ramses 2021

SOUS LA DIRECTION DE **THIERRY DE MONTBRIAL** ET **DOMINIQUE DAVID**

ifri

LE GRAND BASCULEMENT ?

- **SANTÉ/CLIMAT :** COVID-19, ET MAINTENANT ?
- **EUROPE :** SE REFAIRE OU SE DÉFAIRE
- **MONDE ARABE :** 10 ANS APRÈS LE FAUX PRINTEMPS

DUNOD

Contrôle et surveillance numérique

Pas de pause avec le COVID-19

Depuis dix ans, les pratiques de contrôle numérique ont évolué avec la technologie et le comportement des États, autoritaires comme démocratiques. La dissémination récente des applications d'Intelligence artificielle favorise le contrôle de l'espace public. Le COVID-19 sera-t-il un accélérateur vers une surveillance numérique généralisée ?

Les stratégies de contrôle numérique évoluent

Porté par la démocratisation de l'accès à internet dans les années 2000, le web connaît un essor fulgurant, avec la multiplication des espaces d'interaction, d'échange et de conversation. Le web social, les blogs, Facebook et Twitter, peu coûteux et faciles d'utilisation, donnent à chacun la possibilité d'être informé et d'informer en temps réel. Ils parachèvent la déliaison de l'imprimé et de l'écrit, installent le multimédia au cœur des pratiques courantes, et confirment que la proximité virtuelle n'a plus rien à voir avec la contiguïté de l'espace.

Face aux répercussions politiques du web, les États, et surtout les États autoritaires, ont déployé des stratégies de contrôle variant dans leur intensité comme dans leur sophistication. Une première génération de contrôle s'est focalisée sur le déni d'accès et la censure de contenus spécifiques, une méthode pratiquée dès l'origine en Chine puis dupliquée, en fonction des événements politiques, en Iran et dans le monde arabe. Une deuxième génération correspond à la création d'un environnement juridique, et de capacités techniques, permettant de refuser l'accès à certaines informations – une version plus évoluée de contrôle, que le droit doit pouvoir légitimer.

Une troisième génération de contrôle consiste à passer d'une politique réactive à une politique proactive : il s'agit moins de refuser l'accès, que de rivaliser avec des menaces potentielles au moyen de campagnes de contre-information efficaces, qui discréditent ou démoralisent les opposants. C'est là une stratégie commode pour des pouvoirs qui visent à éviter le passage de l'activisme numérique à la rue. En Russie par exemple, cherchant à affecter et à façonner la façon dont l'information est reçue par les internautes, les autorités manipulent le référencement sur les moteurs de recherche, afin de rendre difficile l'accès à l'information à caractère sensible.

Enfin, ces stratégies de contrôle numérique s'étendent au-delà de l'opposition traditionnelle entre régimes autoritaires et pays démocratiques. La préservation de l'ordre public, qui peut servir de justification à des mesures de restriction ou de censure dans l'usage de l'internet, la lutte contre la cybercriminalité, la défense d'intérêts économiques, sont autant d'éléments qui se conjuguent pour justifier et prôner les politiques de contrôle. En Europe, la série d'attentats d'origine islamiste commis en 2015-2016 a ainsi incité plusieurs gouvernements à adopter des lois numériques intrusives. Au Royaume-Uni, la question du chiffrement s'est trouvée au cœur d'une loi sur le renseignement très controversée. En 2015, le gouvernement français a avalisé la mise en place d'un système de surveillance du trafic sur internet. Des débats similaires ont eu lieu en Allemagne, remettant en question le dogme de la liberté des flux d'informations échangés sur le réseau.

Reconnaissance faciale : une surveillance algorithmique démultipliée

Le champ du contrôle numérique s'est considérablement élargi à la faveur de l'essor récent et spectaculaire de l'Intelligence artificielle (IA). L'une des applications majeures de cette technologie est la reconnaissance faciale qui, de plus en plus répandue, permet d'identifier une personne sur une photo ou une vidéo, en comparant son visage avec ceux sauvegardés dans une base de données. Elle combine les techniques biométriques, l'IA, la cartographie 3D et le *deep learning*, et doit son récent essor aux avancées effectuées dans les domaines des métadonnées (*big data*), des réseaux de neurones et des puissances de calcul des microprocesseurs[1].

Le recours à la reconnaissance faciale à des fins de contrôle et de surveillance se répand dans le monde entier. Il n'est certes pas surprenant que des régimes autoritaires investissent massivement dans ce domaine : du golfe Persique à l'Asie du Sud et du Sud-Est, de nombreux États se procurent des systèmes d'analyse avancée et des caméras de reconnaissance faciale. La Chine de 2020 constitue l'exemple le plus abouti de la mise en place d'un contrôle social, au moyen d'outils numériques recourant massivement aux Intelligences artificielles.

L'Europe sous emprise ?

La nouveauté réside dans la généralisation de ces technologies au sein des démocraties libérales, en particulier européennes, lesquelles déploient des systèmes de contrôle automatisés aux frontières, de prévision policière, de *safe cities* (technologies de surveillance de l'espace urbain), ainsi que des systèmes de reconnaissance faciale[2]. Deux exemples récents : à l'été 2019, le *Financial Times* révélait que des sociétés privées testaient, à l'insu des citoyens, des systèmes de reconnaissance faciale dans plusieurs quartiers de Londres ; dans la capitale britannique, les tests effectués par la police métropolitaine ont révélé un taux d'erreur d'identification

1. Le *deep learning* est une méthode d'apprentissage automatique (*machine learning*), qui s'inspire des neurosciences, ses algorithmes ressemblant à des réseaux de neurones connectés entre eux et s'activant selon les stimuli reçus. Cette technique succède aux méthodes dites « expertes », qui ont fleuri dans les années 1970-1980, avant de décliner.

2. Voir la cartographie interactive intitulée « Countries Using AI Surveillance Technology », Carnegie Endowment for International Peace.

des personnes supérieur à 80 %. En France, la ville de Nice s'est positionnée à l'avant-garde de ces usages. Le déploiement de la reconnaissance faciale pendant le carnaval 2019, de portiques biométriques dans deux lycées, ainsi que la signature d'une convention visant à établir une *safe city*, à travers la mise en relation de toutes les données reçues par les objets connectés de la ville, ont alimenté de nombreuses polémiques.

Pour les États, ces technologies offrent deux avantages principaux : automatiser des fonctions de suivi et de surveillance généralement déléguées à l'humain ; structurer un réseau de surveillance plus vaste que ceux des méthodes traditionnelles, afin d'instaurer un autocontrôle, dérivé du modèle chinois de « crédit social ».

Dans une perspective européenne, trois risques principaux découlent de ces tendances de fond. Le premier est celui d'une dépendance croissante de l'Europe à l'égard d'une stratégie technologique chinoise prédatrice. Les entreprises chinoises sont les principaux fournisseurs mondiaux de ces technologies de contrôle et de surveillance. À lui seul, l'équipementier Huawei (placé sous sanctions américaines depuis mai 2019) en livre à plus de 50 pays, sur tous les continents. Incarnant de façon décomplexée la *tech* autoritaire, Pékin fournit les autocraties comme les démocraties : particulièrement ciblée, l'Europe est maillée de projets de *safe* ou *smart cities* chinois dans des villes allemandes, espagnoles, françaises, italiennes et serbes.

Le deuxième risque est lié à la question démocratique : le déploiement de moyens de surveillance aussi invasifs pour la vie privée devrait susciter des mouvements de résistance en Occident – c'est déjà le cas à Londres, ou à San Francisco dont la municipalité a interdit la reconnaissance faciale pour les forces de police, ainsi que dans d'autres États américains. Ce facteur de risque interroge l'absence de réels débats publics sur des enjeux de libertés fondamentales.

Troisièmement, l'Europe révèle ses contradictions profondes : en adoptant la surveillance affinée à l'Intelligence artificielle, les pays européens envoient un mauvais signal au reste du monde, alors qu'ils s'étaient positionnés à l'avant-garde de la régulation des données avec le Règlement général sur la protection des données (RGPD). Invoquer l'éthique – des données ou de l'Intelligence artificielle – ne peut constituer une politique en soi. En l'espèce, les lacunes du RGPD expliquent en partie comment ces technologies de surveillance grignotent du terrain sur le continent.

Enfin, l'exportation par la Chine de ses technologies de contrôle numérique se double d'un effet de mimétisme dans certains pays. À Moscou, certaines autorités observent avec envie la gestion algorithmique des masses par le pouvoir chinois – ce qui « fonctionne » en Chine devrait ainsi pouvoir être répliqué en Russie, d'où la multiplication des installations de reconnaissance faciale à travers le pays, surtout dans la capitale.

Le COVID-19, accélérateur de la surveillance numérique ?

La survenue de la pandémie mondiale du COVID-19, en début d'année 2020, a entraîné un recours aux outils technologiques pour appuyer les politiques de suivi du coronavirus. Partout dans le monde, les initiatives ayant recours à la

géolocalisation, et parfois à d'autres données numériques, se sont multipliées, un nombre croissant de gouvernements mettant en place des applications permettant de tracer le parcours des personnes contaminées, ou de s'assurer qu'elles restaient à leur domicile.

C'est notamment par un usage massif de la localisation des téléphones portables que la Corée du Sud a pu contrôler le virus sans recourir à un confinement national. La surveillance numérique, à travers les données générées par les téléphones ou les ordinateurs, peut constituer un efficace outil de gestion de crise. Dans plusieurs pays, scientifiques et ingénieurs développent des applications dans ce sens. Cependant, adoptés dans l'urgence, et parfois sans contrôle démocratique, ce type de dispositifs de surveillance généralisée de la population comporte des risques évidents pour les libertés fondamentales.

Foyer de départ de l'épidémie, la Chine a rapidement déployé des mesures technologiques destinées à limiter sa propagation. Le géant du numérique Alibaba a créé une application qui attribue aux citoyens des QR codes de différentes couleurs en fonction de leur état de santé. Seuls ceux bénéficiant d'un code vert pouvaient se déplacer librement. La Russie utilise aussi un système de QR code, et la ville de Moscou a développé une application qui demande l'accès à la localisation, à la caméra, au journal d'appels, et à plusieurs autres données des téléphones, pour s'assurer que les malades respectent la quarantaine. En Inde, le gouvernement a lancé une application analogue qui requiert une autorisation d'accès à la géolocalisation précise du smartphone où elle est installée, en plus du Bluetooth. Le débat autour de la protection des données personnelles en Inde a un précédent avec la carte Aadhaar, système d'identification de la population nationale fondé sur la biométrie. Aux États-Unis, l'administration Trump s'est tournée vers les géants de la *tech* afin d'identifier les foyers épidémiques et d'enrayer la propagation du virus. En Europe enfin, les débats, en France ou au Royaume-Uni par exemple, butent sur les problématiques de confidentialité et les risques qu'induirait le maintien de tels dispositifs, supposant une surveillance numérique à durée indéterminée.

J. N.

Pour en savoir plus

- S. Arsène, « China's Social Credit System: A Chimera with Real Claws », *Asie.Visions*, n° 110, Ifri, novembre 2019.
- A. Polyakova et C. Meserole, « Exporting Digital Authoritarianism: The Russian and Chinese Models », *Policy Brief*, Brookings Institution, août 2019.
- O. Tesquet, *À la trace. Enquête sur les nouveaux territoires de la surveillance*, Paris, Premier Parallèle, 2020.