Surveillance numérique

Félix Tréguer

Surveillance numérique*

Félix Tréguer**

février 2021

En ce mois de décembre 2016, les arguments fusent au sein du groupe de travail « Défense et sécurité » constitué autour d'Emmanuel Macron, candidat déclaré à la présidence de la République. Depuis quelques semaines, par messages interposés[1], la petite équipe réfléchit à la réponse qu'il convient d'opposer au programme « sécurité » de François Fillon. Le concurrent de droite a émis le vœu d'imposer une carte d'identité biométrique aux Français ? Qu'à cela ne tienne ! Les conseillers du candidat Macron envisagent de reprendre la proposition, à l'image de François Heisbourg, expert en géopolitique et jadis directeur de Thomson CSF (devenu le géant de la défense Thales), ou encore de la commissaire Marianne Tarpin, hiérarque de la Direction générale de la sécurité intérieure (DGSI). Dans les échanges, les protagonistes insistent sur la nécessité de lutter contre la fraude à l'identité, en évoquant notamment les terroristes venus de Syrie ayant librement pu circuler à travers l'Europe à l'aide de faux-papiers, et on convient de creuser la question.

Anne Bouverot, alors présidente-directrice générale de Morpho (depuis devenu Idemia), le leader français de l'identité biométrique, a récemment été cooptée par le petit groupe de conseillers. Dans une note qu'elle soumet à la réflexion collective, elle commence par souligner le coût de la carte d'identité biométrique – 2 euros l'unité, soit 140 millions d'euros environ pour l'ensemble de la population française – et invite à la faire directement payer par les citoyens. Le déploiement de cette carte permettra selon elle « une baisse de la fraude et des coûts associés », « une plus grande sécurité et [une] meilleure lutte contre le terrorisme ». Mais ce n'est pas tout : grâce

*Contribution à l'ouvrage collectif *Le Nouveau Monde : Tableau de la France néolibérale*, Popelard Allan, Anthony Burlaud et Grégory Rzepski (éds.), Paris, Éditions Amsterdam, 2021.

**Félix Tréguer est post-doctorant au CERI Sciences Po et chercheur associé au Centre Internet et Société du CNRS. Il est membre de La Quadrature du Net, une association dédiée à la défense des libertés dans le contexte d'informatisation, et l'auteur de *L'utopie déchue : une contre-histoire d'Internet, XV^e^-XXI^e^ siècle* (Fayard, 2019).

[1]La retranscription de ces échanges est réalisée à partir des courriers électroniques de la campagne Macron divulgués sur la plateforme WikiLeaks (disponibles en ligne sur wikileaks.org).

à la reconnaissance faciale et aux données biométriques stockées sur la puce électronique de ce nouveau titre d'identité, une myriade d'autres usages sont également possibles, notamment pour le secteur privé. Bouverot évoque ainsi la possibilité « de valider l'identité d'une personne au moment d'une transaction numérique sécurisée : signature d'un contrat, achat d'un billet d'avion, transfert d'argent entre pays différents, etc. »

Dès le lendemain, le 12 décembre, Didier Casas, haut fonctionnaire et à l'époque directeur général adjoint de Bouygues Télécom, adresse un message à Alexis Kohler, le conseiller d'Emmanuel Macron qui deviendra secrétaire général de l'Élysée, et à Ismaël Emelien, en charge de la communication et des affaires stratégiques au sein de la campagne : l'identité biométrique, « vous achetez ou pas, franchement ? » « Honnêtement, bof », tranche Emelien quelques heures plus tard. La proposition ne figurera donc pas au programme du candidat Macron. L'identité biométrique – instaurée en France en 2009, sous la pression des États-Unis, avec la création du passeport biométrique – réalisera pourtant une percée décisive sous son mandat, que ce soit au travers de l'application pour smartphone ALICEM, expérimentée depuis juin 2019, ou de cette fameuse « carte nationale d'identité électronique » (CNIe), finalement lancée à l'été 2021.

Ces échanges, à la fois banals et remarquables, offrent un bon aperçu des processus qui président à la fuite en avant de la surveillance numérique : les intérêts à court terme des élites politiques, administratives et économiques s'entrecroisent, voire s'alignent au gré de leurs allers et retours entre public et privé, tandis que les désordres du monde et la surenchère politicienne nourrissent une escalade sécuritaire qui alimente à son tour l'industrie de la surveillance en lui assurant des débouchés. À la croisée des velléités de contrôle social, du soutien aux fleurons industriels, des tentatives de rationalisation bureaucratique et d'une propension toujours plus grande au « solutionnisme technologique », la surveillance se déploie et entretient la flambée du libéralisme autoritaire.

Des années Giscard à la Startup Nation

Certes, ces processus ne datent pas d'hier. Dès les années 1970, à la fin des « Trente Glorieuses », l'informatique revêt déjà une importance cruciale pour le pouvoir. Elle est le rouage clé de la « société de l'information » tant espérée par les élites réformatrices de l'époque, et l'on compte déjà sur elle pour moderniser l'État et relancer la croissance. En février 1975, le ministre de l'Industrie, Michel d'Ornano, assure ainsi qu'« aucun pays industrialisé ne pourra maintenir son potentiel ou son indépendance économique et socioculturelle s'il reste à l'écart des développements de ces nouvelles technologies

qui seront au cœur de l'organisation future de nos sociétés[2] ». Pourtant, au sein de la population, l'ordinateur est volontiers associé au fichage généralisé et à la gestion technocratique des sociétés de masse. Dans le sillage de Mai 68, les réformateurs doivent composer avec de puissants courants technocritiques au sein de la société, tandis que l'Organisation des nations unies (ONU), le Conseil de l'Europe ou l'Organisation de coopération et de développement économiques (OCDE) alertent sur les risques que l'informatique fait peser sur les droits fondamentaux. Au sein même des élites politiques et administratives, beaucoup partagent ces préoccupations. Il faut dire que la question des libertés publiques se pose avec acuité chez une génération qui a connu la Seconde Guerre mondiale et, pour une bonne part, s'est battue dans les rangs de la Résistance.

Alors, pour réconcilier informatique et libertés, on s'en remet au droit. Lorsqu'en mars 1974, le journal *Le Monde* révèle un vaste programme d'interconnexion de fichiers de l'état civil, de l'Insee, de la police, des armées, de la sécurité sociale ou des impôts, le gouvernement donne un coup d'arrêt à ce projet et met en place une commission censée définir un cadre pérenne. Ces réflexions aboutiront en 1978 à la création de la Commission nationale de l'informatique et des libertés (CNIL) par la loi dite « Informatique et libertés ». Les dispositions de ce texte constituent aujourd'hui encore le socle juridique de la protection des citoyens face à la surveillance numérique. L'article premier proclame solennellement : « L'informatique doit être au service de chaque citoyen » ; « elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Quarante ans plus tard, ces promesses ont fait long feu. La surveillance tant redoutée a bel et bien prospéré. Un processus intrinsèquement lié à l'informatisation toujours plus poussée de la société, laquelle demeure un marqueur de modernité et de puissance. Alors que, jusque dans les années 1980, l'ordinateur était une machine réservée aux grandes bureaucraties publiques et privées, l'apparition du *personal computer* (PC) engage alors une démultiplication de l'informatique à travers l'ensemble de la société. Puis, dans les années 1990, l'essor rapide d'Internet va marquer une nouvelle rupture dans l'histoire du capitalisme de surveillance. Désormais, une grande part des activités sociales, économiques, politiques, migrent vers l'éther du « cyberespace ». La quantité quasi infinie de traces numériques ainsi générées se transforme en une matière brute extraite et valorisée par une poignée d'acteurs économiques qui, à l'image de Google, les exploitent à des fins de ciblage publicitaire. Profitant de l'« effet réseau » et des rendements croissants permis par la reproductibilité numérique, ces multinationales acquiè-

[2]Conférence sur les politiques en matière d'informatique et de télécommunications, compte rendu de la conférence tenue à l'OCDE du 4 au 6 février 1975, OCDE, 1976.

rent rapidement des positions dominantes et amassent des fortunes colossales. Bientôt propulsées en tête des classements des plus grandes valorisations boursières mondiales, elles sont autant de modèles à suivre dans l'économie de l'« hyper-innovation » vantée par Macron dans une ode à la « Startup Nation » en juin 2018[3].

À ces ressorts technologiques et économiques de la surveillance s'ajoutent des facteurs politiques et juridiques. Accompagnant la consolidation de l'ordre néolibéral, les nouvelles élites dirigeantes semblent pour l'essentiel avoir mis de côté les scrupules de leurs aînées en matière de libertés. Grâce aux « puits à données » constitués par les parangons du capitalisme de surveillance et grâce aux innovations sorties des laboratoires de la recherche publique et privée, la surveillance d'État se fait plus massive, plus systématique. Les crises, qu'elles soient terroristes, économiques ou sanitaires, constituent autant d'occasions à saisir pour légitimer et légaliser ces nouvelles pratiques, permettant ainsi à la surveillance de « passer à l'échelle » en s'affranchissant autant que faire se peut du débat démocratique. Les réformes s'empilent et instaurent un état d'exception permanent, qui suspend ou contourne l'État de droit et affaiblit les contre-pouvoirs. Un exemple parmi tant d'autres : alors que la CNIL s'était opposée durant les années 1990 à la vidéosurveillance et à la fuite en avant du fichage policier, le gouvernement et le Parlement s'entendent en 2004 pour la priver du droit de veto prévu par le législateur en 1978. Depuis, ses avis sur les décrets ou arrêtés créant de nouveaux traitements de données personnelles ne sont que consultatifs.

Internet, laboratoire de la surveillance de masse

Dans cette longue dérive amorcée dès les années 1980, la grande crise sécuritaire ouverte par les attentats du 11 septembre 2001 aura joué un rôle clé. Les projets à l'étude au sein des services de police ou de renseignement en matière de surveillance d'Internet bénéficient alors d'un gigantesque coup d'accélérateur, tandis que les résistances chez les responsables politiques comme dans l'opinion publique sont vaincues. Aux États-Unis, la National Security Agency (NSA) lance de nouveaux programmes de surveillance comme le « *Total Information Awareness* » et s'allie avec une myriade d'acteurs privés. Les États membres de l'Union européenne imposent aux opérateurs télécoms le stockage des métadonnées – les données techniques qui fournissent des renseignements sur qui communique avec qui, quand, depuis quel lieu, pendant combien de temps, etc.–, et ce non pour les seules personnes suspectées, mais pour l'ensemble de la population.

En France, la Direction générale de la sécurité extérieure (DGSE) lance

[3] « Discours du Président de la République, Emmanuel Macron, au salon VivaTech 2017 », *elysee.fr*, 15 juin 2017.

en 2007 un plan d'investissement qui doit lui permettre de rattraper son retard sur les agences de renseignement anglo-saxonnes. L'objectif est de construire des stations d'interception destinées à la collecte et à l'analyse du trafic Internet qui transite par les câbles sous-marins raccordés au territoire national. Pour ce faire, elle dispose d'importants atouts, à commencer par ses liens avec les câblo-opérateurs de rang mondial comme Alcatel et Orange, mais aussi de « jeunes pousses » comme Qosmos ou Amesys, spécialisées dans les outils permettant de « scanner » à la volée ces immenses flux de données. Lors d'une réunion à l'Élysée en janvier 2008, les patrons du renseignement et des caciques du Conseil d'État font valider leur projet par Nicolas Sarkozy. Le chef de l'État acceptera de débloquer près de 700 millions d'euros sur quatre ans, malgré l'illégalité patente de ce programme classé secret défense. L'année suivante, le renseignement intérieur expérimente à son tour l'usage de sondes placées sur les infrastructures des principaux fournisseurs d'accès à l'Internet français afin de détecter des communications « suspectes ». Comme le résume en 2010 Bernard Barbier, alors directeur technique de la DGSE (depuis passé dans le privé), la France joue désormais « en première division ».

À la suite des attentats de janvier 2015, le gouvernement de Manuel Valls légalise ces dispositifs en faisant adopter la loi relative au renseignement. Le pouvoir promet qu'il s'agit de faire rentrer les services secrets dans le giron de l'État de droit mais cela ne les empêchera pas de persister dans l'illégalité. Fin 2016, la presse révèle l'existence d'un contrat conclu entre la DGSI et l'entreprise californienne Palantir. Pour passer les téraoctets de données perquisitionnés dans le cadre de l'état d'urgence à la moulinette du Big Data, la direction générale s'en remet à cette entreprise liée au complexe militaro-industriel états-unien. Cette collaboration, qui suscite les réserves de certains responsables du renseignement inquiets pour la « souveraineté numérique » de la France, sera pourtant validée par le député Cédric Villani : en 2018, dans un rapport sur « l'intelligence artificielle », il légitime ces pratiques – illégales car nullement autorisées par la loi – en les enrobant du langage « startup », évoquant une « expérimentation » dans une « logique de bac à sable[4] ». La presse dévoilera aussi, fin avril 2019, la création de l'« entrepôt ». Attenant au siège de la DGSE à Paris, ce bâtiment ultrasécurisé et consacré à la mutualisation des données entre services leur permet de s'affranchir, hors de tout réel contrôle, de certains des garde-fous inscrits dans la loi de 2015.

[4]Villani Cédric, *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, mission confiée par le Premier ministre Édouard Philippe, Paris, 2018.

La surveillance des mouvements sociaux : une priorité

Si la lutte contre le terrorisme est systématiquement invoquée pour justifier l'extension continue des capacités de surveillance du renseignement, cette finalité ne représente, en réalité, qu'un peu plus d'un tiers de ses activités. Parmi les autres missions dévolues aux « services », on compte par exemple le renseignement économique ou encore la surveillance des mouvements sociaux. Au motif de lutter contre « les violences collectives de nature à porter gravement atteinte à la paix publique », de prévenir « les atteintes à la forme républicaine des institutions » ou « la reconstitution de groupements dissous », la loi de 2015 autorise les services de renseignement à surveiller les associations et autres groupes militants. Or, cette activité a connu un important regain ces dernières années. Entre 2017 et 2019, sa part dans le total des mesures de surveillance administrative est passée de 6 à 14 %.

À cet égard, le mouvement des Gilets jaunes a constitué un tournant. Dès la fin 2018, les services de renseignement s'organisent pour identifier les « meneurs » de cette mouvance protéiforme et décentralisée, malgré les réserves de certains agents et même de quelques préfets gênés par cette opération de police politique. En janvier 2019, le Service central de renseignement territorial (SCRT, anciens « Renseignements généraux ») est sommé de repérer « les personnalités exerçant une réelle influence sur le mouvement ou se signalant par des commentaires vindicatifs ou subversifs trouvant de l'écho sur les réseaux sociaux », dans le but de les interpeller lors des manifestations ou de les « retourner » pour en faire des informateurs. Quant à la CNIL, elle ne sera avisée de ces activités qu'un an et demi plus tard, lorsque le gouvernement lui soumettra des projets de décrets visant à régulariser et à étendre encore davantage ce fichage politique. Son avis, qui recommande notamment d'« exclure explicitement la possibilité d'une collecte automatisée de ces données » captées sur les réseaux sociaux, ne sera pas suivi par le gouvernement.

Entre temps, la stratégie nationale du renseignement publiée à l'été 2019 avait consacré « l'analyse et le suivi des mouvements sociaux et crises de société » au rang de priorité du renseignement : comme s'en justifiait quelques mois plus tard Pierre de Bousquet de Florian, alors coordonnateur national du renseignement (depuis devenu directeur de cabinet de Gérald Darmanin), il s'agit de faire face à « une forme d'ensauvagement général de la société ». Au ministère de l'Intérieur, on explique la hausse rapide du nombre de personnes inscrites dans ces fichiers – passé d'environ 40 000 à 60 000 en à peine trois ans – par les « troubles graves à l'ordre public qui se sont développés depuis 2015 ».

« Expérimenter pour que nos industriels progressent »

Derrière le développement de la surveillance, il y a donc des impératifs politiques. Mais les politiques industrielles jouent également un rôle prépondérant. Au gré de rachats et autres fusions et acquisitions, deux entreprises françaises figurent désormais dans le peloton de tête mondial du secteur : d'un côté, Idemia, née en 2017 de la fusion de Morpho (ex-Safran Identity and Security) et d'Oberthur Technologies ; de l'autre, Thales, géant de la défense renforcé sur le marché de la surveillance par le rachat de Gemalto en 2019.

Édifiés par le succès économique des plateformes Internet comme Google ou Facebook, ces groupes cherchent à imiter leurs stratégies fondées sur le traçage constant des populations. Mais plutôt que d'en passer par le stockage de « cookies » dans les navigateurs web ou par la captation des données comportementales depuis les applications pour smartphones, ces groupes français misent sur le déploiement de quantité de capteurs dans l'espace public urbain. « Le monde physique, déplore Ajay Amlani, vice-président senior d'Idemia, est un immense vide de données ». Un vide que ces entreprises entendent combler avec le soutien actif de l'État, présent à leur capital. Le député LREM de la Loire, Jean-Michel Mis, fin connaisseur du milieu, résume : « Il faut se positionner par rapport aux Américains ou Chinois, notamment sur les questions d'identification ou de reconnaissance biométrique. » Le secrétaire d'État au numérique Cédric O, promoteur d'Alicem et ancien cadre chez Safran, est sur la même ligne : selon lui, « expérimenter la reconnaissance faciale est nécessaire pour que nos industriels progressent ».

Dans ce contexte, les financements abondent afin de permettre aux industriels français de développer leurs solutions techno-sécuritaires, souvent en lien avec des organismes de recherche publics. Depuis 2016, dans le cadre de projets de recherche menés en collaboration avec la préfecture de police de Paris et l'Institut national de recherche en informatique et en automatique (INRIA), Idemia et Thales développent des solutions de vidéosurveillance automatisée. Ces outils recourent à l'intelligence artificielle pour analyser automatiquement les images captées par les caméras de surveillance. Un document de présentation de l'un de ces projets précise que l'objectif consiste à « combler le *gap* entre le niveau macro de la surveillance d'une foule et l'observation micro d'individus ou de groupes ». Outre la lutte contre la grande ou la petite délinquance, il s'agit plus largement d'automatiser la détection des comportements réputés déviants. En juin 2018, dans un discours consacré aux doctrines de maintien de l'ordre en manifestation, l'ancien ministre de l'Intérieur Gérard Collomb voyait dans ces outils un moyen de « repérer dans la foule des individus au comportement bizarre ».

L'État soutient aussi ses « champions nationaux » par l'octroi de sub-

ventions ou la passation de marchés publics. C'est Thales qui a développé l'application d'authentification par reconnaissance faciale Alicem. Encore Thales qui, à Nice, a reçu une aide de 11 millions d'euros de la part de la Banque publique d'investissement (BPI) pour contribuer à l'émergence de solutions de « Safe City » (« ville sûre »), un marché prometteur au croisement du secteur de la sécurité, lequel réalise 7 % de croissance annuelle au niveau mondial, et de celui de la « Smart City », qui recouvre l'ensemble des projets d'informatisation massive de la gestion urbaine et devrait représenter près de 820 milliards de dollars d'ici 2025. La convention d'expérimentation conclue en juin 2018 entre le consortium dirigé par Thales et la Ville de Nice envisage ainsi la fusion de diverses technologies de surveillance au sein d'un « centre d'hypervision et de commandement », avec pour objectifs d'« évaluer chaque situation pour pouvoir anticiper les incidents et les crises », d'identifier les « signaux faibles » afin de fournir une « aide à la planification » et de proposer des « prédictions sur base de scénarios », dans le cadre d'une « gestion en temps réel » fondée sur l'exploitation du « maximum de données existantes ».

Enfin, l'État encourage l'exportation de ce savoir-faire national, notamment à travers une structure baptisée Civipol dont il détient 40 % du capital. Parmi les actionnaires de cette société de droit privé, on retrouve aussi Thales et Idemia. Grâce à des financements européens consacrés au contrôle des migrations ou à l'aide au développement, elle intervient auprès de pays comme le Mali ou le Sénégal pour concevoir et mettre en œuvre des systèmes d'identité biométrique. Une bonne manière pour les entreprises françaises de se positionner sur un marché africain de l'identité estimé à 1,4 milliard d'euros. Anciennement dirigé par Pierre de Bousquet de Florian, le conseil d'administration de Civipol a également eu pour membre un certain Alexis Kohler.

Des contrôles d'identité permanents et invisibles

Lorsque les élites dirigeantes évoquent leur préoccupation pour les libertés publiques, il s'agit le plus souvent de se distinguer des concurrents ou pays plus franchement autoritaires, d'afficher leur prétendue supériorité morale et d'écarter d'un revers de main les critiques « droits-de-l'hommiste ». Le traçage numérique ? « Ce n'est pas la culture française », esquivait l'ancien ministre de l'Intérieur Christophe Castaner au début de la pandémie de Covid-19, alors qu'on l'interrogeait sur les pratiques du régime chinois. Si, dans les discours, la Chine fait encore figure de repoussoir, sa domination du secteur de la surveillance en fait pourtant un partenaire incontournable. Ses entreprises se taillent d'ailleurs régulièrement la part du lion dans les marchés publics français : en juillet 2020, lorsque le ministère de l'Intérieur

passe une commande de 15 millions d'euros pour l'achat de 30 000 nouvelles « caméras-piétons » destinées à filmer les interventions des forces de l'ordre, c'est le chinois Hikvision qui remporte l'appel d'offres.

D'ailleurs, certains assument de s'inspirer du régime de Pékin. Dans une note de l'école des officiers de la gendarmerie nationale consacrée à la reconnaissance faciale, un colonel estime qu'une fois couplée aux dizaines de milliers de caméras de vidéosurveillance installées sur la voie publique, cette technologie permettra d'instaurer « un autocontrôle limitant les incivilités (respect du code de la route, déjections animales, dépôts d'ordures) sur le modèle du crédit social chinois[5] ». L'auteur y voit même le moyen de « mettre fin à des années de polémiques sur le contrôle au faciès, puisque le contrôle d'identité serait permanent et général », mais aussi « invisible ». Pour assurer l'« acceptabilité sociale » de la reconnaissance faciale, ses promoteurs misent sur les Jeux olympiques de 2024, une grande manifestation sportive avec, à la clé, de juteux marchés publics, où les enjeux sécuritaires seront à la fois immenses et en partie dissimulés par la nature à la fois consensuelle et festive de ce « grand événement ».

Du côté du ministère de l'Intérieur, on pense à plus long terme. Au mois de novembre 2020, en pleine mobilisation contre les violences policières et la proposition de loi dite « Sécurité globale », le gouvernement publie discrètement le Livre blanc de la sécurité intérieure. Identification biométrique par reconnaissance faciale, par le son de la voix ou les odeurs corporelles, intelligence artificielle « pour faire face au volume croissant d'informations », centres de commandement nourris aux Big Data afin de procéder à « l'analyse des données du passé comme outil de rétrocontrôle et d'aide à la décision », ou encore multiplication des drones de surveillance : la panoplie technosécuritaire y est passée en revue. Et, bien sûr, pour « porter le ministère de l'Intérieur à la frontière technologique », les financements devront suivre : le Livre blanc propose de consacrer 1 % du PIB aux missions de la sécurité intérieure à l'horizon 2030, soit une augmentation budgétaire de 30 % sur la décennie.

[5] Dominique Schoener, *Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité*, Centre de recherche de l'école des officiers de la gendarmerie nationale, 2019.