ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Relevé des échanges

Lundi 27 avril 2020
Séance de 14 heures

Relevé des échanges n° 4

SESSION ORDINAIRE DE **2019-2020**

Office parlementaire d'évaluation des choix scientifiques et technologiques

Présidence de M. Gérard Longuet, *président*

ASSEMBLÉE NATIONALE

Office parlementaire d'évaluation des choix scientifiques et technologiques

Lundi 27 avril 2020

- Présidence de M. Gérard Longuet, sénateur, président de l'Office -

La réunion est ouverte à 14 h 05.

L'Office parlementaire d'évaluation des choix scientifiques et technologiques s'est réuni, le lundi 27 avril 2020, en visioconférence, pour auditionner M. Cédric O, secrétaire d'État auprès du ministre de l'économie et des finances et du ministre de l'action et des comptes publics, chargé du numérique, sur les initiatives numériques de l'État pour lutter contre l'épidémie de Covid-19.

M. Gérard Longuet, sénateur, président de l'Office, a remercié M. Cédric O, secrétaire d'État chargé du numérique, d'avoir accepté de consacrer du temps pour présenter à l'Office les initiatives numériques de l'État au service de la lutte contre le Covid-19. L'Office a beaucoup travaillé sur ce sujet et souhaite pouvoir éclairer pleinement le Parlement sur les enjeux, les bénéfices et les risques des outils numériques qui pourraient être déployés pour contribuer à la lutte contre l'épidémie.

Cette audition a pour but de discuter de l'utilisation du numérique dans les solutions visant à tracer les personnes potentiellement contaminées par le SARS-CoV-2, avec le double objectif de rassurer les citoyens et de permettre un retour à une situation plus normale que celle qui prévaut actuellement.

M. Cédric O, secrétaire d'État auprès du ministre de l'économie et des finances et du ministre de l'action et des comptes publics, chargé du numérique, s'est réjoui de pouvoir s'exprimer devant l'Office sur un sujet aussi important dans le débat public et a indiqué partir du principe que l'Office a déjà connaissance des grandes lignes de l'application StopCovid et de son fonctionnement.

StopCovid est une application pour smartphone qui historise les contacts de proximité en enregistrant sur le téléphone, sous la forme de pseudonymes, les personnes avec lesquelles le porteur du smartphone a été en contact. Différentes architectures existent pour mettre en œuvre une telle fonction.

Ce n'est pas une solution de géolocalisation comme ont pu en choisir certains pays européens, mais une solution reposant sur la technique *Bluetooth*, qui ne permet de repérer que des positions relatives, de détecter une proximité. Personne, pas même l'État, n'a accès à la liste des interactions sociales. L'utilisateur ne peut lui-même connaître ni la liste de ses interactions, ni le contact d'où aurait pu venir la contamination en cas d'alerte.

L'application permet de se déclarer positif au Covid-19 pour que les personnes avec lesquelles on a été en contact soient averties, puissent se mettre en relation avec des enquêteurs sanitaires et puissent prendre des mesures de prophylaxie pour ne pas contaminer d'autres personnes.

Pour les épidémiologistes, ces enquêtes sont le seul moyen d'éviter la reprise de l'épidémie et un nouveau confinement, avec ses conséquences économiques et sociales, voire démocratiques. Elles ont été réalisées à petite échelle en France, notamment aux Contamines-Montjoie, et à très grande échelle en Corée du Sud, qui a mis en place pour cela une organisation quasi industrielle. Elles devront être mises en œuvre par tous les pays du monde. Les exemples japonais, chinois ou singapourien montrent que les tests et les masques, s'ils sont nécessaires, ne sont pas suffisants. Il est également indispensable de mettre en place un système d'enquête sanitaire, humain et peut être technique.

Les enquêtes sanitaires sont menées sous forme d'un entretien en face-à-face ou téléphonique, ce qui n'implique donc aucune exigence pour les individus concernés en termes de connectivité ou de possession d'un smartphone. Ainsi, aux Contamines-Montjoie, des enquêteurs sont allés voir les personnes identifiées ou leur ont téléphoné. Ces enquêtes se heurtent néanmoins à plusieurs difficultés, dont deux significatives. D'une part, en raison du stress lié à la contamination, les individus porteurs du virus ne se souviennent pas de l'ensemble des personnes croisées, même parmi leurs connaissances, ne serait-ce que dans les cinq derniers jours. De fait, en dehors des périodes de confinement, le nombre de contacts quotidiens peut être de vingt à quarante, d'après les spécialistes. D'autre part, dans les zones urbaines denses, notamment dans les transports en commun, les lieux publics et les commerces, retrouver les personnes croisées s'avère impossible. Par exemple, personne ne serait capable d'identifier les passagers rencontrés par un patient dans le métro. Au mieux, ceux-ci seront symptomatiques et contamineront d'autres personnes durant quelques jours, avant d'être testés et isolés. Au pire, ils seront asymptomatiques et en contamineront un très grand nombre. C'est un cas de figure où l'application trouve toute son utilité : pour une population urbaine, active, empruntant les transports en commun, qui se croise dans des lieux de forte densité.

Il faut bien comprendre comment l'application sera utilisée. Certains commentateurs politiques, probablement insuffisamment informés, affirment qu'il faudrait que 60 % au moins de la population utilisent l'application pour qu'elle soit efficace. Ce taux n'a aucun sens, comme l'a clairement indiqué Christophe Fraser, épidémiologiste à Oxford, directeur de l'étude qui a été publiée sur ce sujet dans la revue *Science*[1]. Dès que l'application commence à être diffusée et utilisée, notamment en zone urbaine, elle permet de toucher des personnes que les enquêtes sanitaires ne pourraient jamais atteindre d'une autre façon. Ces quelques pourcents ou quelques centaines de personnes pourront entrer dans un processus sanitaire, alors qu'elles en resteraient exclues faute d'application. Bien sûr, plus sa diffusion sera large, plus l'application sera utile, parce qu'elle permettra de toucher plus de monde. La question d'un taux minimum de diffusion dans la population n'a donc pas grand sens, ainsi que les plus éminents épidémiologistes et de nombreux personnels sanitaires l'ont rappelé dans une tribune parue le 25 avril dans le quotidien *Le Monde*.

Pour autant, l'utilité indéniable de cette application ne donne évidemment pas un blanc-seing au Gouvernement sur les conditions de son déploiement. Toutes les garanties sont prises pour que la vie privée soit préservée : l'installation de l'application est volontaire ; l'application est non identifiante, car compte tenu du protocole choisi, il n'existe nulle part de liste des personnes infectées, y compris sur un serveur central ; personne n'a accès à la liste des interactions sociales d'un utilisateur de l'application, car celui-ci n'est alerté que dans la mesure où il a été en contact avec une personne infectée, et il ne reçoit cette information que pour être

[1] Cette étude est parue le 8 mai 2020. Elle est consultable à l'adresse suivante : https://science.sciencemag.org/content/368/6491/eabb6936.

averti du risque qu'il court et qu'il peut faire courir à ses proches ; enfin, les données seront effacées après un nombre de jours déterminé, qui sera fixé par les épidémiologistes, en fonction des connaissances sur la temporalité de l'infection. Évidemment, l'application n'a pas vocation à réaliser d'autres opérations que celles décrites ici, ou à être déployée au-delà de l'épidémie.

Enfin, ce projet est totalement transparent. Le protocole développé par l'INRIA et l'Institut Fraunhofer, dénommé Robert, a été publié voici une dizaine de jours. L'application sera *open source*, ce qui implique que tout informaticien pourra examiner son code et assurer à la société civile qu'elle fait bien ce que le Gouvernement annonce. Pour la partie serveur, dont le code est nécessairement moins accessible, le Gouvernement souhaite installer un comité de suivi et de transparence, composé d'organisations non gouvernementales, de spécialistes du numérique, de parlementaires, de juristes, etc. Ce comité aura toute latitude pour faire réaliser les audits techniques qui permettront de garantir aux Français que l'ensemble de l'architecture est conforme aux objectifs affichés.

Ce projet est un projet interétatique européen. Y travaillent en effet les Anglais, les Italiens, les Espagnols, les Français et les Allemands, ainsi que les Luxembourgeois et les Monégasques, ou encore les Estoniens. Au demeurant, la France a demandé, par la voix du secrétariat d'État au numérique, qu'une réunion du Conseil de l'Union européenne « Télécommunications » se tienne début mai, afin de mieux coordonner les efforts européens. Un lien étroit a été établi avec le commissaire Thierry Breton, car le sujet entre dans son champ d'attributions.

Un débat a lieu, au sein de la communauté scientifique, sur les risques que présentent les deux types de protocoles pouvant être utilisés, à savoir le protocole décentralisé DP3T et le protocole centralisé Robert.

À l'origine, la France et l'Allemagne ont étudié les deux protocoles, avant même que Google et Apple n'entrent dans le débat. Au tout premier stade, les Suisses préconisaient un protocole décentralisé et les Allemands un protocole centralisé – la France ne s'est en effet jointe à la réflexion qu'une semaine après eux.

Selon les estimations concordantes de l'INRIA, de l'Institut Fraunhofer, de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de son homologue allemand, le protocole Robert offre plus de garanties, tant dans le domaine de la protection de la vie privée qu'en matière d'interactions avec le système de santé.

D'abord, même s'il n'y a pas de solution technique sans défaut, le protocole Robert se borne à enregistrer, sous forme de pseudonymes, l'historique des contacts de chaque individu sur son téléphone au gré de ses allées et venues. Cet historique n'existe que sur son téléphone. Le jour où l'utilisateur est déclaré positif au Covid, son application envoie cette liste de pseudonymes de contacts sur un serveur central. Ce dernier centralise donc, sous forme de pseudonymes, les contacts de toutes les personnes testées positives, mais non la liste de ces personnes elles-mêmes. Des listes de contacts cohabitent ainsi sur un serveur central, sans qu'il soit possible de les relier à une quelconque personne testée positive. Régulièrement, chaque téléphone sur lequel est installée l'application consulte le serveur pour savoir si l'un de ses propres pseudonymes n'est pas présent dans ces listes. Le cas échéant, le téléphone se voit notifier immédiatement que son possesseur a été en contact avec une personne testée positive au Covid.

Voilà comment fonctionne le protocole Robert. Il n'y a nulle part de liste des personnes contaminées. Il y a certes un serveur central sur lequel sont stockées les listes des pseudonymes des contacts des personnes contaminées. Mais, de ce fait, il n'existe pas de liste des personnes contaminées elles-mêmes, sur laquelle un groupe de hackers ou une agence de renseignement pourrait mettre la main après s'être introduit frauduleusement sur le serveur. C'est un avantage très important par rapport à la solution dite « décentralisée ».

Le protocole DP3T, promu par les Suisses et favorisé par Apple et Google, prévoit d'emmagasiner de la même manière l'historique des pseudonymes des contacts sur le téléphone de l'utilisateur. Si celui-ci est déclaré positif au Covid, son propre pseudonyme est communiqué, non à un serveur central, mais à un outil répartiteur (*dispatcheur*), qui le renvoie à l'ensemble des téléphones sur lesquels l'application est installée. Chaque téléphone rapproche alors le pseudonyme reçu de la liste des pseudonymes de contacts qu'il a stockés, pour voir s'il y apparaît.

Par conséquent, l'ensemble des pseudonymes des personnes contaminées au niveau européen est transmis à l'ensemble des téléphones des citoyens européens… Cela doit amener à considérer de plus près le mot « décentralisé ». Car ce que l'on décentralise ici, c'est… une centralisation.

Évidemment, l'application est protégée et cryptée. Mais tant l'INRIA que l'ANSSI considèrent que ce type d'architecture est vulnérable à des attaques telles que l'« attaque du paparazzi ». Celle-ci consiste à exploiter la liste des pseudonymes des gens testés positifs afin de savoir, au prix de quelques manipulations, si votre voisin d'immeuble est contaminé ou de connaître le nombre de personnes contaminées dans votre immeuble. Cela n'est pas possible avec le protocole Robert, puisqu'avec lui il n'existe pas de liste de personnes contaminées. C'est pourquoi l'INRIA et l'ANSSI, en lien avec l'Institut Fraunhofer, estiment que le protocole décentralisé n'est pas une option acceptable au regard de la protection de la vie privée.

Sur ces entrefaites, Apple et Google sont entrés dans la discussion, au moment où les autorités étaient de plus en plus inquiètes de la situation à Singapour, où l'application s'avère ne pas fonctionner, ou très mal, sur iPhone : en effet, les iPhones ne permettent pas d'utiliser la connexion Bluetooth en arrière-plan de façon continue. Or une détection efficace des contacts suppose que l'application soit opérationnelle non par intermittence, mais en permanence, et il n'est pas possible d'en faire en permanence la tâche de premier plan, car la personne doit évidemment pouvoir utiliser son smartphone à autre chose.

Apple et Google ont proposé de travailler à une architecture technique qui permette de mieux intégrer et interconnecter les iPhones et les smartphones Android. Mais ils ont refusé de travailler à un protocole centralisé, préférant les options retenues par DP3T. Telle est la condition qu'ils ont posée à leur coopération. La discussion n'était pas facilitée par le fait qu'à ce moment-là, les Suisses étaient encore présents dans le consortium et qu'ils discutaient donc en parallèle, d'un côté avec Apple et Google, de l'autre avec nous.

La France et l'Allemagne ont opposé une fin de non-recevoir aux propositions d'Apple et Google. Elles ont, de manière souveraine, après avoir consulté leurs autorités de santé et pris en considération leurs systèmes d'information, considéré que le protocole promu par ces entreprises n'était pas protecteur des citoyens et qu'il ne permettait pas un interfaçage efficace avec les organisations sanitaires. Elles ont donc demandé de modifier la manière dont fonctionnent les iPhones – les téléphones fonctionnant sous Android posent moins de problèmes.

Ce débat est encore en cours. Mais il n'y aura pas d'application française qui fonctionne sur l'interface de programmation d'application (API) développée par Apple et Google, dans la mesure où celle-ci contraint à utiliser le protocole DP3T. Cela pourrait aboutir, dans certains cas, à ce qu'une telle application ne puisse être déployée que sur 80 % des téléphones, à savoir ceux fonctionnant sous Android. Cela serait très insatisfaisant, mais ce serait déjà mieux que rien, dans un contexte où chaque alerte envoyée à un cas contact réduit le risque de transmission du virus.

Cependant, on peut encore espérer faire entendre raison à Apple. Cet espoir est raisonnable, dans la mesure où la discussion est menée de manière coordonnée avec l'Italie, l'Espagne, la Commission européenne et l'Allemagne.

Revenons à l'Allemagne, dont les positions ont pu paraître surprenantes. Il y a seulement trois jours, un porte-parole indiquait que ceux qui « préfèrent les États » devraient passer par un système centralisé, tandis que ceux qui « préfèrent Apple et Google » devraient passer par un système décentralisé. Cette présentation rapide a le mérite de mettre l'accent sur la nature de l'instance décisionnelle ultime en matière d'application sanitaire.

Mais, ce dimanche, l'Allemagne a annoncé vouloir travailler à une solution décentralisée, tout en donnant à cette déclaration une formulation assez sibylline. La raison de cette volte-face n'est pas technique : le gouvernement allemand demeure persuadé que l'application centralisée est la meilleure solution pour protéger la vie privée des citoyens. La raison est politique : les partisans d'une application décentralisée risquaient d'avoir un poids assez important dans la coalition gouvernementale. Cependant, au-delà des effets d'annonce, le lien entre les équipes françaises et les équipes allemandes n'est pas rompu. Elles continuent à travailler à une solution qui soit la plus proche et la plus interopérable possible.

Quoi qu'il en soit, la position des autorités allemandes ne remet pas en cause l'utilité de l'application comme élément d'un système sanitaire global pour contrôler l'épidémie ; elle ne fait qu'ouvrir la possibilité d'une application qui, le cas échéant, ne serait pas interopérable avec la solution retenue par la France. Cela traduirait une coordination européenne clairement sous-optimale, inconvénient certain mais cependant secondaire par rapport à l'utilité réelle de l'application. On ne peut que regretter ces atermoiements, d'autant que la nouvelle position allemande n'a pas été communiquée aux autorités françaises avant d'être rendue publique. Les discussions avec les autorités allemandes continuent et l'on peut espérer que sera finalement mise en œuvre l'architecture initialement évoquée, en lien avec l'Allemagne, l'Espagne, l'Italie et d'autres pays européens. Tenir la date du 11 mai est un défi compliqué, mais n'est pas impossible. Il faudra en effet tester l'application pour vérifier son bon fonctionnement et son calibrage.

Les entités les plus impliquées dans le projet d'application StopCovid en France sont : l'INRIA, qui assure la maîtrise d'ouvrage et qui est spécialement chargé des algorithmes et de l'interfaçage avec les pays européens ; CapGemini, qui est chargé de la maîtrise d'œuvre, de l'infrastructure globale et de l'architecture du projet ; Dassault Systèmes, qui héberge les données – il n'y a donc pas d'interférences possibles à l'égard du *Cloud Act* – ; Orange, qui s'occupe de la partie applicative, de l'interfaçage avec les téléphones et des questions de connectivité. Deux start-up françaises sont aussi très impliquées : Lunabee Studio réalise l'interface utilisateur en tant que telle et Withings, entreprise connue dans le monde de l'« Internet des objets » – les objets connectés –, travaille sur la capacité à déployer une solution qui ne passe pas par les smartphones. Cette solution ne serait pas disponible le 11 mai, mais plus probablement vers le 15 juin. Elle aurait l'avantage de pouvoir être déployée au profit des

personnes n'ayant pas de smartphone ou ne sachant pas s'en servir. Mais la capacité à réussir ce dernier projet reste sujette à caution et son industrialisation serait compliquée.

M. Gérard Longuet, sénateur, président de l'Office, a remercié M. Cédric O pour les informations détaillées ainsi portées à la connaissance de l'Office.

M. Cédric Villani, député, premier vice-président de l'Office, a relevé que les États européens se sont accordés sur le protocole Robert, mais que plusieurs acteurs développent néanmoins leurs projets séparément. Des équipes allemandes développent-elles en parallèle leur propre solution ?

M. Cédric O, secrétaire d'État chargé du numérique, a rappelé que les différents projets sont fondés sur des briques communes, notamment le recours à la technique *Bluetooth* et l'exigence d'interopérabilité.

L'interopérabilité est d'abord liée à l'architecture choisie. Il n'est pas certain que DP3T soit interopérable avec le protocole Robert. Pour être certain de l'interopérabilité, il faut s'appuyer sur la même architecture. C'est pourquoi Italiens, Français et Allemands travaillaient sur une même base, même si les applications qui en découleront ne seront pas forcément identiques. Cela tient aussi à ce que la définition d'un cas contact n'est pas la même d'un pays à l'autre, non plus que les critères d'inclusion d'un cas positif dans l'application. Les messages officiels diffèrent eux aussi, de même que les conséquences qui en sont tirées sur le plan sanitaire.

Même si l'infrastructure est commune, la partie émergée de l'iceberg ne l'est donc pas forcément. Ainsi une équipe allemande développe une interface allemande et une équipe française développe une interface française.

M. Cédric Villani, député, premier vice-président de l'Office, s'est interrogé sur le rôle de l'INRIA : l'Institut travaille-t-il pour la seule partie française ou dans un cadre plus large ?

M. Cédric O, secrétaire d'État chargé du numérique, a indiqué que l'INRIA et l'Institut Fraunhofer effectuent des développements parallèles, mais communiquent régulièrement. Par exemple, les équipes allemandes ont réalisé un travail très important sur la calibration du *Bluetooth,* c'est-à-dire sur la manière dont est calculée la distance entre deux smartphones, point qui a longtemps constitué une difficulté importante. Elles ont communiqué leurs résultats à l'INRIA et celui-ci a pu les exploiter dans le cadre du projet français.

Chacun a ensuite poursuivi ses développements propres. Il y a donc à la fois de la coordination et des travaux parallèles. Le but est d'aboutir à des applications certes interopérables, mais dont l'utilisation se fera essentiellement dans un cadre sanitaire national.

M. Cédric Villani, député, premier vice-président de l'Office, a souligné l'importance du fait que deux protocoles différents existent pour une application de type StopCovid. L'attention a été attirée sur les critiques faites au protocole Robert, notamment celles formulées par un collectif de chercheurs dans le texte « Le traçage anonyme, dangereux oxymore. Analyse de risques à destination des non-spécialistes ». Le protocole DP3T est certes décentralisé, mais conduit à copier sur le téléphone de chaque utilisateur la base de données des personnes contaminées. Dans le protocole Robert, une telle base n'existe pas. L'ANSSI estime

que ce protocole est donc le plus sûr face aux attaques de pirates. Que répondent à cela Google, Apple ou les équipes suisses ?

M. Cédric O, secrétaire d'État chargé du numérique, a relevé que le document évoqué, disponible sur le site risques-tracage.fr, énumère des failles possibles, mais que certaines sont déjà prises en compte par le protocole. Par exemple, celui-ci ne permet pas de notifier une alerte à une personne dont les contacts ont été trop peu nombreux. Le scénario « paparazzi » présenté dans le document ne peut donc pas se réaliser, puisqu'il consiste à placer un téléphone dédié à côté d'une célébrité de sorte qu'une alerte signifiera que c'est cette célébrité, contact unique du téléphone, qui est infectée. Certaines « failles » ne sont que pures hypothèses.

Pour autant, d'autres failles évoquées dans le document ne font pas débat. Chacune des solutions, Robert et DP3T, présente des inconvénients qui sont appréciés diversement selon les pays. Apple, Google et les équipes suisses ne nient pas que DP3T est sensible au « risque paparazzi », mais ils estiment que ce risque est préférable à celui qui résulte du transit des données par un serveur central placé sous le contrôle d'un État, comme c'est le cas avec le protocole Robert. Cela exprime des préférences collectives différentes et, en quelque sorte, clôt le débat.

M. Cédric Villani, député, premier vice-président de l'Office, a estimé que Google et Apple craignent d'ouvrir des droits qui les conduiraient à devoir demain fournir des solutions à des États qui surveillent leurs citoyens.

M. Cédric O, secrétaire d'État chargé du numérique, a admis que c'était, en effet, une préoccupation d'Apple et de Google – car, sur un plan purement technique, il ne serait pas très difficile à ces entreprises d'accéder à la demande du gouvernement français. Mais ce serait pour Apple créer un précédent. Apple ne veut pas ouvrir un accès permanent au *Bluetooth* afin d'éviter qu'un État puisse surveiller ses citoyens. Il considère qu'il ne peut pas accepter d'ouvrir cet accès à des pays tels que le nôtre et le refuser à d'autres. C'est un argument qu'un État démocratique ne peut pas entendre, surtout dans un temps de crise. Qu'Apple argue ainsi de sa qualité d'entreprise privée pour décliner tout engagement, pour refuser de choisir, voilà qui témoigne d'une extrême inconséquence. Même dans un secteur aussi sensible que l'armement, les entreprises ont la possibilité de choisir leurs clients et d'ajuster leur offre. Mais Apple paraît envisager autrement les rôles respectifs des États et des entreprises privées.

Pour éviter de se retrouver dans une position délicate vis-à-vis d'autres pays, l'entreprise pourrait au demeurant déléguer la décision d'ouvrir l'accès au *Bluetooth* à une tierce autorité, comme le Comité européen de la protection des données (CEPD). Il reviendrait à cet équivalent européen de la CNIL de certifier, tous les trois mois, que l'application française reste respectueuse des libertés publiques et mérite de demeurer sur sa « liste blanche ». En refusant de faire aucune distinction entre les États, Apple se soustrait à ses responsabilités. C'est dramatique dans la crise sanitaire que nous vivons, alors que des dizaines de milliers de personnes décèdent sur le sol européen.

M. Julien Aubert, député, a interrogé le secrétaire d'État sur le statut des données qui seront générées par l'application.

M. Cédric O, secrétaire d'État chargé du numérique, a confirmé qu'il s'agissait de données de santé.

M. Julien Aubert, député, s'est interrogé sur le fait que ces données de santé puissent être hébergées par une entreprise d'armement, de droit privé, dépourvue de tout lien avec une activité médicale.

M. Cédric O, secrétaire d'État chargé du numérique, a précisé que Dassault Systèmes n'est pas une entreprise d'armement, mais une entreprise de logiciels informatiques, impliquée depuis longtemps dans la production de services numériques pour le secteur médical – elle est connue pour la réalisation de simulations du système cardiovasculaire. Son expertise a été enrichie par la récente acquisition de l'entreprise américaine Medidata, ce qui en fait l'une des meilleures entreprises de logiciels au niveau mondial dans le domaine de la santé. L'entreprise a donc des activités totalement distinctes de celles du groupe Dassault, même si elle a des liens capitalistiques avec celui-ci.

M. Julien Aubert, député, a demandé des précisions sur l'appartenance des données générées par l'application StopCovid, au regard des modalités de leur hébergement. Si une entreprise privée les héberge, ces données ne risquent-elles pas d'être utilisées par celle-ci ou par ses filiales, comme pourraient le faire des filiales des GAFAM ?

S'agissant de données de santé, il semblerait plus pertinent que la Caisse nationale d'assurance maladie (CNAM) héberge ces données, comme elle le fait déjà pour beaucoup d'autres données médicales. Pourquoi, dans un système centralisé, ne pas faire confiance à la Sécurité sociale – qui n'est d'ailleurs pas l'État ? Un tel dispositif pourrait tirer avantage du fait que la CNAM connaît déjà le numéro d'identification spécifique à chaque individu, et serait alors en mesure d'alerter directement ceux ayant été en contact avec une personne signalée positive au Covid-19. Un dispositif public est préférable à une intervention des entreprises privées, même si celles-ci sont françaises.

M. Cédric O, secrétaire d'État chargé du numérique, a rappelé que tout le protocole repose sur l'anonymat : un crypto-identifiant est généré par l'application, ce qui rend les données non identifiantes. Elles le seraient si le numéro de sécurité sociale leur était associé. Il est vrai que l'anonymisation totale des données rend la solution moins efficace, d'un point de vue sanitaire. D'autres pays, asiatiques mais aussi européens, ont fait le choix de systèmes moins anonymes et plus intrusifs, mais plus efficaces sur le plan sanitaire. En tout état de cause, un stockage de données identifiantes n'aurait probablement pas été approuvé par la CNIL, compte tenu de la législation française.

S'agissant de l'hébergement des données par une entreprise privée, en l'espèce Dassault Systèmes, il faut rappeler que le ministère des solidarités et de la santé reste le responsable légal du traitement des données. L'entreprise Dassault Systèmes a été choisie car elle est bien meilleure que l'État pour déployer une solution de serveur *cloud* sécurisé. L'entreprise, dont les solutions PLM *(Product Lifecycle Management* – Gestion du cycle de vie d'un produit) sont utilisées par de très nombreuses entreprises industrielles à travers le monde, est soumise à des milliers d'attaques informatiques chaque jour ; elle est donc rodée à la sécurisation des données. Ses capacités de résilience aux attaques informatiques vont bien au-delà de celles de la CNAM. Choisir la meilleure entreprise française du domaine nous apporte les meilleures garanties.

M. Ronan le Gleut, sénateur, a indiqué qu'une lettre ouverte, signée par 140 experts en sécurité informatique, du CNRS, du CEA, de l'INRIA et de différentes universités, alertait sur le fait que l'application StopCovid, retraçant les interactions des individus, permettrait de reconstituer ce que l'on appelle le « graphe social ». Les solutions sur lesquelles travaillent les

équipes françaises apportent-elles toutes les garanties au regard des inquiétudes ainsi manifestées ?

M. Cédric O, secrétaire d'État chargé du numérique, a assuré que toutes les garanties possibles sont apportées. Dans le cadre institutionnel et démocratique actuel, l'action du Gouvernement est contrôlée par des contre-pouvoirs et un usage illégal des données est impossible.

Néanmoins, toute solution informatique comporte des risques, tels que ceux pointés par les experts en sécurité informatique. À ce stade, une mise au point s'impose si l'on veut clarifier quelque peu les termes du débat : il n'appartient pas aux experts du numérique de dire si une application est utile ou non pour sortir d'une épidémie. Leur rôle est d'alerter sur de potentielles failles ou d'argumenter en faveur d'une solution plutôt qu'une autre, sur la base des garanties de sécurité qu'elles apportent. Cette expertise est reconnue et bienvenue. Néanmoins, la décision relative à l'utilité de l'application dans la lutte contre l'épidémie de Covid-19 revient aux épidémiologistes, seuls compétents en la matière.

C'est à la CNIL et aux juristes qu'il revient de dire si celle-ci respecte nos lois, nos règles et nos valeurs – la CNIL l'a d'ailleurs fait le week-end dernier, estimant que la solution envisagée était proportionnée au regard des circonstances actuelles.

Enfin, compte tenu de ces informations et de l'ensemble des options disponibles, c'est aux responsables politiques qu'il appartient de prendre la décision finale – en l'occurrence le choix entre un déconfinement suivi d'un reconfinement, et un déconfinement associé à certains outils, dont une application, visant à éviter un reconfinement.

À cet égard, ceux qui, dans l'écosystème numérique, indiquent ne « jamais » vouloir céder au suivi par une application ont beau jeu d'invoquer les grands principes libertaires, car ils n'en assument en aucune manière les conséquences, qu'il s'agisse du nombre de victimes ou d'un nouveau confinement.

M. Pierre Ouzoulias, sénateur, a souligné qu'une application telle que StopCovid sera nécessairement complémentaire des enquêtes sanitaires, qui resteront la base de la lutte contre la pandémie. C'est d'ailleurs ce que démontre l'exemple de la Corée du Sud, État démocratique qui connaît le prix des libertés publiques et a eu recours à cette solution. En France, l'État sait aussi se donner les moyens nécessaires quand la situation l'exige : 32 maladies infectieuses sont ainsi soumises à déclaration obligatoire et donnent lieu systématiquement à une enquête sanitaire qui permet de remonter les chaînes de contamination.

Le choix fait par le Gouvernement de garantir un degré élevé d'anonymat n'est-il pas, justement, contradictoire avec cet objectif d'identification des chaînes de contamination ?

Ensuite, que répondre à l'objection de la CNIL, qui, dans son récent avis, a relevé que l'algorithme 3DES n'est pas recommandé par l'ANSSI car il ne garantit pas un chiffrement suffisamment sécurisé et qu'il ne devrait donc plus être utilisé ?

Enfin, alors qu'Apple persiste dans son opposition à toute forme d'interopérabilité et n'entend pas céder aux demandes des pouvoirs publics, il apparaît urgent que la France se préoccupe de sa souveraineté numérique, sujet qui a été analysé de façon très approfondie par une récente commission d'enquête du Sénat.

M. Cédric Villani, premier vice-président de l'Office, a estimé que, si le Covid-19 devait être inscrit au nombre des maladies à déclaration obligatoire, ce que plusieurs professionnels demandent, il faudrait – comme le suggère l'Ordre des médecins – que la déclaration soit faite par le médecin lui-même pour des raisons d'efficacité, *via* le système d'information de l'assurance-maladie ou du ministère de la santé. Cela n'implique pas que le fichier ainsi constitué soit le même que celui qui serait issu de la mise en œuvre de StopCovid.

M. Cédric O, secrétaire d'État chargé du numérique, a indiqué qu'il n'était pas envisagé de faire du Covid-19 une maladie à déclaration obligatoire, tout en rappelant que seul le ministre des solidarités et de la santé était compétent sur le sujet.

S'agissant de l'apparente contradiction entre l'objectif de garantie de l'anonymat et la nécessité de remonter les chaînes de contamination, le Gouvernement assume son choix de privilégier la protection des libertés publiques. Ce choix pourrait susciter un débat, mais la culture française fait que ce n'est pas le cas.

Certes, l'efficacité de cette application dépend du nombre de ses utilisateurs ; mais dès lors qu'elle commencera à être diffusée, notamment dans les villes ou auprès de personnes qui auront été sensibilisées aux bénéfices qu'elle apporte, elle sera utile, même si elle ne touche que quelques pourcents de la population française et quelques dizaines de pourcents dans les villes. Le Gouvernement fera donc tout pour déployer cette application aussi largement que possible, une fois que tous les paramètres en auront été validés. Pour ce faire, il sait pouvoir compter sur la mobilisation de nombreux acteurs, comme les élus de France urbaine, ainsi que les élus des autres collectivités locales, très demandeurs d'une telle solution du fait des risques propres aux transports en commun, les agences régionales de santé (ARS), les professionnels de santé ou encore les associations caritatives, soucieuses de toucher des publics peu équipés en outils numériques.

Si les Français parviennent à être rassurés sur les garanties que l'application présente, ils l'installeront. Ne s'agit-il pas d'une application non risquée, qui permet non seulement de savoir si l'on prend des risques pour soi, mais aussi si l'on en fait courir à ses proches ?

S'agissant des réserves de la CNIL sur l'algorithme 3DES, il n'a pas semblé que celles-ci soient dirimantes, mais il est trop tôt pour apporter une réponse définitive à ce stade. Le sujet est étudié par l'ANSSI.

S'agissant de la souveraineté numérique, la crise actuelle montre avec encore plus de force la dépendance de la France aux outils américains, en l'absence d'outils européens de qualité équivalente. On peut être impressionné par la qualité de certains outils de visioconférence proposés par des sociétés américaines ; toujours est-il que toutes les garanties ne sont pas nécessairement au rendez-vous. Après avoir étudié différentes solutions françaises, le Gouvernement vient d'ailleurs de décider d'utiliser une solution proposée par Orange.

S'agissant des modalités de déclaration, nous travaillons à un système d'information très robuste capable de gérer les alertes associées à plus de 100 000 tests par jour. Un patient testé positif pourra se signaler dans l'application, en scannant avec son smartphone le *QR code* non-identifiant figurant sur le document qui lui sera remis. Certes, rien ne garantit que celui qui scannera le *QR code* et le patient infecté seront bien la même personne, mais c'est là une conséquence indépassable d'un système que le Gouvernement a tenu à organiser sur une base volontaire.

Mme Florence Lassarade, sénatrice, a demandé si les collégiens et lycéens, dont le retour en établissement est imminent, seraient autorisés à communiquer eux-mêmes leurs données s'ils sont déclarés positifs ou s'il leur faudrait l'accord de leurs parents.

M. Cédric O, secrétaire d'État chargé du numérique, a estimé que, compte tenu des modalités prévues pour le traitement des données, il ne devrait pas y avoir d'obstacle à ce que les mineurs puissent s'équiper de StopCovid – la solution inverse ferait d'ailleurs fi de ce qu'ils semblent être, en l'état des connaissances, un facteur important de diffusion du virus. Au demeurant, les enquêtes sanitaires sont traditionnellement réalisées par entretien direct ou téléphonique, ce qui concerne les mineurs comme les majeurs. Anne Genetet, membre de l'Office, qui a réalisé de telles enquêtes sanitaires, pourrait faire part à l'Office de son expérience. Cela pourrait utilement éclairer le fait que cette application est singulièrement mieux disante que les enquêtes traditionnelles au regard de la protection de la vie privée.

M. Gérard Longuet, sénateur, président de l'Office, a remercié M. Cédric O pour la richesse des informations apportées à l'Office au cours de cette audition et indiqué que celle-ci l'avait conforté dans son opinion favorable à une politique d'alerte numérique volontaire, dans le respect des conditions présentées par le secrétaire d'État.

La réunion est close à 15 h 10.