

Le double paradoxe de l'application « StopCovid »

21 avril 2020

Le Gouvernement présente l'application « StopCovid » comme un outil d'accompagnement du déconfinement respectueux des libertés. A y regarder de plus près, StopCovid n'est pas aussi « indolore » sur le plan de la vie privée qu'annoncé, et risque d'être d'une efficacité limitée.

Dans son intervention du 13 avril 2020, le Président de la République confirmait que le Gouvernement, à l'instar d'autres pays et entreprises, travaillait à une application mobile qui « *permettra de savoir si, oui ou non, l'on s'est trouvé en contact avec une personne contaminée* ». Quelques jours plus tôt, des représentants du Gouvernement présentaient les grands traits de ce projet, « StopCovid ». StopCovid fonctionnerait comme suit : lorsque deux personnes munies de smartphones dotés de l'application se rapprocheraient, les smartphones s'enverraient leurs coordonnées respectives. Dès lors qu'un utilisateur serait testé positif, les utilisateurs entrés en contact avec lui les jours précédents en seraient informés et pourraient alors prendre les mesures nécessaires (tests médicaux, confinement renforcé).

Pour l'heure, StopCovid est à l'étude. Cela n'a pas empêché le Gouvernement d'énoncer d'emblée ses principes, éminemment protecteurs de la vie privée : installation volontaire ; données anonymes ; aucune géolocalisation ; fermeture de l'application une fois la crise sanitaire passée. En somme, un traçage « zéro impact » pour la vie privée ! A l'analyse cependant, StopCovid baigne dans un double paradoxe : paradoxe d'une application de *contact tracing* « indolore » sur le plan de la vie privée, d'abord ; paradoxe d'un outil qui s'émanciperait des contraintes de la société dans laquelle il se déploie, ensuite.

Les « données anonymes » : invraisemblables

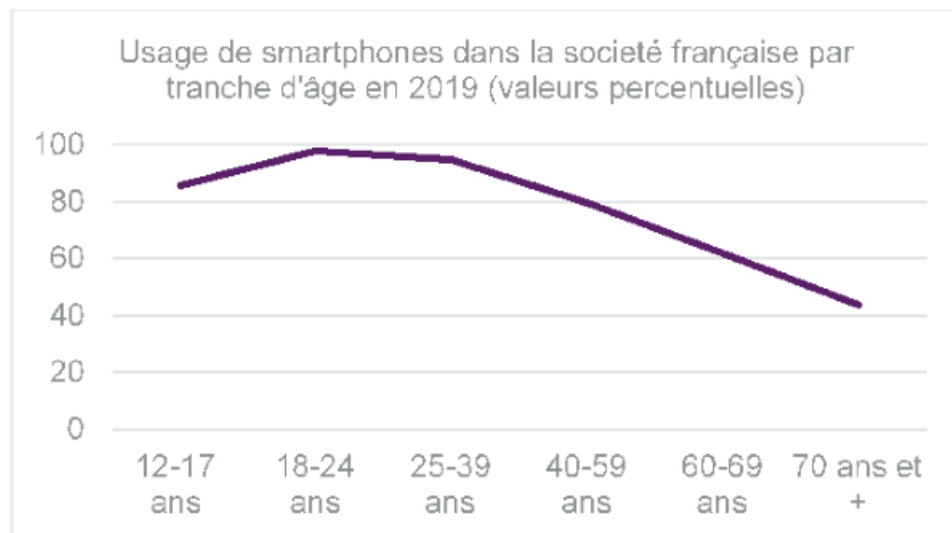
Il paraît peu vraisemblable que les données collectées par StopCovid constituent des « données anonymes » au sens du Règlement Général sur la Protection des Données (« RGPD »). Aux termes de ce texte, une donnée est anonyme lorsqu'elle ne concerne aucun individu identifié ou identifiable. Pour évaluer si tel est le cas, le RGPD requiert d'examiner si l'entité responsable de l'usage des données – ici certainement l'Etat – ou toute autre personne – tel qu'un utilisateur de l'application – peut, à l'aide des moyens d'identification à sa disposition, distinguer un utilisateur parmi les autres.

Or, on voit mal comment l'Etat, ou l'utilisateur de l'application dans certains cas, ne pourrait être en mesure d'isoler un utilisateur parmi les autres. Dès l'installation de l'application en effet, l'utilisateur sera probablement invité à fournir une adresse email ou un numéro de téléphone, si bien que chaque compte sera relié à un individu. Ensuite, l'utilisateur devra pouvoir indiquer *via* l'application ou auprès des autorités sanitaires s'il est infecté – ce qui constitue une donnée de santé – et cette information devra être relayée par un serveur auprès d'autres utilisateurs. Enfin, les utilisateurs informés de ce qu'ils ont été en contact avec une personne infectée pourraient, dans le cas où ils ont croisé peu de personnes au cours de la période de référence, déduire l'identité de la personne infectée.

Aussi, en parlant de « données anonymes », les annonces pour l'heure font l'économie d'une réflexion sur les risques d'identification de StopCovid.

L'obligation d'installation : impensable

L'efficacité de StopCovid sera fonction de plusieurs facteurs, dont le taux d'équipement de la population en smartphones. D'après le CREDOC, ce taux était de 77% en moyenne en 2019, et baissait avec l'âge de la population.



Autrement dit, les populations les plus fragiles face au COVID-19 – les personnes âgées – sont les moins susceptibles de posséder un smartphone ! Réfléchir à la maximisation de l'outil requiert donc de dépasser la position de principe d'une application optionnelle et s'interroger : StopCovid peut-il se passer du consentement des utilisateurs et être obligatoire ?

Sur le consentement, d'abord : il peut justifier la collecte de données personnelles s'il est totalement libre (dans le contexte de StopCovid, étant donné la pression sociale à contribuer à la lutte contre le COVID-19, le consentement ne sera libre que s'il est évident que la participation est optionnelle et sans conséquence). Le RGPD prévoit d'autres moyens pour justifier la collecte de données : l'Etat pourrait *a priori* s'appuyer sur la nécessité de sauvegarder les intérêts vitaux de la population ou d'exécuter une mission d'intérêt public (en l'occurrence assurer la sécurité sanitaire).

Toutefois, il faut compter avec les exigences d'une autre législation importante, la Directive « e-privacy ». Son article 5(3) impose, sous réserve d'exceptions, d'obtenir le consentement de l'utilisateur avant toute action visant à stocker ou à accéder à des données localisées dans son « équipement terminal » (ici son smartphone), que ces données soient personnelles ou non. Or, StopCovid effectuera nécessairement une telle action (par exemple en accédant aux coordonnées chiffrées du smartphone, ou en y stockant le nom et les caractéristiques de l'application). Par conséquent, le seul moyen pour le Gouvernement d'échapper au consentement serait de faire adopter une loi d'exception, la Directive « e-privacy » l'autorisant pour les besoins de sauvegarder la « sécurité publique » (qui pourrait recouvrir la sécurité sanitaire).

Sur l'obligation d'installer l'application, ensuite : outrepasser le consentement des utilisateurs à la collecte de leurs données n'est pas suffisant pour rendre l'installation de StopCovid obligatoire, et donc pleinement efficace. Une étape supplémentaire est nécessaire : édicter un devoir légal et le « sanctionner », par exemple par des amendes. Une telle démarche soulèverait évidemment de nombreuses difficultés, dont celle que les personnes peu accoutumées au numérique ou ne disposant pas d'un smartphone en seraient disproportionnellement affectées (la Commission

européenne y est d'ailleurs opposée).

L'appel de l'Europe

Les défis du *contact tracing* ne pourront être surmontés sans la coopération européenne. Ironie du destin, le jour où le Gouvernement dévoilait StopCovid, la Commission européenne lançait un appel aux Etats Membres pour développer des orientations communes concernant les applications de lutte contre le COVID-19, ce qui fut fait le 15 avril. Cette « boîte à outils » devrait permettre d'harmoniser les démarches nationales, d'assurer leur compatibilité avec le droit de l'Union, et de faire fonctionner les applications lorsque des utilisateurs de différents pays entrent en contact.

A crise globale, réponse globale ou à tout le moins européenne doit être apportée, en visant la meilleure efficacité tout en préservant les droits fondamentaux. En tout état de cause, StopCovid ne sera qu'un des outils permettant d'entrevoir un déconfinement, mais sûrement pas le remède au virus qui a ravagé nos sociétés.

Vos contacts principaux



Christophe Fichet

Associé, Paris

D + 33 1 42 68 35 30

M +33 6 60 64 94 77

christophe.fichet@dentons.com