IDÉES • VIE PRIVÉE

Caroline Lequesne Roth : « L'encadrement des technologies de surveillance est une condition de la démocratie »

TRIBUNE

Caroline Lequesne Roth
Maître de conférences en droit public à l'université Côte d'Azur, cofondatrice du projet de recherche « Deep Law for Technologies » et responsable du Master 2 Droit algorithmique et gouvernance des données

La généralisation de la reconnaissance faciale à des fins de surveillance serait attentatoire aux libertés, estime, dans une tribune au « Monde », la juriste Caroline Lequesne Roth, qui plaide pour un large débat public afin de distinguer les usages acceptables ou non.

Publié le 22 janvier 2020 à 06h00 | Lecture 4 min.

Tribune. A l'ère des technologies de surveillance, où les scénarios dystopiques prennent forme dans l'espace public, l'actualité place la reconnaissance faciale au cœur des débats. Le déploiement accéléré de cette technologie constitue un phénomène authentiquement global. Plébiscitée par les régimes libéraux comme autocratiques, de Londres à Pékin, la reconnaissance faciale est progressivement érigée en outil incontournable de l'arsenal sécuritaire. Elle suscite également l'intérêt croissant du secteur privé : identification des personnes condamnées pour vol dans les commerces, identification des mineurs pour la vente d'alcool ou la consultation de sites pornographiques, contrôle à l'entrée des casinos... Autant d'expérimentations qui dessinent les contours des modèles de consommation de demain.

Lire aussi | **Reconnaissance faciale : « Il existe encore en France des garde-fous en matière de données biométriques »**

La France n'échappe pas au phénomène. Alors que la ville de Nice, très motivée en ce domaine, a testé un système de reconnaissance faciale en février 2019 à l'occasion de son carnaval, le gouvernement prévoit de faire reposer sur la reconnaissance faciale l'accès au système Alicem (Authentification en ligne certifiée sur mobile). Ce système doit permettre à tout citoyen de se connecter aux services publics en prouvant de manière sécurisée son identité à partir d'un smartphone. Le secrétaire d'Etat chargé du numérique, Cédric O, encourage en outre les expérimentations, dans un contexte où l'industrie européenne est fortement concurrencée par les géants sino-américains.

L'introduction de ces dispositifs n'emporte toutefois pas le plein assentiment de la société civile. Celle-ci y entrevoit, tour à tour, le spectre du Léviathan technocratique ou du Big Brother que constituent les géants mondiaux du numérique. La multiplication des usages liberticides au-delà de nos frontières alimente déjà un bilan à charge : répression de la minorité des Ouïgours en Chine, arrestation de manifestants à Hongkong, traque de militants palestiniens en Cisjordanie sont autant d'exemples d'usages de la reconnaissance faciale fermement condamnés par les associations de défense des droits de l'homme. Dans l'Hexagone, le dispositif Alicem a donné lieu à l'introduction d'un recours devant le Conseil d'Etat, et les expérimentations conduites dans les lycées de la région Sud (Provence-Alpes-Côte d'Azur) ont été désavouées par la Commission nationale informatique et libertés (CNIL).

A pluralité des usages, pluralité des effets

Dans une société démocratique, l'interdiction de la surveillance de masse doit demeurer le principe. La généralisation de l'outil de reconnaissance faciale à des fins de surveillance serait manifestement attentatoire aux libertés et disproportionnée au regard de l'objectif de maintien de l'ordre public. Rappelons qu'un tel dispositif repose sur la captation continue de milliers de visages, sans le consentement des individus et en dehors de toute procédure les mettant en cause. La CNIL rappelle en ce sens que *« les enjeux de protection des données et les risques d'atteintes aux libertés individuelles que de tels dispositifs sont susceptibles d'induire sont considérables, dont notamment la liberté d'aller et venir anonymement »*.

Lire aussi | **« Big Brother » : quand les Chinois se rebiffent**

Les usages de cette technologie ne font pas, à ce jour, l'objet d'une législation idoine. Le Règlement général sur la protection des données comme la directive européenne « Police Justice » interdisent le traitement des données biométriques aux fins d'identification, sauf exception circonstanciée, fondée sur la nécessité publique. Ces exceptions doivent être strictement encadrées et prévoir les mesures appropriées et spécifiques à la sauvegarde des droits fondamentaux.

Si, en France, les textes requièrent l'adoption d'un décret en Conseil d'Etat, le pluralisme des intérêts qui s'expriment et le choix de société que l'adoption de ces dispositifs implique appellent à notre sens une intervention du législateur et un large débat public. Celui-ci permettrait de distinguer les usages « acceptables » au regard de nos valeurs démocratiques, et ceux qui doivent être résolument bannis, à l'instar du fichage des migrants ou de l'identification de suspects dans les délits mineurs. A pluralité des usages, pluralité des effets.

Repenser notre rapport à l'objet technique

Les appels en faveur de moratoires se multiplient déjà outre-Atlantique au sein de la communauté universitaire. Plusieurs propositions de loi ont parallèlement été introduites, en Grande-Bretagne et dans divers Etats américains, pour engager une telle démarche. En France, le secrétaire d'Etat chargé du numérique plaidait, en octobre 2019, en faveur d'expérimentations *« pour que nos industriels progressent »*. Il proposait la création d'une instance de supervision de ces expérimentations, mais n'envisageait que *« dans un deuxième temps »* l'ouverture d'un *« débat citoyen »* sur *« l'équilibre entre usages, protection et libertés »,* position réaffirmée à l'occasion d'un entretien au *Parisien,* le 24 décembre.

Contestable dans la méthode – comment faire l'économie d'un débat dans un Etat de droit ? –, la position de Cédric O fait fi de l'acceptabilité sociale de ces dispositifs, qui rencontrent des résistances nombreuses. Elle se heurte également à « l'effet cliquet » technologique qui menace nos administrations : comment justifier le démantèlement a posteriori de dispositifs coûteux qui ne donneraient pas satisfaction ?

Lire aussi | **Reconnaissance faciale : une start-up analyse les photos des réseaux sociaux pour la police américaine**

Ce chantier invite plus fondamentalement à repenser notre rapport à l'objet technique. La présomption d'efficacité et de neutralité, dont bénéficie souvent la technologie dans le discours de nos responsables, en occulte les lacunes : erreurs, biais et failles de sécurité obèrent encore son fonctionnement vertueux. Nous plaidons aussi pour une « méfiance institutionnalisée », qui opposerait au secret des affaires une obligation d'audit et envisagerait le standard technique sous l'angle des droits fondamentaux. L'encadrement des technologies de surveillance en général, de la reconnaissance faciale en particulier, s'impose aussi comme une condition et une urgence de la démocratie « technologique ».

Caroline Lequesne Roth (Maître de conférences en droit public à l'université Côte d'Azur, cofondatrice du projet de recherche « Deep Law for Technologies » et responsable du Master 2 Droit algorithmique et gouvernance des données)