvoir de contrôle. Dans tous les cas, face à la pandémie, les autorités ont concrètement amplifié le développement de bases de données contenant des informations à caractère personnel enregistrées par les services de l'État.

VERS LA RECONNAISSANCE FACIALE ?

La gestion de l'épidémie de Covid-19 a ravivé le sujet de la reconnaissance faciale et de ses usages, alimenté par l'enchevêtrement de la crise sanitaire et du risque terroriste. Les dispositifs de reconnaissance faciale existaient déjà : les aéroports d'Orly et de Roissy disposent de sas permettant de comparer le visage des voyageurs avec les données biométriques contenues dans leur passeport, et les forces de l'ordre s'appuient sur des techniques de reconnaissance faciale pour comparer des images recueillies avec les données du fichier de traitement des antécédents judiciaires (TAJ)⁶.

À Taïwan et en Corée du Sud

Dès le début de l'épidémie, la fermeture des frontières et le filtrage des populations à Taïwan comme en Corée du Sud se sont également accompagnés d'un suivi des déplacements par les autorités *via* un système automatisé permettant d'assembler les données d'organisations publiques et privées : opérateurs téléphoniques, police et compagnies de cartes de crédit. Cette surveillance vise à s'assurer que les personnes contaminées ne quittent pas leur domicile. Elles sont d'ailleurs régulièrement appelées par les services de police. Toute personne porteuse du virus est ainsi identifiée et tracée, et des applications permettent de visualiser leurs itinéraires avant leur mise en quarantaine. La population reçoit quotidiennement des notifications pour l'alerter si elle a côtoyé des personnes porteuses du virus. Chaque individu peut demander par la suite à être dépisté et mis en quarantaine à son tour⁷.

Récemment pourtant, dans les discours médiatiques et politiques, la reconnaissance faciale s'est imposée comme un sujet plus consensuel. Des personnalités politiques y voient une solution durable face à l'insécurité. Cependant, les techniques de reconnaissance faciale ne font l'objet d'aucun contour réglementaire strict. Elles sont même interdites par le RGPD. Début 2020, le club de football de Metz a créé la polémique en testant une solution de comparaison faciale pour faire respecter les interdictions de stade. Les supporters ont manifesté leur mécontentement d'être la cible de technologies de surveillance à l'entrée du stade de leur club, mais Roxana Maracineanu, la ministre de la Jeunesse et des Sports, a soutenu l'initiative et le savoir-faire français en la matière : « Dans le cadre de ces expérimentations, ce ne sont pas les supporters qui sont visés expressément, mais c'est la sécurité autour de l'événement sportif de manière générale. »⁸

Par ailleurs, la crise sanitaire a aussi permis l'entrée dans le débat public de nouveaux usages en matière de surveillance. C'est le cas des drones, qui étaient jusqu'à présent interdits en France. Mi-mai 2020, le Conseil d'État a ordonné de cesser la surveillance par drone, jugée illégale faute de réglementation encadrant le dispositif et alors même que les zooms optiques utilisés permettent de collecter des données identifiantes. Six mois plus tard, l'article 22 de la proposition de loi relative à la sécurité globale est venu précisément répondre à cette décision, et poser, pour la première fois, un cadre autorisant l'usage des « dispositifs aéroportés de captation d'images ». Dernier rebondissement, le Conseil constitutionnel a censuré plusieurs articles de la loi, dont celui consacré à l'usage des drones, quelques jours avant sa promulgation, le 25 mai 2021.

Sujets controversés, la reconnaissance faciale et la protection des données personnelles soulèvent des enjeux qui ne se limitent pas au champ d'action des pouvoirs publics. Les géants du web détiennent les données personnelles de millions d'utilisateurs, et installent des systèmes de reconnaissance faciale et digitale sur un nombre croissant de smartphones, et ce, sans réel débat public sur l'usage et la conservation de ces données.

Sous le coup de la crise liée à la Covid-19, la rencontre des marchés sanitaires et sécuritaires s'est opérée en France comme partout dans le monde⁹. La crise liée à l'épidémie vient renforcer des tendances qui étaient déjà à l'œuvre en matière de sécurité et de surveillance, amorcées par la lutte contre le terrorisme, notamment. Cependant, cette politique sécuritaire soulève bien des questions. L'expression « la sécurité, première des libertés¹⁰ » s'est répandue dans les discours politico-médiatiques sans aucun débat sur ce qu'elle implique comme modèle de sécurité publique ni sur son impact sur la relation entre la police et la population. La succession des crises sanitaire et sociale ainsi que le risque terroriste continu ne peuvent cependant occulter le nécessaire équilibre entre le besoin de sécurité et la préservation des libertés individuelles dans un État de droit démocratique. ■

Camille Gosselin, urbaniste
mission Prévention sécurité (Sylvie Scherer, directrice)

RESSOURCES

- Cnil, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », décembre 2017.
- Cnil, « Reconnaissance faciale, pour un débat à la hauteur des enjeux », novembre 2019.
- Fernandez Rodriguez L., Elie M., « La smart city est-elle autoritaire ? », *La Gazette des communes*, le 17 septembre 2019.
- Mucchielli L., *Vous êtes filmés, enquête sur le bluff de la vidéosurveillance*, Armand Collin, Paris 2018.
- Untersinger M., « Coronavirus : le risque est d'entrer dans une nouvelle ère de surveillance numérique invasive », *Le Monde*, le 5 avril 2020.

1. Lemaire É., *L'œil sécuritaire, mythes et réalités de la vidéosurveillance*, Éditions La Découverte, Paris, 2019.
2. Gosselin C., « La sécurité à l'heure de l'intelligence artificielle », *Note rapide*, n° 833, L'Institut Paris Region, février 2020.
3. Délibération 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports.
4. Le Bluetooth est un réseau permettant l'échange de données à courte distance en utilisant des ondes radio. Il permet ainsi de connecter facilement plusieurs appareils électroniques.
5. Lorsqu'un cas est confirmé positif, l'Assurance maladie se charge de l'identification des personnes ayant eu un contact avec le malade (48 h avant l'apparition de ses symptômes ou 7 jours avant son prélèvement) jusqu'à son isolement. Différents réseaux sont mobilisés : employeur, Éducation nationale, etc.
6. Ce fichier a été institué en 2016, en plein état d'urgence, tout comme le fichier des titres électroniques sécurisés (TES), qui compile l'ensemble des données personnelles et biométriques des Français possédant une carte nationale d'identité ou un passeport.
7. Mozur P., Zhong R., Krolik A., « In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags », *The New York Times*, le 1^{er} mars 2020 ; Benoit M., « La vie privée en ligne, l'autre victime du coronavirus », *Sciences et Avenir*, le 25 mars 2020 ; Ojardias F., « Comment la Corée du Sud a réussi, jusqu'ici, à dompter l'épidémie de coronavirus », *France Inter*, le 1^{er} avril 2020.
8. Interview sur France bleu, le 31 janvier 2020.
9. Gosselin C., « Les données personnelles au cœur de la lutte contre l'épidémie », *Chronique des confins* n° 2, avril 2020.
10. Fradin A., « La sécurité est la première des libertés, ou l'inverse ? », *L'Obs*, le 21 novembre 2016.

DIRECTEUR DE LA PUBLICATION

Fouad Awada

DIRECTRICE DE LA COMMUNICATION

Sophie Roquette

RÉDACTION EN CHEF

Laurène Champalle

MAQUETTE

Jean-Eudes Tilloy

MÉDIATHÈQUE/PHOTOTHÈQUE

Inès Le Meledo, Julie Sarris

FABRICATION

Sylvie Coulomb

RELATIONS PRESSE

Sandrine Kocki

33 (0)1 77 49 75 78

L'Institut Paris Region

15, rue Falguière
75740 Paris cedex 15
33 (0)1 77 49 77 49

ISSN 2724-928X
ISSN ressource en ligne
2725-6839



institutparisregion.fr

