Quand les applications de *contact tracing* font (la) peur

Par Christophe Dubois, Sociologue, ULiege

La pandémie de covid-19 constitue un drame sanitaire et socio-économique dont nous commençons à peine à mesurer l'ampleur. Comme toute crise, celle-ci a notamment permis de questionner nos échelles de production et de consommation, nos espaces de travail, notre modèle d'Etat (a)social, la surpopulation carcérale ou encore la place de nos droits fondamentaux. La sortie de crise a également été perçue par quelques entrepreneurs et élus politiques comme l'opportunité de développer et de mettre en œuvre des applications numériques de *contact tracing* présentées comme « prometteuses ».

En quoi consistent ces dispositifs ? Leur principe repose sur l'usage des smartphones. Ainsi, lorsque deux smartphones s'approchent l'un de l'autre à une distance de quelques mètres, ils échangent entre eux des signaux codés. Ainsi, si Mr A croise Mme B lundi à 14h, leurs smartphones échangent par Bluetooth une suite aléatoire de chiffres et de lettres. Ce code est stocké par les producteurs de téléphones durant 14 jours. Grâce aux applications de *tracing*, si Mr A apprend vendredi qu'il a le covid-19, il peut signaler son diagnostic à la plateforme – dans le cas d'un dispositif centralisé – qui alerte automatiquement toutes les propriétaires de smartphones ayant croisé Mr A au cours des 14 derniers jours. Ainsi, Mme B sera incitée à se montrer vigilante quant à son état de santé et au respect des gestes barrières afin de ne pas propager le risque de contamination. Dans le cas d'un dispositif décentralisé, l'alerte sera automatiquement donnée par Mr A à tous les propriétaires de smartphones croisés au cours des 14 derniers jours, sans passer par une plateforme centrale.

Les concepteurs de tels dispositifs les présentent comme intelligents, efficaces et sûrs non seulement pour les mettre sur le marché ou pour faire parler d'eux, mais aussi, très probablement, parce que leur foi en ces technologies est authentique. Cette confiance dans les vertus – et, à l'inverse, dans les dangers – des algorithmes est typique du déterminisme technologique. Celui-ci postule que le développement et l'usage des technologies s'imposent à nous pour le meilleur ou pour le pire. Ces dispositifs sont pourtant façonnés et utilisés par des individus intelligents qui mettent leur rationalité limitée[1] au service d'objectifs souvent louables *a priori*. Toutefois, la portée de ces développements et de ces usages est politique, éthique et morale. Ces dispositifs doivent par conséquent faire l'objet d'expertises, de délibérations politiques et de décisions prudentes afin de mettre en balance les « bonnes raisons »[2] des concepteurs et des utilisateurs d'une part, et leur adéquation aux normes et aux valeurs sociétales d'autre part[3].

Divers experts en cryptographie, en droit des technologies et en sécurité ont ainsi récemment mis en évidence diverses zones d'incertitude relatives aux processus de conception et d'utilisation des applications numériques de *contact tracing.* Ces avis éclairent les limites de la confiance que les citoyens peuvent témoigner envers de tels dispositifs présentés comme « intelligents », « efficaces » et « sûrs ».

---

[1] March, J. G. (1978). Bounded rationality, ambiguity, and the engineering of choice. *The Bell Journal of Economics*, 9, 587-608.

[2] Boudon, R. (2003). *Bonnes raisons*. Paris: PUF.

[3] Kuty, O., & Dubois, C. (2019). *De la valeur à la norme: Introduction à la sociologie*. De Boeck Supérieur.

Premièrement, ces dispositifs sont-ils vraiment intelligents ? Revenons à l'exemple de Mr A : le fonctionnement du dispositif dépend de la nature du diagnostic posé sur l'état de santé de Mr A. S'agit-il d'un autodiagnostic, du résultat d'un test (il existe divers types de tests dont on sait que la fiabilité n'est pas absolue) ou du diagnostic posé par son médecin traitant ou par un médecin hospitalier ? Toutes ces options ne se valent pas. Comment le système les intègre-t-elles ? De plus, le système n'est-il pas impuissant si Mr A est porteur asymptomatique du virus (et donc non testable spontanément) ou s'il se signale malhonnêtement comme « porteur » pour nuire au système, à son voisinage ou à son employeur ?

Deuxièmement, ces dispositifs sont-ils vraiment efficaces ? Malgré les limites qui viennent d'être évoquées, l'efficacité de tels dispositifs suppose que les citoyens l'adoptent en masse. A supposer que le seuil minimum d'adoption du dispositif soit de 60% de la population, sa nature exclut *a priori* diverses catégories parmi les plus vulnérables au virus, telles que les personnes âgées, incarcérées, internées, hospitalisées ou sans domicile fixe ne possédant pas de smartphone ou n'utilisant pas la fonctionnalité Bluetooth. Cela fait beaucoup de monde ! Ces catégories vulnérables sont plus exposées à la fracture numérique, mais elles constituent également des porteurs et donc des transmetteurs potentiels du virus. Au-delà de ces limites, et indépendamment de ces catégories de (non-)utilisateurs, le dispositif comporte des angles morts. Ainsi, il ne peut tenir compte des risques de contamination par les objets ou par des surfaces infecté(e)s.

Troisièmement, ces dispositifs sont-ils vraiment sûrs ? De tels dispositifs reposent sur la pseudonymisation, c'est-à-dire l'assignation d'un code alphanumérique à chaque smartphone. Par conséquent, ces systèmes d'information ne reprennent directement ni les noms, ni les adresses physiques des propriétaires de ces smartphones. Toutefois, les possibilités (et donc les risques) de réidentification de ces propriétaires et de leurs contacts sont bien réels, si bien que l'on ne peut pas parler d'anonymisaton au sens entendu par le RGPD. Les dispositifs de *tracing*, en contrevenant au RGPD et au respect de la vie privée, sont donc porteurs d'insécurité juridique. Ils s'articulent ainsi difficilement aux valeurs et aux normes qui caractérisent nos démocraties occidentales.

« Les trois zones d'incertitudes mentionnées ici prêtent à débat » diront les concepteurs et promoteurs des dispositifs de *tracing*. Certains s'empresseront même de démontrer que ces incertitudes sont relatives et provisoires. Divers avis, comme celui délivré par l'Autorité de Protection des Données le 28 avril 2020, indiquent les nombreuses conditions auxquelles ces dispositifs devraient répondre. Ces avis informent les travaux parlementaires qui visent à définir le cadre juridique et les procédures de mise en œuvre de ces dispositifs. Or, comme l'enseignait déjà Michel Crozier il y a 60 ans[4], ces règles et procédures sont elles aussi incomplètes, si bien qu'elles ne parviennent jamais à supprimer les zones d'incertitudes mais seulement à les déplacer, tout en multipliant les risques de leur contournement et détournement.

Mais comme les acquis de la sociologie des organisations restent peu connus et rarement appliqués, il convient d'insister sur les risques culturels induits par de tels outils. En effet, dans le contexte pandémique, la peur joue un rôle central. On peut dire qu'elle constitue « le » principal dispositif de contrôle social. Celui-ci se compose de cinq dimensions facilement saisissables.

[4] Crozier, M. (1963). Le phénomène bureaucratique, Ed. du Seuil, coll. *Points, Paris*.

Commençons par les quatre premières composantes de la peur. Celle-ci est d'abord (1) **une émotion** qui se manifeste au travers de sensations physiques chaque fois que nous sommes menacés. La peur de marcher sur un serpent et celle face à un individu en colère provoquent une accélération de notre pouls, des frissons ou une boule au ventre et nous incitent à fuir ou à affronter la menace. Chaque menace constitue une source d'informations que traite notre cerveau pour nous permettre de réagir de manière adaptée face à des événements similaires et récurrents[5]. La peur est donc aussi (2) **un ensemble d'apprentissages** permettant à notre cerveau de connaître et reconnaître les dangers. À ce titre, les peurs affectent notre vie physiologique et sociale. La peur est en outre (3) **une réaction**. Ainsi, j'ai respecté le confinement ; je mets désormais un masque pour aller travailler ; je me lave les mains dès que j'arrive dans un magasin, au bureau et chez moi, etc. La peur est également (4) **une interprétation** et non un réflexe pavlovien. Ainsi, j'interprète le fait d'aller faire les courses, d'aller travailler et de rentrer à la maison comme une source de risque pour moi et pour les autres.

Diverses recherches ont mis en évidence le dispositif de contrôle social que constitue la peur dans le système pénal et carcéral[6] (la prison fait peur à tout le monde). D'autres recherches ont étudié son instrumentalisation dans les politiques urbaines (la théorie de la vitre brisée). D'autres encore ont souligné son importance dans ce que Michel Foucault appelle la gouvernementalité[7]. Ce concept désigne la rationalité permettant de gouverner la conduite des personnes en s'appuyant sur la participation volontaire de celles-ci. Nombreux sont les dispositifs de gouvernementalité peuplant nos existences : caméras de surveillance, identifiants et mots de passe, cartes d'identité et cartes bancaires, statistiques et indicateurs de performances, etc. Les outils numériques de *tracing* s'inscrivent dans cette panoplie. Leur (non-)adoption constitue une décision politique de première importance. Leur adoption consisterait à responsabiliser toujours plus des citoyens conçus comme de « simples » facteurs de risque et contraints de s'auto-surveiller, en bons citoyens dociles et disciplinés. Leur non-adoption consisterait à responsabiliser l'État et les institutions publiques conçus comme serviteurs de la population et soucieux de réduire le sentiment d'anxiété, la peur et les risques pathogènes qu'elle entraîne, surtout en temps de crise.

L'adoption ou le rejet de tels dispositifs engage donc les élus mais aussi les générations futures car, si la peur est une émotion, un processus d'apprentissage, une réaction et une interprétation, elle est aussi (5) **une mémoire individuelle et collective**[8]. C'est cette cinquième dimension qui permet de saisir la force des dispositifs de contrôle social qui, tous, reposent sur la peur. Par conséquent, l'adoption d'une application de *contact tracing* renforcerait l'anxiété et la méfiance entre citoyens. Parmi ces citoyens, comment les enfants, exposés depuis leur plus jeune âge aux mises en garde omniprésentes les incitant à se méfier de soi et d'autrui peuvent-ils encore parvenir à tisser avec confiance les liens au monde ? Comment apprendront-ils la confiance nécessaire à la vie ? Comment apprivoiseront ils l'idée que la maladie et la mort peuvent à tout moment frapper l'être humain qu'ils sont aussi bien que leurs proches, par-delà – et parfois, indépendamment de – leur responsabilité et celle de l'État, au même titre que tous ceux qui les ont précédés sur Terre ? A ce niveau, la prudence dont a fait preuve l'Autorité de Protection des Données dans son avis du 28 avril 2020 est encourageante. Puisse-t-elle inspirer nos élus.

---

[5] Debiec, J., & LeDoux, J. (2004). Fear and the brain. *Social Research*, 71, 4, 807-818.

[6] Chauvenet, A. (2009). Les longues peines: le «principe» de la peur. *Champ pénal/Penal field*. https://journals.openedition.org/champpenal/7556

[7] de Courville Nicol, V. (2006). Pour une sociologie culturelle foucaldienne... de la peur. *Sociologie et sociétés*, *38*(2), 133-150.

[8] Debiec & LeDoux (idem).