ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Relevé des échanges

Office parlementaire d'évaluation des choix scientifiques et technologiques

– **Audition** de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) 2

Mardi 12 mai 2020
Séance de 17 heures

Relevé des échanges n° 7

SESSION ORDINAIRE DE **2019-2020**

Présidence de M. Gérard Longuet, *président*

ASSEMBLÉE NATIONALE

Office parlementaire d'évaluation des choix scientifiques et technologiques

Mardi 12 mai 2020

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

La visioconférence est ouverte à 17 h 10.

Audition de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

M. Gérard Longuet, sénateur, président de l'Office. – Je souhaite la bienvenue à M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Cédric Villani, qui est physiquement présent dans la même salle que M. Poupard, animera cette réunion à laquelle les autres membres de l'Office participent à distance.

M. Cédric Villani, député, premier vice-président de l'Office. – Chers collègues, cette audition de M. Guillaume Poupard, directeur général de l'ANSSI, portera sur le développement de l'application française de traçage numérique, couramment appelée StopCovid. Nous avons eu l'occasion d'aborder ce sujet à plusieurs reprises au sein de l'Office, et j'ai fait devant vous des points réguliers le concernant. Cependant, il était indispensable, pour éclairer la représentation nationale et les citoyens, d'entendre un expert nous éclairer sur les questions clés de sécurité informatique.

Monsieur Poupard, peut-être pouvez-vous d'abord expliquer en quelques mots les fonctions de l'ANSSI, puis dresser à grands traits la chronologie du projet StopCovid, la façon dont il est né et dont il s'est développé. Nous souhaiterions en particulier aborder les questions suivantes. Qui le développe, comment et selon quel protocole ? Avec quel degré de publicité ? Quels sont les potentiels conflits d'intérêts ? Quels enjeux se posent en relation avec la protection de la vie privée ? Quel est le rôle de l'ANSSI dans le développement du projet ? Quelle est la situation actuelle du développement, aussi bien du point de vue français qu'international ?

Cette audition un peu particulière se tient au tout début de la sortie progressive du confinement, alors que l'Assemblée nationale et le Sénat ne peuvent pas encore accueillir d'auditions physiques par leurs organes en formation plénière compte tenu des contraintes sanitaires qui subsistent. L'audition fait l'objet d'une captation vidéo visualisable sur Internet à toutes fins utiles, en tant que document susceptible d'éclairer le débat.

M. Guillaume Poupard, directeur général de l'ANSSI. – Je suis directeur général de l'ANSSI, autorité nationale chargée de la défense et de la sécurité des systèmes d'information, placée auprès de la secrétaire générale de la défense et de la sécurité nationale. Le rôle de l'ANSSI est de traiter de manière verticale les sujets liés à la cybersécurité, en particulier ceux qui concernent les structures les plus critiques pour la nation, qu'elles soient publiques ou privées. Par conséquent, l'ANSSI doit faire de la prévention dans le domaine cyber, opérer la régulation, détecter les attaques et aider les victimes. À l'inverse, nous

n'intervenons pas dans le domaine offensif ni dans celui du renseignement. Nous ne sommes pas un service de police ni un service enquêteur, mais plutôt une structure d'experts assez fournie – dans laquelle travaillent aujourd'hui plus de 600 personnes – capable de porter les sujets cyber pour l'ensemble de la nation.

L'application StopCovid vise à tracer les contacts à risque dans le cadre de la crise sanitaire. L'ANSSI n'a pas d'avis à faire valoir sur un certain nombre de sujets : intérêt sanitaire du traçage, paramétrage et utilité de l'application, niveau d'acceptation pour qu'elle fonctionne, etc. Globalement, le pari consiste à développer une telle application pour constater si, une fois en circulation, elle trouve un cas d'usage ou non. Tout en restant dans mon rôle, il me paraît néanmoins important de noter qu'une telle application de traçage de contacts n'est pas anodine, ainsi que l'ont rappelé tous les défenseurs des libertés. C'est pourquoi il est hors de question d'en faire un outil de renseignement et de contrôle des populations. Il est essentiel de prendre garde à ce point, car tout traçage des contacts pourrait rapidement entraîner des dérives s'il était mal opéré.

En définitive, ma position est assez simple : l'outil n'est pas anodin et si son utilité n'est pas avérée, il ne faudra pas le mettre en circulation. Disant cela, c'est davantage le citoyen qui s'exprime. En revanche, si l'utilité d'une telle application est avérée dans le cadre d'une pandémie, un certain nombre de précautions s'imposeront dans le choix des protocoles. En effet, de nombreux choix sont assez dimensionnants, de nature à conserver l'utilité de l'application tout en limitant les risques en termes de sécurité numérique et sur les libertés individuelles.

S'il est décidé de développer et d'utiliser l'application, la première remarque est que le capteur intéressant pour réaliser le traçage est le *smartphone*, que nous sommes nombreux à posséder. Nous l'avons très souvent sur nous, notamment lorsque nous prenons les transports en commun. Il peut donc s'agir d'un usage pertinent, rappelé par le Premier ministre il y a quelques jours. Lorsque deux *smartphones* arriveront à proximité suffisamment étroite – un mètre – pour une durée suffisamment longue – quinze minutes – on pourra considérer qu'il existe un risque sanitaire. Dans ce cas, il faudra prévenir les personnes qui auront été en contact avec un malade, qui lui-même ne se savait pas tel à ce moment-là.

Pour estimer la proximité entre deux personnes sur la base de l'usage de leur téléphone portable, il existe deux techniques possibles. Le positionnement GPS a été écarté dès le départ car beaucoup trop intrusif. En effet, la seule information nécessaire en termes de santé publique est de savoir si une personne à risque était proche à un moment donné, et ce quel que soit l'endroit où il se trouvait. En cela, le GPS fournit beaucoup trop d'informations, dont un certain nombre sont dénuées d'intérêt pour la finalité poursuivie. La deuxième technique possible, retenue par toutes les expérimentations sérieuses, est le *Bluetooth*, protocole conçu pour raccorder divers équipements sans fil au téléphone ou à une tablette. Il s'agit d'un protocole radio ayant pour caractéristiques de fonctionner uniquement à courte distance. C'est précisément ce qui nous intéresse, mais il faut être conscient que le *Bluetooth* n'a pas été conçu pour l'utilisation que nous envisageons aujourd'hui. Par conséquent, le travail de l'ingénieur consiste à transformer le capteur de communication en capteur de mesure de proximité avec d'autres *smartphones*.

Nous avons donc opté pour ce système car il n'y a pas d'autre voie.

Une application de traçage n'aura de sens que si elle est utilisée par nos concitoyens, à charge pour les autorités d'en faire comprendre l'intérêt. Celui-ci est probablement réel, mais il n'est pas facile à expliquer, de sorte qu'une véritable pédagogie sera nécessaire. C'est pourquoi il m'apparaît que ce travail ne devra pas être mené uniquement par des ingénieurs, pour avoir une chance de succès. La confiance sera essentielle, ce qui renforcera la nécessité d'explications. La communication étant un véritable métier, l'équipe projet y travaille d'ores et déjà. Si 10 % seulement des personnes téléchargeaient l'application, le résultat épidémiologique n'aurait pas grand sens. C'est d'ailleurs ce qui s'est produit à Singapour, premier pays qui a lancé une telle expérimentation : le taux d'adhésion volontaire des citoyens n'y a pas dépassé 10 à 15 %. C'était bien trop peu pour obtenir un véritable résultat.

Nous sommes nombreux à considérer que l'utilisation doit reposer sur le volontariat, car la coercition ne serait pas une bonne méthode. En tout état de cause, ce n'est absolument pas la piste ouverte aujourd'hui.

Une fois ceci précisé, comment réaliser une telle application ? Sur quels protocoles s'appuyer ? Quels sont les risques pris ?

L'idée d'une solution parfaitement anonyme qui protégerait l'ensemble des données tout en ne fournissant que l'information signifiante (avoir été en contact avec un cas à risque) n'est pas atteignable. Ce n'est pas une critique contre tel ou tel protocole, mais il faut être conscient qu'aucune solution actuelle ne garantit un anonymat parfait. Pour s'en convaincre, il est possible d'imaginer divers scénarios. Par exemple, une personne confinée chez elle, qui aurait pour tout contact hebdomadaire une aide-ménagère, saurait immédiatement en cas d'alerte de la part du système, que la personne présentant un risque est l'aide-ménagère. Par conséquent, quels que soient le soin apporté au protocole et la qualité de la sécurité numérique, des fuites d'information sont susceptibles de se produire. L'anonymat parfait ne peut être garanti, mais cela signifie-t-il pour autant qu'on ne peut rien faire ? Tel est l'enjeu, qui ne peut relever que du choix politique.

Les seules solutions acceptables sont celles qui conduisent à ne pas publier la liste des malades et à ne pas communiquer d'informations sur le graphe des interactions sociales, afin d'éviter leur utilisation à d'autres fins que celles prévues. Pour pallier toute dérive, l'effort politique reposera sur la maximisation de la protection des libertés, en suivant les recommandations de la Commission nationale informatique et libertés (CNIL), de l'Institut national de recherche en sciences et technologies du numérique (INRIA), du Conseil national du numérique et de l'ANSSI. De même, au niveau européen, une boîte à outils publiée dès le début du processus, pourrait être utile. Si toutes ces recommandations sont suivies, nous pourrons arriver à une solution acceptable. Encore une fois, il ne m'appartient pas d'en décider car il s'agit d'un choix politique.

Si l'on entre dans le détail du fonctionnement, quelles que soient les applications, le schéma de départ est toujours similaire. Il convient tout d'abord d'installer l'application sur le téléphone. Celui-ci commence à émettre des « pseudonymes temporaires ». Ce n'est pas le nom du possesseur du téléphone qui est émis, ni son numéro de téléphone, mais des identifiants non signifiants permettant de faire le lien entre eux et une identité plus fixe. Tous les systèmes fonctionnent ainsi.

Si une personne se déclare malade (étant observé que plusieurs choix de déclaration sont possibles, celle-ci pouvant émaner du porteur lui-même ou d'un médecin), l'idée est de prévenir les personnes avec lesquelles elle a été en contact rapproché suffisamment

longtemps, durant les quatorze jours précédents. Pour ce faire, deux approches se dessinent, dénommées avec des termes qui ne plaisent pas mais qui sont aujourd'hui consacrés : l'approche centralisée et l'approche décentralisée.

La première est l'approche française, choisie par les experts de l'INRIA, qui l'ont jugée être la plus efficace. Concrètement, cela signifie que le smartphone de la personne malade transmet à un serveur central de confiance (en principe piloté par l'autorité de santé) des informations permettant d'alerter les personnes contacts. Dans le cadre centralisé, seront transmis les pseudonymes temporaires des personnes croisées durant les quatorze derniers jours. Le cadre décentralisé met en place la procédure inverse : la personne malade envoie ses propres pseudonymes.

Le choix entre approche centralisée et approche décentralisée est très dimensionnant. Dans le cadre implémenté en France, avec le protocole de l'INRIA dénommé « Robert », le serveur central piloté par l'autorité de santé reçoit les pseudonymes des personnes à risque, dont les téléphones rechercheront régulièrement si une alarme est émise. Le principal défaut de ce système tient à la nécessaire confiance devant entourer le serveur central. En effet, un tel modèle développé dans un État totalitaire pourrait être détourné, pour en faire un outil de traçage des populations.

Néanmoins en France, il peut être vérifié que la construction du serveur central est suffisamment précautionneuse, et que ce serveur ne sera pas détourné pour être utilisé à d'autres fins. De plus, l'ANSSI joue pleinement son rôle pour s'assurer que le serveur est sécurisé au sens informatique du terme. Si toutes les conditions de sécurité et de confiance sont réunies, l'outil ainsi élaboré est assez robuste. Il présente en outre l'avantage de permettre de récolter de l'information anonyme très intéressante à des fins épidémiologiques à grande échelle, pour mieux comprendre comment se propage le virus. L'autre avantage d'une telle approche est de réguler les alertes émises.

Lorsque StopCovid sera utilisé dans une rame de métro, le paramétrage fin de l'application sera intéressant à réaliser. En cela, un modèle centralisé, capable d'être corrigé en permanence en fonction de la réalité, est particulièrement adapté. Je reviendrai plus tard sur les coopérations dont nous aurons besoin avec les géants du numérique que sont Apple et Google, pour parvenir à nos fins.

Dans le strict champ de la sécurité numérique, l'application installée sur les téléphones devra être bien conçue, « propre » et de confiance, c'est-à-dire bien développée et auditée.

Les experts de l'ANSSI travaillent actuellement à auditer le code afin de s'assurer qu'il remplit son usage de façon correcte, et uniquement cet usage. Il faudra aussi publier le contenu de l'application, pour que chacun vérifie – les experts indépendants en particulier – que tout est bien fait. À l'heure où je vous parle, les premiers codes sources de l'application sont en voie de publication par l'INRIA : ils sont rendus librement disponibles sur internet afin que chacun puisse en examiner le contenu. Les experts indépendants, qui sont parfois très critiques sur ce type d'applications, pourront ainsi opérer toutes les vérifications qu'ils souhaitent et éventuellement suggérer des améliorations. C'est la logique même de l'*open source*, qui permet d'associer la communauté des développeurs pour faire progresser les fonctionnalités et le système.

Je souhaiterais également que nous fassions appel à du *bug bounty* (« chasse aux bugs »), ce qui consiste à mobiliser des *hackers* - qui savent attaquer les systèmes pour la bonne cause - pour qu'ils trouvent des failles moyennant récompense. Cette démarche permet de ne pas rester dans l'entre soi des experts étatiques et d'associer la communauté afin de créer de la confiance.

Enfin, tant que l'application sera utilisée, la sécurité devra être suivie. Il s'agira, dès que d'inévitables *bugs* surviendront, de les corriger.

Du côté du serveur central, il conviendra également d'être très transparent et de donner un accès à toutes les personnes souhaitant pratiquer un contrôle.

Dans les systèmes décentralisés, il n'est pas possible de réguler l'émission des alertes ni, en fait, d'être totalement décentralisé. En effet, il est difficile de se passer d'une forme d'autorité qui, à la fin, décidera qui est un cas à risque ou non. Tous les pseudo-identifiants émis seront rendus publics, pour que chacun vérifie s'il a croisé un identifiant à risque. En quelque sorte, nous confions à nos téléphones le choix de faire cette régulation et de prendre la décision médicale et épidémiologique. Or, il ne s'agit pas réellement de nos téléphones, mais de ceux d'Apple et de Google. Je le rappelle sans aucune animosité. Par conséquent, tout choix d'un modèle décentralisé doit être fait en ayant conscience qu'il donne un rôle épidémiologique et médical à Apple et Google, qui s'y préparent. Ainsi, les prochaines versions de leurs systèmes d'exploitation intègreront des capacités de traçage de contacts à risque.

La France a fait le choix de ne pas emprunter cette voie, car l'État doit rester à la manœuvre, et ne pas mettre ce sujet dans les mains des géants numériques extra-européens. Nous n'avons pas de défiance *a priori*, mais considérons que ce serait un vrai risque d'abandonner notre souveraineté.

En définitive, savons-nous faire une telle application ? A-t-elle une chance d'aboutir ? Sur les téléphones équipés d'Android, nous sommes assez confiants sur le fait que l'application fonctionnera car l'accès au *Bluetooth* est aisé. En revanche, tel n'est pas le cas avec l'iPhone. Pour de très bonnes raisons de sécurité, Apple produit des solutions volontairement fermées, qu'il est difficile d'utiliser sans son autorisation. J'insiste sur le fait que si Apple empêche toute utilisation de ses solutions, c'est pour de bonnes raisons. Toutefois, sans la coopération d'Apple ou, pire, face à son opposition, l'application StopCovid ne fonctionnera pas. Plus prosaïquement, si Apple ne souhaite pas référencer l'application dans son Store, il lui sera loisible de nous opposer un refus.

Quoi qu'il en soit, nous sommes convaincus qu'il était important de passer par une approche centralisée, pour ne pas laisser Apple et Google mener le travail à notre place. À l'inverse, dans le modèle décentralisé, Apple et Google seraient en première ligne pour maîtriser l'intégralité du dispositif.

La France a toujours été claire sur ses principes, mais dans d'autres pays européens l'attitude est différente. Certains considèrent depuis le début qu'il faut laisser agir Apple et Google, qui sont déjà présents dans des champs multiples. D'autres ont changé d'avis, à l'instar de l'Allemagne. En revanche, comme nous, les Britanniques sont en passe de retenir une approche centralisée. Tous les choix ne sont pas encore tranchés à l'échelle européenne, mais nous souhaiterions que toutes les applications soient compatibles pour être capables de fonctionner ensemble. Dans un déconfinement plus avancé, où la circulation en Europe serait

rétablie, il serait intéressant en effet de repérer les contacts, même entre personnes de nationalités différentes.

Je termine en insistant sur la notion de souveraineté. Je suis inquiet, en tant que citoyen, de voir les géants du numérique avancer sur les sujets de santé. Ils savent ce que nous mangeons, ce que nous lisons, ils connaissent notre sommeil… Si nous leur confions demain des sujets de santé, des conflits d'intérêt vont apparaître. Que se passerait-il si Apple décidait demain d'être présent dans le domaine de l'assurance-santé ? Cet acteur sait tout de nous. Apple pourrait prendre le parti d'assurer uniquement les personnes en bonne santé, et refuser d'assurer les autres. Dans ce modèle, l'ensemble du système mutualiste serait mis à mal. Il faut conserver ce sujet en tête, même s'il nous écarte de StopCovid. Nous sommes nombreux à être inquiets et à nous méfier. L'État doit rester un acteur de confiance, comme c'est le cas en France. Les acteurs du numérique américains, même s'ils ont une bonne image, ne doivent pas remplacer l'État.

M. Cédric Villani, député, premier vice-président de l'Office. – On pourrait imaginer qu'une nuance soit introduite par un recours au GPS, sans que l'information de localisation absolue soit conservée. Cela pourrait-il fonctionner ? Est-ce trop sensible par rapport à la question des libertés publiques ?

M. Guillaume Poupard. – Si l'on pousse la logique du traçage à l'extrême, plus les informations recueillies seront nombreuses, plus les épidémiologistes auront de facilité à retracer les cas contacts. L'enjeu de StopCovid est de savoir jusqu'où aller. Nous pourrions aller plus loin avec le GPS, mais les données personnelles ne seraient plus protégées, ce qui pourrait aboutir à de graves conséquences. De ce fait, alors qu'il serait difficile d'expliquer son intérêt aux utilisateurs, l'utilisation du GPS serait trop risquée car elle montrerait un rapport coût-bénéfice peu favorable.

Le cas d'usage sur lequel nous devons réfléchir est celui de la rame de métro. Si une personne se trouve malade, l'enquête épidémiologique conduite au bureau, chez elle ou dans un cercle amical permettra de déterminer l'ensemble de ses contacts mis en risque. En revanche dans le métro, l'identification des contacts est impossible, et le GPS apparaît inutile. C'est la raison pour laquelle le Premier ministre a cité cet exemple.

La solution la plus appropriée réside donc dans un *Bluetooth* bien calibré.

M. Cédric Villani, député, premier vice-président de l'Office. – Les dénominations « système centralisé » et « système décentralisé » sont malheureuses mais correspondent à l'usage désormais établi. Dans l'état de développement actuel, quel système peut être considéré comme plus sûr que l'autre, et par rapport à quel type d'attaque raisonnable ?

M. Guillaume Poupard. – La solution centralisée nécessite que le serveur centralisateur soit absolument digne de confiance. Pour cela, il ne doit pas être attaqué et il doit être bien protégé. Le grand avantage de cette approche est de réduire le périmètre à sécuriser. Cependant, nous ne prétendons pas qu'il n'y a aucun risque. C'est pourquoi l'ANSSI sera extrêmement vigilante et veillera à ce que le serveur soit très bien protégé, à l'instar d'autres systèmes sensibles. Dans une version dite décentralisée, il y a une couche d'opacité non maîtrisée, c'est-à-dire en substance les fonctionnalités directement implémentées par Apple et Google. De surcroît, tous les risques apparaîtront lorsque les téléphones seront attaqués. En d'autres termes, l'ANSSI prétend être capable de sécuriser un

serveur, mais elle n'est nullement en mesure de faire de même avec les téléphones de nos concitoyens – ce n'est pas non plus dans nos missions.

Nous savons que le serveur centralisé sera une cible pour les attaquants de haut niveau qui voudront accéder aux informations stockées, ainsi que pour tous ceux qui entendront créer la confusion. Pour autant, nous sommes en mesure de nous y préparer, car c'est partie intégrante de notre métier.

L'INRIA étudie actuellement une troisième voie qui combinerait les avantages du centralisé et du décentralisé. Il s'agirait d'éviter d'accorder une trop grande confiance au serveur central, tout en bénéficiant des capacités de régulation et d'usage épidémiologique permises par la solution centralisée. Ces travaux ne sont pas encore achevés, mais ils ouvrent une piste intéressante autour d'un protocole dénommé « Désiré », qui pourrait s'avérer fédérateur. Si le protocole « Robert » était implémenté par un pays totalitaire, on pourrait comprendre qu'Apple et Google refusent de coopérer. En France, bien évidemment nous ne sommes pas dans cette situation. Il est cependant concevable qu'Apple et Google ne souhaitent pas jouer les arbitres entre les pays totalitaires et ceux qui ne le sont pas. L'avantage du protocole « Désiré » est qu'il évite le risque de détournement par des pays totalitaires, de sorte qu'il n'aurait pas de raison d'être refusé par Apple et Google, sauf s'ils avaient des arrière-pensées.

Tel est l'état actuel de la réflexion. Cette piste est intéressante mais ne sera pas implémentée dans StopCovid, qui sortira le 2 juin prochain. Elle pourrait fonder une évolution intéressante de ce type d'application si elle permettait d'obtenir davantage de coopération de la part d'Apple et Google.

M. Patrick Hetzel, député. – Merci pour ces informations très claires. Ma première question concerne l'orientation prise par l'Allemagne. Manifestement dans un premier temps, ce pays avait décidé de se diriger vers une formule décentralisée, laissant le champ libre à Google et Apple. Aujourd'hui, il semble revenir en arrière. Pouvez-vous nous en dire quelques mots ?

Par ailleurs, vous évoquez cette troisième voie, dite « Désiré ». A-t-on une visibilité sur l'arrivée potentielle de cette solution, d'un point de vue technique ?

M. Guillaume Poupard. – Initialement, les Allemands se sont dirigés vers une approche centralisée, similaire à celle de l'INRIA et coordonnée avec les experts de cet organisme. Par la suite, une campagne médiatique pas toujours honnête a opposé les tenants de la centralisation à ceux de la décentralisation. Sans que l'on sache précisément qui était à l'origine de cette campagne, on imagine bien à qui elle a pu bénéficier, d'autant qu'elle a tiré parti d'une certaine forme de confusion dans la communauté scientifique. Dans ce contexte, l'Allemagne a alors souhaité promouvoir un système décentralisé. Cependant, les Allemands se rendent compte peu à peu des désavantages d'un tel système en termes d'efficacité et de perte de souveraineté vis-à-vis de Google et Apple. Aujourd'hui, nul n'est capable de prévoir quelle sera la solution définitivement adoptée en Allemagne. Un autre avantage de « Désiré» est qu'il permettrait à tout le monde de sortir de ce débat par le haut.

Cela étant, le 2 juin, c'est bien le protocole « Robert » qui sera implémenté, et non « Désiré ». Une pression maximale repose sur les équipes de l'INRIA et les équipes de développement – qui incluent d'ailleurs des équipes de sociétés privées. Les personnes qui travaillent sur cet ensemble sont de haute qualité. La pire des décisions serait de développer

trop rapidement une solution inaboutie, qui occasionnerait de vrais problèmes de sécurité, ou pourrait même ne pas fonctionner. « Désiré » est une belle idée, mais il faut s'assurer techniquement de son caractère implémentable et de sa sécurité d'ensemble.

Finalement, il m'apparaît nécessaire de conserver à court terme le protocole « Robert », tout en gardant une vigilance sur « Désiré ». S'il est ensuite possible d'embarquer les autres pays européens tout en bénéficiant d'une meilleure coopération d'Apple et Google, nous aurons atteint notre objectif. J'insiste sur le fait qu'une décision politique consistant à nous mettre la pression pour implémenter « Désiré » le 2 juin serait une erreur.

M. Jean-François Eliaou, député. – Je ne suis pas informaticien mais médecin et député. Je suis préoccupé, actuellement, par la une éventuelle reprise de l'épidémie. Le Parlement a voté ce week-end – cela n'a pas été simple – une loi dérogeant à deux grands principes : le secret médical et le consentement des personnes à communiquer des informations personnelles. La décision du Conseil constitutionnel rendue hier montre bien que nous nous situons sur une ligne de crête entre le droit à la santé, consacré également par la Constitution, et ces droits tout aussi constitutionnels (la liberté d'aller et venir, la liberté d'entreprendre…) mis entre parenthèses pendant l'état d'urgence sanitaire.

Nous avons besoin d'outils efficaces qui vont dans le prolongement de la loi votée par le Parlement. Tel est pour moi, le cahier des charges. Je vois assez mal la différence, en termes de *design*, entre un système centralisé et un système décentralisé. En revanche, je tiens absolument à ce que la déclaration de lac maladie soit effectuée par un professionnel de santé. C'est fondamental : seul le médecin doit être en mesure de déclencher le dispositif. Dans le métro, l'efficacité de l'outil StopCovid paraît avérée, même si au départ j'y étais opposé car il existe des zones en France qui souffrent de la fracture numérique. Or ce ne seront pas ces zones qui auront la principale utilité de l'application, mais bel et bien les zones très denses et disposant d'un réseau de transports en commun important.

Dans ce cadre, le système devra-t-il être centralisé ou décentralisé, sachant que lorsque la France sortira de l'état d'urgence sanitaire, toutes les informations recueillies devront être effacées car c'est la condition même de la confiance ?

En second lieu, comment peut-on calibrer de façon quantitative une interaction *Bluetooth* entre deux appareils qui ne sont pas de la même génération ? Quelles capacités aura StopCovid au mois de juin ?

M. Guillaume Poupard. – Nous sommes entièrement d'accord sur le fait que nous nous trouvons sur une ligne de crête. Il s'agit de véritables mesures d'exception, que nous ne prendrions jamais dans un contexte normal. C'est pourquoi la démarche n'est pas anodine et le traçage automatique ne doit servir qu'à cela. J'attire constamment l'attention là-dessus. Il ne faudrait pas que cette nouvelle fonctionnalité mesurant qui est en contact avec qui, se généralise et crée de nouveaux usages. Avec un tel capteur, un écosystème entier pourrait se monter, alors même que la détermination des interactions sociales n'est en rien anodine. C'est pourquoi il est indispensable que l'outil soit conçu exclusivement à des fins sanitaires. La confiance dans le système passe par là. La responsabilité de l'État – et la vôtre – est d'y veiller. Nous sommes donc sur cette ligne de crête, ce qui explique l'investissement aussi fort de l'ANSSI dans l'équipe projet.

M. Cédric Villani, député, premier vice-président de l'Office. – Il n'est pas anodin que l'ANSSI participe au développement de StopCovid.

M. Guillaume Poupard. – Il est de notre devoir de participer à ce développement car l'équipe projet, à la fois portée politiquement et confiée à des chercheurs, est sérieuse et ne présente aucun risque de dérive commerciale. L'intérêt des acteurs est de promouvoir le projet le plus sérieux et protecteur.

Sur les aspects techniques, qui posaient au début de réelles difficultés, une partie des équipes a été mobilisée car elles connaissent bien la technologie *Bluetooth*. Les équipes allemandes y ont également travaillé. Nous avons réfléchi aux possibilités d'utiliser ce signal radio pour en faire un capteur fiable de distance, ce qui n'était pas évident au départ. Les experts ont réussi à établir des abaques qui tiennent compte du type de téléphone et du système. Quand le modèle de téléphone est croisé avec la puissance du signal perçu, les abaques fournissent la distance qui sépare les deux smartphones de manière précise. Je n'entrerai pas davantage dans le détail. Sur cette partie, nous sommes confiants dans le fait que le fonctionnement est acquis, à la condition importante d'avoir accès au capteur *Bluetooth*. Sur Android, l'accès est relativement ouvert, ce qui n'est pas le cas des téléphones Apple. Il faut donc que cette société nous y autorise. Une telle autorisation n'est en rien compliquée à délivrer, mais cela ne fait pas partie de la politique habituelle d'Apple.

M. Cédric Villani, député, premier vice-président de l'Office. – J'ai vu que les deux camps (centralisé et décentralisé) s'accusaient mutuellement d'opacité. Une pétition circule même pour demander la publication du code source de la solution centralisée. Ceci va-t-il être fait rapidement ?

M. Guillaume Poupard. – La publication du code source est une démarche normale, qui ne doit pas résulter d'une pétition. Nous l'avons envisagée dès le départ du projet car nous n'avons rien à cacher. De plus, nos experts sont très sérieux mais pourraient ne pas voir toutes les erreurs possibles. Nous devons donc mettre toutes les chances de notre côté en bénéficiant du regard d'autres experts, qui d'une certaine façon participeront ainsi au projet.

Le paradoxe est que la publication de ces éléments ne pose aucune difficulté dans le cadre d'une solution centralisée, car ils ont trait uniquement du fonctionnement du moteur et non à son contenu. Je serais très surpris, en revanche, que les tenants de solutions décentralisées s'appuyant sur l'interface de Google et Apple, puissent publier leur code.

En définitive, la solution centralisée telle que nous la concevons en France sera plus « auditable » que la solution décentralisée.

M. Cédric Villani, député, premier vice-président de l'Office. – Finalement, si avec le meilleur protocole du monde Apple refusait de coopérer, il n'y aurait aucun moyen de proposer une application qui fonctionne.

M. Guillaume Poupard. – Je précise que la publication des codes source a débuté il y a environ une heure.

Si Apple refuse de coopérer, et même refuse que l'application soit publiée dans son Store, nous devrons nous rabattre sur les seuls téléphones Android, pour un fonctionnement moins optimal. Par conséquent l'objectif n'est pas de nous passer d'Apple.

Par ailleurs, il existe plusieurs niveaux de coopération possibles avec Apple. Si cette société ne nous aide pas à utiliser *Bluetooth* mais que nous sommes autorisés à installer l'application sur le téléphone, nous pourrons malgré tout identifier un grand nombre de cas

contacts. L'idéal est néanmoins d'aboutir à une coopération totale, en garantissant à Apple qu'il ne prendra pas de risque. En cela, « Désiré » pourrait représenter une garantie sérieuse puisque ce protocole n'est pas détournable. Cette solution présenterait le mérite de permettre à chacun de sortir par le haut.

M. Cédric Villani, député, premier vice-président de l'Office. – Merci beaucoup pour cette audition. Nous ne manquerons pas de revenir vers vous.

La visoconférence est close à 18 h 10.