Face au Covid-19, le « solutionnisme technologique » est de nouveau à l'œuvre

« Chacune des crises qui a marqué le 21e siècle ont été l'occasion d'une régression des libertés publiques. Les attentats terroristes du 11 septembre 2001 ont vu l'Europe adopter la Directive sur la rétention des données de connexions électroniques et l'obligation faite aux opérateurs de stocker celles de tous leurs clients. Les attentats terroristes qui ont touché la France en 2015 ont permis le vote sans débat de la loi renseignement. Ils ont aussi entraîné la mise en place de l'état d'urgence dont des mesures liberticides ont été introduites dans le droit commun en 2017.

La pandémie de Covid-19 menace d'entraîner de nouvelles régressions : « discriminations, atteintes aux libertés, à la protection des données personnelles et à la vie privée… » extrait du communiqué de l'observatoire des libertés et du numérique (OLN) du 8 avril 2020

La crise sanitaire impose à travers le monde, à des milliards de personnes, des technologies de surveillance. Ces outils technologiques qui reposent bien souvent sur la géolocalisation des individus (qu'ils soient contaminés ou pas) permise par les smartphones, a, en théorie, deux fonctions : faire respecter le confinement par les populations en aidant les polices (nationales, municipales, gendarmerie) dans leurs fonctions répressives et tracer les individus dans leur déplacement pour lutter contre la propagation du virus ou assurer qu'il n'y a plus de risque de contamination. Ce traçage apparaît, non nécessairement lié à une géolocalisation, comme indispensable aux autorités dans la période de dé-confinement qui s'annonce, d'autant plus que les Etats dont la France, ne se sont pas donnés les moyens de tester leurs populations pour savoir qui est contaminé ou non. Ce dépistage des malades était indispensable dès le début de la pandémie pour limiter le nombre de décès comme l'ont prouvé la Corée du Sud et l'Allemagne. Devant le manque criant de masques chirurgicaux pour les personnes contaminées et de masques de protection respiratoire individuelle (de type FFP2) pour les soignants, le personnel d'entretien … Le confinement s'est imposé comme étant le seul moyen de lutter contre l'expansion de la pandémie.

Comme l'a affirmé dès le début de la crise sanitaire la quadrature du net : « la loi renseignement adoptée en 2015 permet à l'État de surveiller la population pour une très large variété de finalités, notamment « pour le recueil des renseignements relatifs à la défense des intérêts économiques, industriels et scientifiques majeurs de la France. » Si, comme Macron, on admet que « cette crise sanitaire sans précédent aura des conséquences […] économiques majeures », on peut conclure que la loi renseignement autorise déjà l'État à surveiller la population afin de lutter contre l'épidémie. Parmi les mesures autorisées par la loi renseignement, le code de la sécurité intérieure prévoit que les services du renseignement peuvent exiger la transmission par les opérateurs téléphoniques des « données techniques relatives […] à la localisation des équipements terminaux utilisés » par leurs clients. Ces données peuvent même être « recueillies sur sollicitation du réseau et transmises en temps réel par les opérateurs ». Pour exiger ces transferts, l'administration agit seule, sans le contrôle ou l'autorisation préalable d'un juge et sans même informer la population. « La Quadrature du Net concluait : « Nous n'avons à ce stade aucune information permettant de corroborer l'utilisation de ces pouvoirs de surveillance dans le cadre de la lutte contre l'épidémie du virus COVID-19 ». En fait, il semble bien que l'Etat n'ait pas voulu utiliser cette « ficelle » trop grosse car même si « nous sommes en guerre » cette pandémie ne peut pas être considérée comme une attaque terroriste d'autant plus que les personnes contaminées et contaminatrices n'ont pas le profil de terroristes, loin s'en faut !

Malgré tout, l'Etat français cherche une solution technologique pour garantir le succès du dé-confinement. Macron va, à partir du 24 mars, mettre en place le comité CARE (Comité Analyse Recherche et Expertise) devant accompagner la réflexion des autorités « *sur l'opportunité de la mise en place d'une stratégie numérique d'identification des personnes ayant été au contact de personnes infectées.* » Celle-ci s'appuierait, évidemment, sur les smartphones où nous serions invités à télécharger une application baptisée « StopCovid » et à activer son « Bluetooth » (1). En France, de part notre histoire de résistance au fichage, cette stratégie numérique ne peut reposer que sur le volontariat pour télécharger cette application. Il faut, de plus, qu'il n'y ait pas, en théorie, de conséquences pour celui qui refuserait de télécharger cette application et que ce fichage soit temporaire. En culpabilisant le citoyen grâce à tous les grands médias, l'Etat peut espérer un certain succès. Cela sera-t-il suffisant pour avoir une partie importante de la population ? Nous en doutons, d'autant plus que seulement 77% de la population française a un smartphone et moins d'un français sur 2 âgé de plus de 70 ans (44% en 2019) en possède un. Si on ajoute à cela les zones rurales (ou pas d'ailleurs) où il y a des difficultés de connexion ce n'est pas gagné !

Comme le dit si bien l'Observatoire des libertés et du numérique : « En matière de lutte contre la pandémie et notamment de fin de confinement, il semble que le gouvernement tente de masquer ses manques et ses erreurs avec des outils technologiques présentés comme des solutions miracles. Et alors que leur efficacité n'a pas été démontrée, les dangers pour nos libertés sont eux bien réels.

Source : laquadrature.net

Denis – OCL Reims

(1) Bluetooth est une norme de communication permettant l'échange bidirectionnel de données à très courte distance en utilisant des ondes radio UHF sur une bande de fréquence de 2,4 GHz. Sa destination est de simplifier les connexions entre les appareils électroniques en supprimant des liaisons filaires. La technologie sans fil Bluetooth est un protocole de communication qui permet la synchronisation et l'échange de données sur une petite distance (environ 10 mètres), entre des téléphones mobiles, des ordinateurs portables, et autres équipements sans fil.