A S S E M B L É E N A T I O N A L E

X V^e L É G I S L A T U R E

Compte rendu

Commission des lois constitutionnelles, de la législation et de l'administration générale de la République

Mercredi
8 avril 2020
Séance de 10 heures

Compte rendu n° 51

SESSION ORDINAIRE DE **2019-2020**

Présidence de Mme Yaël Braun-Pivet, *présidente*

ASSEMBLÉE NATIONALE

La réunion débute à 10 heures 05.

Présidence de Mme Yaël Braun-Pivet, présidente.

La Commission auditionne, en visioconférence, Mme Marie-Laure Denis, Présidente de la Commission nationale de l'informatique et des libertés (CNIL), M. Jean Lessi, Secrétaire général, et M. Gwendal Le Grand, Secrétaire général adjoint.

Mme la présidente Yaël Braun-Pivet. Mes chers collègues, nous allons d'abord auditionner, ce matin, Mme Marie-Laure Denis, présidente de la Commission nationale de l'informatique et des libertés (CNIL). MM. Jean Lessi, secrétaire général de la CNIL, et Gwendal Le Grand, secrétaire général adjoint, pourront également intervenir.

Cette réunion s'inscrit dans le prolongement des décisions prises par le bureau de la Commission jeudi dernier, au lendemain de la constitution de la mission d'information mise en place par la Conférence des Présidents sur « l'impact, la gestion et les conséquences dans toutes ses dimensions de l'épidémie de Coronavirus ».

La commission des Lois a été « en première ligne » lors du vote des deux lois dites d'urgence pour lutter contre le coronavirus. Nous travaillerons désormais en visioconférence compte-tenu de la situation sanitaire dramatique qui prévaut dans notre pays. Un relevé de nos échanges sera publié sur la page de la commission. Par ailleurs, à partir de la semaine prochaine, la Conférence des Présidents a décidé que les auditions organisées par les commissions en visioconférence seraient rendues publiques et diffusées sur le site de l'Assemblée nationale.

Le bureau a défini des axes de travail. Nous allons aujourd'hui et demain nous pencher sur des questions qui ont trait à l'utilisation des nouvelles technologies en matière épidémiologique.

Face à la crise sanitaire actuelle et dans la perspective du déconfinement, faut-il recourir à des techniques d'identification de ceux qui ont été au contact de personnes infectées ? Il s'agit d'un enjeu sanitaire majeur, mais également d'un enjeu de libertés publiques et ces sujets sont au cœur des travaux de la commission des Lois. M. Simon Cauchemez, responsable de l'unité de modélisation mathématique des maladies infectieuses à l'Institut Pasteur, nous exposera tout à l'heure très concrètement l'intérêt, sur le plan sanitaire, que pourraient présenter ces nouvelles technologies. Demain, nous auditionnerons 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.

Dans ce contexte, je vais demander à nos invités de dresser le panorama des initiatives étrangères en la matière et de nous faire part de leur analyse. Que permet la législation nationale et européenne ? Que pourrait-il être utile de prévoir ? M. Jean Lessi va commencer en attendant que la présidente de la CNIL soit en mesure de nous rejoindre.

M. Jean Lessi, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL). La protection des données personnelles, durant cette période très particulière, se décline au regard de deux séries d'enjeux.

Premièrement, la continuité des différentes activités suppose une consommation massive de données personnelles – télémédecine, télétravail, cours à la distance, etc. La CNIL, conformément à son rôle, publie régulièrement des conseils pratiques et des

recommandations juridiques pour renforcer notamment la cybersécurité dans l'usage de la visioconférence, du télétravail ou d'autres solutions d'échanges à distance.

Deuxièmement, les données personnelles sont une ressource pour répondre au défi sanitaire : recherche en santé, protection des personnes vulnérables, accompagnement des stratégies de confinement ou de déconfinement en localisant la personne ou en retraçant ses interactions. La CNIL s'est mobilisée pour accompagner les pouvoirs publics, mais aussi les organismes publics. Nous avons publié des contenus pour faciliter l'instruction des projets de recherche en santé liés au Covid-19, et les avons instruits en priorité. Depuis le début de la crise, une dizaine d'autorisations ont été délivrées à des acteurs comme l'Assistance publique-Hôpitaux de Paris (AP-HP), l'Institut national de la santé et de la recherche médicale (INSERM), l'institut Pasteur ou le centre hospitalier universitaire de Lille.

C'est dans ce contexte que se pose la question de l'utilisation des outils capables de localiser la personne ou de retracer son exposition au Covid-19. La CNIL, et notamment sa présidente, entend mettre en avant deux convictions fortes.

Premièrement, le cadre légal et réglementaire protégeant les données personnelles – le règlement général sur la protection des données (RGPD) et la directive sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite *e-privacy* – ne s'oppose pas à la mise en œuvre de solutions de suivi pour des motifs de protection de la santé : il impose seulement de prévoir des garanties d'autant plus adaptées que les technologies sont intrusives. Du fait de l'urgence, on peut avoir la tentation de s'affranchir de ce cadre, alors qu'il comporte déjà en lui-même les solutions propres à répondre à une situation exceptionnelle. Je laisse la présidente, qui nous a rejoints, poursuivre.

Mme Marie-Laure Denis, présidente de la CNIL. La deuxième conviction sur laquelle je souhaiterais insister est qu'il faut se garder de penser qu'une application va tout résoudre, quand bien même les nouvelles technologies peuvent contribuer à une sortie sécurisée du confinement dans le cadre d'une stratégie globale. J'appelle régulièrement à la vigilance contre la tentation du « solutionnisme technologique ». Il faut explorer les opportunités technologiques, mais aussi leurs limites et leurs risques pour les droits des personnes. Si elles peuvent être d'un grand secours dans la gestion de la crise sanitaire, faute de recul suffisant, il est encore difficile d'évaluer leurs bénéfices effectifs, d'autant plus que les usages peuvent varier selon le type de données collectées et les finalités poursuivies.

Dans cette optique, la CNIL a le souci de s'entourer d'une double expertise : la première – notre cœur de métier – consiste à se donner les moyens de connaître et de comprendre, d'un point de vue technique, l'ensemble des dispositifs utilisés, des projets envisagés, des solutions imaginées dans le monde pour lutter contre la pandémie. Nos ingénieurs, nos juristes, nos autres experts, au contact des acteurs de la société civile, en lien avec nos homologues européens, assurent une veille continue depuis la mi-mars.

La seconde expertise peut paraître moins naturelle, mais elle est également utile : c'est la compréhension de l'intérêt des solutions envisagées pour la santé publique, afin de mesurer la légitimité, la proportionnalité et la pertinence des traitements de données. Nous avons auditionné à ce propos le professeur Jean-François Delfraissy, président du conseil scientifique Covid-19, la semaine dernière.

Les technologies utilisées à l'étranger dans la lutte contre la pandémie sont multiples : caméras thermiques, reconnaissance faciale, utilisation de drones diffusant des messages aux personnes ne respectant pas le confinement, collecte d'informations sur les réseaux sociaux, localisation par le biais des téléphones portables et des applications de suivi des contacts, dites de *contact tracing*. Je concentrerai mon propos sur ces dernières technologies, qui reposent sur l'analyse des données de localisation des individus par rapport à des personnes déjà exposées, à leur domicile, à des périmètres de confinement, *etc*.

Les États ont recours aux données de géolocalisation pour trois séries de finalité : cartographier, contrôler, informer. Il s'agit d'abord de cartographier la propagation du virus, de prédire les prochaines zones à risque ou encore de planifier les prochains besoins médicaux urgents.

Il s'agit ensuite de faire respecter les mesures prises pour endiguer la propagation du virus – consignes de distanciation sociale ou obligation de confinement.

Enfin, certains pays utilisent ou ont l'intention d'utiliser, les données à des fins de *contact tracing* pour réaliser le suivi des contacts des personnes potentiellement exposées afin de les avertir et, éventuellement, de les inviter à se faire dépister. Certains vont même jusqu'à recouper les données de localisation avec des données provenant des tests et des diagnostics ou encore des services des douanes ou de l'immigration.

Deux séries de techniques sont utilisées : la localisation individuelle et la localisation collective. La première est utilisée principalement au Moyen-Orient et en Asie, mais aussi en Europe. Ces dispositifs peuvent être imposés aux citoyens ou reposer sur le volontariat. En Israël, un système basé sur les données de localisation des téléphones mobiles détecte les personnes potentiellement exposées et leur envoie un SMS pour leur demander de se mettre en quarantaine. En Chine, les opérateurs de téléphonie mobile ont partagé les données de localisation avec plusieurs agences gouvernementales afin de reconstituer les mouvements des porteurs potentiels du virus, ainsi que ceux des personnes susceptibles d'avoir été en contact avec eux. En Corée du Sud, le gouvernement a ordonné aux personnes en quarantaine d'installer une application pour vérifier le respect du confinement. Des données de localisation détenues par l'opérateur de télécommunications ont également été utilisées pour identifier les personnes exposées. Le résultat est exploité par les autorités, mais aussi par des sites internet gérés par l'État : cela permet notamment aux citoyens d'être informés des nouveaux cas locaux et d'éviter les endroits où le virus est ou était actif.

D'autres dispositifs sont fondés sur le volontariat : à Singapour, une application reposant sur la technologie *Bluetooth* vise à identifier les personnes potentiellement exposées qui doivent être testées. La Pologne utilise une application combinant géolocalisation et reconnaissance faciale afin de faciliter la vérification du respect des obligations de confinement des personnes soumises à une quarantaine obligatoire à leur retour d'un voyage à l'étranger.

Les techniques de localisation collective, par le recours aux données de localisation agrégées, sont quant à elles utilisées dans de nombreux pays européens. En Italie, en Autriche et en Allemagne, plusieurs opérateurs de télécommunications ont déclaré avoir fourni des données anonymisées afin de surveiller les déplacements des personnes et de s'assurer du respect du confinement. En Belgique, le ministre de la santé publique a autorisé les opérateurs de télécommunications à transmettre des cartes de mobilité basées sur des données anonymisées et des agrégats géographiques – comme le code postal. Croisées avec les

données épidémiologiques des autorités, ces données sont censées aider à prédire la propagation du virus.

En liaison avec les opérateurs de télécommunications, le gouvernement britannique analyse les données de localisation anonymisées pour vérifier si la population respecte ses directives de distanciation sociale et les nouvelles restrictions de transport. Aux États-Unis, le gouvernement serait en pourparlers actifs avec Facebook, Google et d'autres entreprises technologiques et experts en santé sur l'utilisation des données de localisation agrégées pour suivre la propagation du virus.

En outre, plusieurs applications de suivi de contacts sont en cours de développement, notamment *Waze for Covid-19* de l'Organisation mondiale de la santé (OMS) ou *Safe Path* développée par une équipe de chercheurs du Massachusetts institute of technology (MIT) et de Harvard. En France, Orange a annoncé partager des données de localisation anonymisées avec plusieurs partenaires, dont l'INSERM, afin que les épidémiologistes modélisent la propagation de la maladie. L'opérateur a précisé que ces données pourraient également être utilisées pour mesurer l'efficacité des mesures de confinement.

Pour ce qui est du cadre juridique, deux textes réglementent l'usage des données de localisation des résidents européens : la directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques (2002/58), dite *e-privacy*, et le règlement général sur la protection des données.

Il découle des articles 5 et 9 de la directive *e-privacy* que, sauf anonymisation, le traitement des données de localisation est soumis au consentement des personnes concernées. Il n'est possible de déroger à ce principe que par des « mesures législatives », et uniquement dans certaines hypothèses limitativement énumérées à l'article 15, notamment la « sécurité publique » entendue au sens large. En France, compte tenu de l'impact d'un tel dispositif et de l'article 34 de notre Constitution, le vote d'une loi serait sans doute nécessaire.

Le RGPD, applicable aux autres techniques de localisation, comme le *contact tracing*, offre un cadre juridique plus souple, mais exigeant, lorsque les données de localisation ne sont pas traitées de manière anonymisée. Trois exigences en découlent. Pour commencer, tout traitement de données doit avoir une base légale. Ensuite, le traitement des données de santé est en principe interdit, sauf exceptions précisément listées : consentement de la personne, nécessités liées à sa prise en charge sanitaire, intérêt public dans le domaine de la santé publique, protection des intérêts vitaux de la personne concernée, recherche et suivi d'une épidémie et de sa propagation. Enfin, même lorsqu'ils ont des raisons légitimes de limiter certains droits, les États doivent respecter les principes de proportionnalité et de sécurité.

Au regard de ce double cadre juridique, et au-delà de la nécessité de disposer d'un fondement juridique adéquat, le traitement des données de localisation devrait respecter les principes suivants.

Premièrement, les finalités du dispositif doivent être définies et limitées.

Deuxièmement, le traitement des données de localisation doit être adéquat, nécessaire et proportionné. L'instrument doit apparaître réellement utile et non relever d'une solution de confort. Les dispositifs les moins intrusifs – le recours à des données anonymisées, par exemple – doivent toujours être privilégiés. Ils doivent également avoir un

caractère temporaire : les données devront être détruites sitôt la crise terminée ou à tout le moins n'être conservées, durant un temps limité et de façon protégée, que pour servir des finalités complémentaires – recherche ou gestion de contentieux, par exemple.

Troisièmement, les données traitées doivent être limitées à ce qui est nécessaire, dans un objectif de « minimisation » des données collectées : certaines applications de suivi-contact ne traitent pas d'informations nominatives, mais associent les données par le biais d'un identifiant unique créé lors de l'installation de l'application.

Par ailleurs, le dispositif doit être conçu de manière à permettre aux utilisateurs d'avoir la maîtrise de leurs données. En l'état du droit, le suivi devrait se faire sur la base du volontariat des personnes concernées. Encore faut-il que le consentement soit valide au sens du RGPD, c'est-à-dire qu'il doit être éclairé, autrement dit précédé d'une information précise, spécifique à la finalité, univoque et libre : le refus de consentir ne doit donc pas exposer la personne à des conséquences, quelles qu'elles soient. J'y insiste car les comparaisons internationales montrent que le volontariat a parfois pour contrepartie une limitation des libertés. À défaut de réel consentement, une loi comportant d'importantes garanties serait nécessaire.

Il convient également de privilégier un stockage des données « en local », autrement dit sur le terminal de l'utilisateur. Les applications s'appuyant sur des données *Bluetooth* offrent à cet égard davantage de garanties que les systèmes de suivi par GPS.

Enfin, le dispositif devra respecter le principe de transparence, assurer la sécurité des données et respecter le droit des personnes : les citoyens doivent savoir quelles données sont susceptibles d'être traitées, par qui, dans quel but, à quelles conditions et avec qui ces données peuvent être partagées.

En somme, à droit constant, un suivi individualisé des personnes devrait être fondé sur le volontariat et s'appliquer pendant une durée limitée. Si un dispositif obligatoire était mis en place, il devrait faire l'objet d'une disposition législative et devrait, en tout état de cause, démontrer sa nécessité et sa proportionnalité, et rester provisoire. Mais j'observe qu'à ce jour, les pouvoirs publics ont exclu le recours à un tel dispositif.

Au niveau européen, à nos yeux le plus pertinent en termes de réflexion, voire de réaction, les différentes autorités nationales de protection des données travaillent en réseau au sein du Comité européen de la protection des données, lequel s'est fixé pour priorité l'élaboration d'orientations sur trois thématiques principales : l'utilisation des données de localisation et leur anonymisation ; le traitement des données de santé à des fins scientifiques et de recherche ; le traitement des données par les technologies utilisées dans le cadre du télétravail.

Le collège de la CNIL est conscient de l'urgence de conjuguer efficacité sanitaire et respect des libertés fondamentales dans les réponses à apporter à cette crise sanitaire sans précédent. À droit constant, un dispositif numérique de suivi individualisé des personnes peut être créé, mais il ne saurait être qu'un des éléments d'une réponse sanitaire plus globale et à condition d'être assorti de garanties particulièrement fortes en ce qui concerne la protection des données personnelles de ses utilisateurs. Il faut en effet gagner la confiance de nos concitoyens pour qu'ils adoptent un tel dispositif de façon suffisamment massive pour en assurer l'efficacité sanitaire. Si un tel dispositif devait voir le jour, la CNIL remplirait ses missions d'accompagnement et de contrôle.

Mme la présidente Yaël Braun-Pivet. Je vous remercie pour cet exposé très clair. Je donne maintenant la parole aux nombreux députés qui souhaitent vous interroger.

M. Philippe Gosselin. Vos explications sont conformes à la jurisprudence habituelle de la CNIL. Ne craignez-vous pas qu'après avoir autorisé, même sur la base du volontariat, l'utilisation généralisée du traçage, la tentation soit forte de mettre le pied dans la porte et d'aller au-delà ? Ne risque-t-on pas d'ouvrir ainsi « la boîte de Pandore » ?

Mme Marietta Karamanli. La CNIL est-elle informée des recherches menées par différents organismes non commerciaux européens ? Avez-vous pu examiner le système proposé par plusieurs instituts de recherche universitaires et qui consiste dans un traçage numérique décentralisé utilisant la technologie *Bluetooth* et un système d'identification éphémère ? Je partage l'inquiétude exprimée par Philippe Gosselin.

Mme Laurence Vichnievsky. Je partage également cette inquiétude. La garde des sceaux devrait être associée au pilotage des travaux sur le dispositif de traçage des données mobiles des personnes contaminées ; or, d'après ce que nous a indiqué le ministre de l'Intérieur, cela ne semble pas être le cas jusqu'à présent. Dans l'hypothèse où un tel dispositif serait appliqué sur la base du volontariat, quelles procédures permettraient de s'assurer que les intéressés ont exprimé un consentement libre et éclairé ?

M. Jean-Michel Mis. La loi sur le renseignement de 2015 autorise la collecte de données de géolocalisation dans certains cas, notamment pour assurer la défense des intérêts économiques de la France. Quelle est votre analyse des éléments de souveraineté qui seraient attachés aux solutions technologiques envisagées dans le cadre de la lutte contre la pandémie ? Comment s'assurer que ces outils seront nécessaires et proportionnés à l'objectif recherché ? Que préconisez-vous contre les risques de banalisation et de pérennisation de telles techniques de surveillance ?

Mme Marie-Laure Denis. Le point soulevé par M. Philippe Gosselin est très important. De fait, on a vu, à propos de l'état d'urgence, par exemple, que la tentation pouvait exister de reconduire des mesures exceptionnelles ou de les intégrer dans le droit commun : cela s'est produit dans certains pays. Nous devons tous être conscients de ce risque et veiller au contrôle du caractère exceptionnel d'un éventuel dispositif de traçage, dont je rappelle qu'il doit être nécessaire et proportionné. Le cadre juridique est, certes, souple, mais il est protecteur. Ainsi, il faudrait prévoir que le dispositif s'autodétruise à l'échéance prévue.

Par ailleurs, la CNIL a des contacts très étroits avec le milieu de la recherche européenne et avec des porteurs de dispositifs de suivi de personnes : nous nous efforçons à chaque fois d'intervenir en amont et nous sommes très impliqués auprès des instituts de recherche publique français, mais également allemands. Quant à la technologie *Bluetooth*, c'est celle qui nous semble offrir le plus de garanties, sous réserve d'une analyse minutieuse de l'architecture retenue.

M. Gwendal Legrand, secrétaire général adjoint de la CNIL. Le grand avantage du *Bluetooth* tient au fait qu'il ne nécessite pas forcément une géolocalisation précise des utilisateurs de l'application. Cette technologie est donc plus protectrice de la vie privée. Encore faut-il qu'elle ait une réelle utilité sur le plan sanitaire.

Mme Marie-Laure Denis. Pour s'assurer que les personnes ont bien donné un consentement libre et éclairé à l'utilisation de l'application, il faut d'abord veiller à ce qu'elles

soient informées, avant l'installation de l'application, de la finalité du dispositif – s'agit-il de les informer ou de contrôler le respect du confinement ? –, des données collectées, de l'utilisation de ces dernières, etc. Toutefois, cette information ne doit pas être trop abondante au risque d'avoir un effet dissuasif, ou à l'inverse d'amener l'utilisateur à donner son consentement sans en avoir cerné tous les enjeux et toutes les implications : le consentement doit en tout état de cause rester un acte positif. Au-delà du respect du droit, c'est une question de confiance dans l'utilisation des données que l'on communique.

Enfin, le dispositif de la loi sur le renseignement n'est pas mobilisable dans le cadre d'une crise sanitaire. En tout état de cause, nous devons attacher la plus grande importance à la sécurité du traitement de ces données sensibles. À cet égard, le fait d'élaborer, le cas échéant, une réponse partiellement ou entièrement européenne contribue, au-delà du symbole, à manifester la volonté de prendre en compte les enjeux de souveraineté en matière de protection des données.

M. Jean-François Eliaou. Pour l'instant, l'éventuel traçage envisagé ne pourrait se faire que sur la base du volontariat. Mais celui-ci n'est pas sans présenter plusieurs biais. Premièrement, on peut se demander si le dispositif sera réellement utile dès lors qu'une partie seulement de nos concitoyens se portent volontaires. Cela pose également un problème d'inégalité entre les citoyens, selon qu'ils y aient accès ou pas. Sans oublier enfin un possible effet de stigmatisation : ceux qui refuseraient de donner leur consentement pourraient se voir considérés comme de mauvais citoyens et accusés de ne pas participer à l'effort national.

M. Arnaud Viala. L'application signalera-t-elle immédiatement à un utilisateur que la personne qu'il croise est potentiellement contagieuse, ou bien la notification sera-t-elle différée ? Si la première option était retenue, cela risquerait de susciter des réactions de nature à dissuader les Français de télécharger l'application.

M. Stéphane Peu. J'ai moi aussi des doutes quant au caractère provisoire de la mesure : l'expérience nous montre, hélas, que les dispositions d'exception ont tendance à devenir pérennes dans notre droit. Par ailleurs, en pleine épidémie, et alors que la part de l'irrationnel est très importante, la pression sociale risque de rendre la notion de volontariat illusoire et de créer des situations intenables, incompatibles avec le libre arbitre. Dans la lutte contre le Covid-19, la technologie permet de cartographier, d'informer et de contrôler, a-t-il été dit. Pour ma part, je ne vois pas autre chose, dans le *tracking*, que le contrôle et la limitation des libertés : d'un strict point de vue scientifique et médical, rien ne prouve l'efficacité d'un tel dispositif.

Mme la présidente Yaël Braun-Pivet. C'est justement l'objet de l'audition suivante : il me paraissait essentiel que nous ayons un point de vue scientifique sur la question.

Mme Danièle Obono. Le « solutionnisme » technologique est une impasse : les solutions prétendument pragmatiques et neutres permettant de résoudre les problèmes, cela n'existe pas. Plutôt que de s'attaquer aux causes du phénomène, on ajuste les comportements des individus. Existe-t-il une méthode de traçage numérique des contacts qui garantisse à 100 % l'anonymat et interdise l'identification par croisement des données collectées, autrement dit qui ne soit pas attentatoire au droit au respect de la vie privée ? La pression sociale sera très forte – on le constate d'ores et déjà. Par quels moyens la CNIL pourra-t-elle vérifier que les données collectées ne sont pas conservées par l'État ou par des opérateurs privés ? La question se pose d'autant plus que des projets visant à développer les techniques

de traçage existent. Enfin, si le *Bluetooth* est présenté comme une solution alternative, il n'est pas sans failles.

Mme Marie-Laure Denis. La question de l'inégalité entre les citoyens mérite une vigilance particulière. Il importe d'avoir conscience de la réalité sociale et de la fracture numérique : un quart au moins de la population ne dispose pas de téléphone permettant de télécharger des applications. Il est même probable que cela corresponde à la catégorie des personnes les plus vulnérables, celles-là mêmes qui, dans le cadre d'une stratégie de déconfinement progressif, resteraient confinées le plus longtemps. C'est un enjeu social important.

Je ne vois pas comment il serait possible de stigmatiser ceux qui n'utiliseraient pas l'application : vous seul savez si vous l'avez téléchargée. À Singapour, seulement 15 % à 20 % des habitants l'ont fait, et l'État s'est finalement résolu à imposer des mesures de confinement. Preuve s'il en est que la mise en place d'une application de suivi des personnes n'est qu'un des éléments de la réponse sanitaire : ce n'est en rien une solution magique.

S'agissant de l'instantanéité de la notification, si j'en juge d'après les dispositifs existant à l'étranger, c'est seulement lorsqu'une personne sait qu'elle a été contaminée que l'historique des numéros – et non le nom – des gens avec qui elle a été en contact est envoyé aux autorités sanitaires.

M. Gwendal Le Grand. Il ne faut pas que la notification soit immédiate, car cela reviendrait à vous dévoiler des informations sur l'état de santé de tous les gens que vous croisez… Qui plus est une application *Bluetooth* a précisément l'avantage de permettre de remonter dans le temps, sachant que c'est seulement au bout de quelques jours que l'on sait qu'on a été infecté. Il serait alors possible de prévenir de manière différée les personnes qu'on a croisées. Le délai précis de vérification reste à fixer, mais elle pourrait être faite à intervalle de quelques heures ou une fois par jour. En outre, pour protéger la vie privée, il est important d'utiliser des identifiants aléatoires et d'échanger seulement les données strictement nécessaires pour informer les gens qu'ils ont été potentiellement exposés au virus. Enfin, sur le plan technique, l'utilisation de technologies de proximité est plus protectrice que la géolocalisation des utilisateurs.

Mme Marie-Laure Denis. Nous avons déjà l'habitude de contrôler les responsables des traitements de données, publics et privés. Tout en espérant que le Parlement nous donne davantage de moyens pour accomplir nos missions, nous effectuerons donc ces contrôles, comme toujours – mais avec une vigilance encore accrue. Se pose d'ailleurs, à cet égard, la question de savoir s'il y aura une seule application ou bien plusieurs applications concurrentes, car on observe un grand foisonnement dans ce domaine, qui ne sera pas sans incidences sur l'activité de contrôle.

M. Sacha Houlié. Je rejoins les propos de M. Eliaou concernant la pression qu'exercerait le corps social sur ceux qui n'utiliseraient pas volontairement l'application. Par ailleurs, le dispositif de traçage est à lui seul insuffisant, comme le montre l'exemple de Singapour. En outre, et dans la mesure où 13 millions de nos concitoyens n'ont pas d'appareils connectés, l'efficacité du dispositif serait limitée.

En 2015, la loi relative au renseignement a autorisé la collecte de données, y compris en temps réel, pour le compte des services de renseignement. Qui, sinon la CNIL, a pu contrôler ces dispositions ? Le Parlement devait évaluer le mécanisme cinq ans après sa mise

en œuvre, soit au mois de juillet de cette année. Quel est votre retour d'expérience s'agissant du contrôle des données collectées dans ce cadre ? Pouvez-vous nous garantir que celles-ci sont détruites, sachant que, pour ma part, je ne crois pas que ce soit possible ?

M. Raphaël Schellenberger. Tout le monde est mal à l'aise avec ce qui est proposé, même si le dispositif repose sur le *Bluetooth*, c'est-à-dire la technologie qui semble la plus acceptable. Nous devons savoir concrètement à quoi correspond ce contrôle de proche en proche des échanges stockés sur les smartphones. Je crains, en dépit de toutes les précautions qui seront prises, qu'on se rapproche d'un système de surveillance des uns par les autres et de délation généralisée. La pression populaire va monter – nous la mesurons d'ores et déjà avec les réseaux sociaux. L'injonction à rester chez soi, même si elle est en soi intéressante, peut très vite basculer dans l'atteinte à la liberté individuelle. Tout comme Stéphane Peu et Sacha Houlié, je crains que le recours à l'application de traçage ne constitue une atteinte aux libertés disproportionnée au regard de son efficacité. Si une telle application devait voir le jour, quel serait le portage le plus intéressant : public, privé ou bien mixte ? Le choix sera révélateur de ce que sera le dispositif en lui-même et sur le contrôle qu'il exercera sur les individus.

M. Philippe Latombe. Le consortium PEPP-PT, qui regroupe des chercheurs de huit pays européens, sera opérationnel en fin de semaine. Le Comité européen de la protection des données (CEPD) peut-il se saisir en urgence du dispositif qui devrait être proposé par ce consortium et émettre un avis ? Si celui-ci devait être positif, le CEPD aurait-il les moyens de faire en sorte que les pays européens souhaitant se doter de dispositifs de *tracking* comparables s'inscrivent dans la même démarche ? Cédric O a indiqué dans *Le Monde* que le Gouvernement réfléchissait à des applications sous le nom StopCovid. Avez-vous été saisis du projet ? Combien de temps vous faudra-t-il pour rendre un avis éclairé ?

Mme Cécile Untermaier. Le dispositif est présenté comme léger, assez anodin : ce n'est que du *Bluetooth*… La CNIL a-t-elle les moyens de faire en sorte que le dispositif reste léger ? Le législateur doit intervenir lui aussi. Le traitement de données à caractère personnel doit revêtir un caractère nécessaire, proportionné et adéquat. Or, le dispositif envisagé ne me semble respecter aucun de ces trois principes. Du reste, lorsqu'on apprend qu'on a été contaminé, on n'a qu'une idée : prévenir tous ceux que l'on a rencontrés. Enfin, quand bien même l'outil en question serait nécessaire, proportionné et adéquat et serait mis en place, quid de la fracture numérique ?

Mme Marie-Laure Denis. La loi de 2015 relative au renseignement ne saurait, en tout état de cause, servir de base à la collecte de données à des fins de lutte contre une crise sanitaire.

M. Jean Lessi. La mise en œuvre des techniques intrusives de collecte de renseignements découlant de la loi de 2015 et le contrôle du devenir de ces données relève de la compétence de la Commission nationale de contrôle des techniques de renseignement (CNCTR). La CNIL n'est autorisée à effectuer que des carottages individuels, lorsqu'une personne souhaite faire jouer son droit d'accès indirect et demande la rectification ou l'effacement de données la concernant. Les demandes formulées en ce sens sont suivies d'effets.

Mme Marie-Laure Denis. Je n'ai pas, à ce stade, un panorama assez précis des solutions de portage existantes pour me prononcer ; il est certain que l'État et la recherche publique devront jouer un rôle déterminant, et il faudra faire appel aux opérateurs sur lesquels l'État peut exercer un contrôle plus étroit.

En ce qui concerne la pression populaire, le fait de ne pas télécharger une application me paraît moins visible que celui de marcher dans la rue quand c'est interdit ou de se tenir trop près d'une autre personne dans un magasin… L'espace numérique, de ce point de vue, est plus protecteur – dès lors que le recours à l'application repose sur le volontariat, s'entend.

Le CEPD sera nécessairement associé aux activités du consortium européen, encore en pleine réflexion, et donnera un avis.

La CNIL n'a pas encore été saisie par le Gouvernement d'un projet finalisé. Notre expertise technologique et juridique est d'ores et déjà mise à profit, en coordination notamment avec l'Institut national de recherche en informatique et en automatique (INRIA), pour appeler l'attention sur les dispositifs les plus protecteurs de la vie privée. Nos équipes sont très compétentes et engagées, mais nous avons tout de même besoin de quelques jours pour rendre un avis sur un dispositif : une fois qu'il a été analysé, il doit être soumis à notre collège, qui est l'organe compétent en la matière.

La fracture numérique est effectivement un réel problème, qui montre d'ailleurs l'intérêt qu'il y a à fonder le dispositif sur le volontariat. Par ailleurs, la transmission automatisée de l'information fait gagner du temps par rapport à une démarche consistant à prévenir soi-même les gens qu'on a rencontrés, ou à l'enquête menée par les autorités sanitaires lorsqu'elles demandent aux personnes malades avec qui elles ont été en contact.

Pour porter une appréciation sur le caractère proportionné, nécessaire et adéquat des traitements mis en œuvre, il importe d'articuler le respect des principes de la protection des données avec une analyse précise de la situation sanitaire. C'est la raison pour laquelle la CNIL a souhaité auditionner le professeur Delfraissy. Vous avez vous aussi à cœur d'avoir la meilleure connaissance possible du contexte sanitaire, d'autant que celui-ci évolue de jour en jour.

Mme Laetitia Avia. À supposer qu'il s'agisse d'une application téléchargée consentie au regard d'un objectif non de surveillance du confinement mais de protection et d'information, la question se pose de sa réelle utilité, mais surtout de l'inégalité de l'accès à ces technologies.

Les comparaisons internationales sont intéressantes, mais il existe en France différents dispositifs utilisant des données personnelles à des fins de géolocalisation, mis en œuvre par des entités privées, à commencer par des applications de rencontres qui permettent à leurs utilisateurs de se reconnaître sitôt qu'ils se croisent dans un certain périmètre. A-t-on une idée du nombre d'opérateurs et d'utilisateurs recourant à ces technologies en France ? Des organismes publics utilisent-ils aussi de tels outils de géolocalisation ? On ne sait pas encore très bien ce qui se cache derrière le concept de *smart cities*, c'est-à-dire de villes intelligentes.

M. Antoine Savignat. On a tous bien compris que ce dispositif était un vrai coup de canif dans le contrat social en matière de libertés et de secret médical. Quand bien même il ne serait pas obligatoire et mis en place à droit constant, ne faudrait-il pas en démontrer la nécessité ? Si tel est le cas, comment la quantifier ?

Mme Maina Sage. Avez-vous d'autres exemples que celui de Singapour quant au pourcentage d'adhésion à ce type de dispositif ?

Ayant été testée positive, je peux témoigner que j'aurais vraiment souhaité pouvoir utiliser ce genre d'application, car il est compliqué de se souvenir de tous les contacts que l'on a eus depuis le moment où on pense avoir été en contact avec une personne positive.

Comment se prémunir des « volontaires malveillants », autrement dit comment vérifier la véracité de la déclaration d'un test positif ? Y a-t-il un lien avec un service public pour garantir la fiabilité de la donnée ? Une fois la personne volontaire identifiée comme positive, comment est-elle contrôlée ? Cela pose la question de l'immédiateté du suivi et de la réactivité du système pour protéger les personnes susceptibles d'être en contact avec une personne testée positive.

M. Ugo Bernalicis. Je m'interroge sur la sécurité intrinsèque de ce genre de dispositif par le biais du *Bluetooth*, même s'il est circonscrit à un périmètre très faible. Nous ne pourrons faire l'économie d'une audition de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sur ce sujet.

À supposer que je fasse croire, par pure malveillance, que j'ai eu le Covid-19, je vais créer un effet de panique. Inversement, si je suis sorti seulement de chez moi pour aller à la boulangerie et que je reçois un signal selon lequel j'ai été contaminé, j'aurai peur de retourner à la boulangerie… Autant d'exemples qui montrent qu'on perd beaucoup de temps et d'énergie à disserter sur la nécessité de tels dispositifs alors que nous avons des problèmes bien plus urgents à traiter. Plutôt que d'imaginer comment contourner nos dispositifs de droit, attachons-nous à les renforcer et à préserver nos libertés individuelles.

Mme Marie-Laure Denis. Madame Avia, je crois avoir déjà répondu sur le caractère potentiellement inéquitable de ce dispositif.

Si vous le souhaitez, la CNIL pourra vous transmettre ultérieurement les éléments qu'elle a déjà pu produire en ce qui concerne les autres dispositifs de géolocalisation qui existent en France, notamment les *smart cities*, avec des exemples très concrets des problématiques soulevées.

Monsieur Savignat, c'est seulement en articulant les informations que vous et nous pourrions recueillir sur la réalité du contexte sanitaire que l'on pourra porter une appréciation sur la nécessité de la mise en œuvre de ce dispositif : ce n'est, je le redis, qu'un élément d'une réponse sanitaire plus globale le cas échéant.

Je m'interroge sur le pourcentage de la population qui devrait adhérer à ce dispositif pour qu'il ait une réelle efficacité sanitaire. Méfions-nous des comparaisons internationales : les différences de culture notamment peuvent donner des résultats très différents. Les pays d'Asie ont une sorte de respect de la règle, une culture numérique plus développée, des habitudes culturelles : les gens ont déjà coutume d'y porter des masques, moins pour se protéger eux-mêmes que pour protéger les autres.

La question de la véracité de la déclaration d'un test positif pose plus largement celle de la fiabilité technique de la mise en œuvre de tels dispositifs : l'utilisation du *Bluetooth* présente beaucoup moins de risques de sécurité que celle du *Wifi*, par exemple, et son rayon est beaucoup plus limité. Il est délicat pour la CNIL de se prononcer *ex ante* sur un outil dont on ne connaît à ce stade les éventuels contours que de manière abstraite et vague ; mais si un dispositif nous était soumis, soyez convaincus que nous le décortiquerions de A à Z. Par ailleurs, je rappelle que nous nous inscrivons, dans le cadre de cette crise sanitaire, dans un

contexte d'accompagnement global et partenarial avec différentes entités publiques, comme l'INRIA, l'ANSSI, etc.

Mme Caroline Abadie. Je m'interroge sur le fonctionnement et le traitement des trente maladies à déclaration obligatoire, comme la dengue et la méningite, qui permettent leur suivi épidémiologique, et obligent les médecins et les biologistes à les déclarer sans que le patient n'ait à y consentir. Quel est votre rôle dans cette procédure, notamment d'anonymisation, d'exploitation et de stockage des données ? Ce système pourrait-il être opérant sur le Covid-19 ?

M. Didier Paris. Le système *Bluetooth* suppose un minimum de conservation de données pour retracer ensuite les contacts. Or les études que j'ai menées sur les modalités de contrôle des fichiers de police ont montré l'énorme différence entre la bonne idée de départ et le point d'arrivée, relativement défaillant, y compris dans le nettoyage des données, déterminant au regard des libertés individuelles. Terra Nova préconise la création d'une nouvelle autorité administrative indépendante, chargée d'encadrer et de contrôler les dispositifs et surtout les algorithmes utilisés, et qui viendrait en complément du travail effectif de la CNIL. La notion de contrôle renforcé par une autorité indépendante peut-elle entrer en ligne de compte pour mieux assurer la protection des libertés publiques ?

M. Hervé Saulignac. Ma première question a trait au consentement libre. Certains, dont Terra Nova, évoquent l'hypothèse de coupler le dispositif à une autorisation de sortie numérisée. Mais ne serait-ce pas une incitation de nature à fausser la liberté de consentement ?

Ma seconde question porte sur la population qui ne possède pas de smartphone, sachant que ce taux est beaucoup plus élevé chez les plus de soixante-dix ans qui sont par ailleurs les plus fragiles et les plus concernés par l'épidémie, ce qui pose la question de l'égalité des citoyens devant l'accès à des mesures de protection. Quelle est la masse critique d'usagers pour que le dispositif soit efficient ?

M. Olivier Marleix. Il me paraît étonnant de créer un dispositif qui permettrait d'informer en temps réel les gens qui sont au contact d'un malade, mais de ne pas les informer pour des questions de respect de l'anonymat… En fait, on organise une espèce de mise en danger délibérée de la vie d'autrui. Je n'aimerais pas être le ministre amené à signer un dispositif juridique aussi baroque…

Votre analyse semble faire abstraction du cadre juridique très particulier dans lequel nous sommes, très attentatoire aux libertés individuelles. La question n'est pas seulement celle de la pression sociale qui fausserait le consentement libre et éclairé, c'est aussi celle du confinement qui, s'il était maintenu, le fausserait tout autant. Ce dispositif, qui reposerait sur la base du volontariat, ne doit-il être envisageable seulement dans le cas où le confinement serait levé ?

Mme Coralie Dubost. De nombreuses applications vont déjà beaucoup plus loin dans la géolocalisation, qu'il s'agisse des réseaux sociaux ou des applications à visée personnelle, avec des durées de conservation des données qui peuvent atteindre soixante-douze heures. Le consentement accordé dans un cadre de loisirs est-il donné de façon suffisamment libre et éclairée ? Cela justifierait-il la mise en place d'un système comparable dans le but de protéger la santé de nos concitoyens et de la collectivité ?

Mme Marie-Laure Denis. Madame Abadie, nous sommes de manière générale très attentifs à l'anonymisation des données qui peuvent être collectées. Je pense que M. Jean Lessi pourra répondre plus précisément à votre question.

M. Jean Lessi. Faut-il inscrire le Covid-19 sur la liste des maladies à déclaration obligatoire ? L'obligation légale de déclaration supposerait une validation scientifique qui fait intervenir le Haut Conseil de la santé publique placé auprès du ministre chargé de la santé ; la CNIL ne remettrait bien évidemment pas en cause cette appréciation.

S'agissant de la protection des données, l'anonymat est renforcé par un numéro et une conservation très limitée dans le temps et très confidentielle. La CNIL peut contrôler l'efficacité de ce dispositif.

Mme Marie-Laure Denis. Monsieur Paris, nous sommes dans une situation tellement exceptionnelle que si un dispositif de ce genre voyait le jour avec des incidences potentiellement aussi exceptionnelles sur les libertés publiques, il devrait être assorti d'un contrôle tout aussi exceptionnel pour s'assurer très concrètement de la destruction, dans un délai très rapide, des données collectées.

A-t-on besoin de créer une nouvelle AAI qui s'occuperait exclusivement des algorithmes ? La CNIL a une expertise très poussée sur cette question, qui naturellement n'est pas exclusive. La loi de 2016 pour une République numérique a confié à la CNIL la mission d'animer le débat éthique et les débats de société sur le numérique. Le premier travail de la CNIL qui s'est échelonné sur une année entière, a abouti à la rédaction d'un rapport sur les algorithmes. Si l'on est passé du dispositif APB à Parcoursup, c'est précisément parce que la CNIL avait mis en demeure le Gouvernement de modifier l'explicitation et le fonctionnement du système de sélection qui était basé sur des algorithmes. Nous avons une expertise sur cette question et nous nous articulons avec d'autres autorités ou institutions pour la parfaire.

Monsieur Saulignac, je n'ai pas entendu parler, dans la bouche des responsables publics, de coupler la liberté du consentement et l'autorisation de sortie. Si tel était le cas, il faudrait analyser de très près la réalité d'un consentement : pour que le consentement soit réellement libre, il ne faut pas que le refus du consentement donne lieu à conséquences.

La masse critique d'usagers est en effet une des conditions essentielles de l'efficacité d'un tel dispositif. La CNIL n'a pas la compétence sanitaire, mais ce sujet mérite d'être débattu en lien avec la communauté scientifique : c'est la raison pour laquelle nous avons auditionné le professeur Delfraissy la semaine dernière. Nous ne manquerons pas de continuer à nous tenir au courant, en temps réel, de la réalité du contexte sanitaire, pour pouvoir apprécier la nécessité et la proportionnalité des mesures qui seraient prises.

J'en viens à la remarque de M. Marleix sur la réalité du confinement qui fausserait en quelque sorte le caractère libre du consentement. Selon que le dispositif s'appuie sur le volontariat ou une obligation, la réponse qui peut être apportée à cette question est très différente. Le téléchargement de l'application, par le fait qu'il est volontaire, ne devrait pas avoir d'incidences, dans la mesure où rien n'empêche de sortir du dispositif. Mais peut-être faut-il tenir compte de la réalité psychologique : on peut évidemment avoir envie de sortir du confinement et donc d'utiliser tous les moyens à notre disposition pour l'accélérer. C'est du reste un des arguments invoqués à l'appui de ce dispositif de suivi numérique.

Enfin, madame Dubost, une application qui utiliserait la technologie *Bluetooth* qui permet de détecter si un autre téléphone équipé de la même application se trouve à proximité, sans données nominatives mais avec la création d'un identifiant et un chiffrement de l'historique de connexion, apporterait davantage de garanties qu'une application reposant sur une géolocalisation précise et continue.

M. Gwendal Le Grand. En réalité, tout dépend de l'application. Avec certaines applications, vous déclarez volontairement que vous entrez dans un lieu. Ici, l'objectif n'est pas du tout le même : nous parlons d'utiliser une capacité de communication, en l'occurrence le *Bluetooth*, qui lorsqu'il est activé permet aux autres personnes de détecter qu'elles sont passées à proximité de notre téléphone. Il faut se garder de comparaisons avec toutes les applications qui utilisent, sous une forme ou une autre, y compris sous une forme déclarative, la géolocalisation.

L'intérêt d'une telle application tient au fait qu'elle vous permet de détecter, *a posteriori*, que vous avez été potentiellement exposé. On ne sait pas nécessairement à l'instant T qu'on est porteur du virus ; c'est seulement une fois qu'on a été testé positif qu'il est important d'informer les autres personnes qui sont passées à proximité. Cette information ne peut donc pas être donnée en temps réel.

Mme la présidente Yaël Braun-Pivet. Madame Denis, je vous remercie. Cette audition était indispensable, en témoignent les nombreuses questions qui ont été posées. Certains collègues ont déjà leur idée, tandis que d'autres ont encore besoin de se forger une conviction au regard de toutes ces données internationales et locales. Nous ne manquerons pas de faire à nouveau appel à vous si c'est nécessaire. Les questions relatives aux libertés publiques et à la protection des données sont essentielles dans la situation que nous traversons.

Mme Marie-Laure Denis. Bien évidemment, la CNIL se tient à la disposition de la représentation nationale, *a fortiori* dans ce contexte sanitaire exceptionnel.

*

La Commission accueille M. Simon Cauchemez, responsable de l'unité de modélisation mathématique des maladies infectieuses à l'institut Pasteur et membre du conseil scientifique Covid-19.

Mme la présidente Yaël Braun-Pivet. Monsieur Cauchemez, vous avez pu constater, en nous écoutant, que l'utilisation de vecteurs numériques pour lutter contre l'épidémie soulève de nombreuses questions : elle doit se faire seulement si elle s'avère « adéquate, nécessaire et proportionnée », selon les termes employés par la présidente de la CNIL. Qui plus est, pour être efficaces, les outils numériques mis en place, le cas échéant, supposent de recueillir un taux d'adhésion élevé. Enfin, ne risque-t-on pas de considérer le « solutionnisme technologique » comme l'alpha et l'oméga, et nous contenter des technologies pour freiner, voire contrôler l'épidémie ?

M. Simon Cauchemez, responsable de l'unité de modélisation mathématique des maladies infectieuses à l'institut Pasteur. Depuis vingt ans, ma spécialité consiste à étudier la propagation des virus dans les populations humaines afin de mieux anticiper ses conséquences et d'évaluer les stratégies de contrôle à adopter. J'ai étudié Ebola, Zika, le coronavirus du syndrome respiratoire du Moyen-Orient (MERS-CoV) ou la grippe

pandémique, souvent pour aider les autorités locales concernées. Mais jamais nous n'avions été confrontés à une situation aussi compliquée.

Le virus Covid-19 est très transmissible et sévère : en moyenne, une personne infectée le transmet à trois personnes, ce qui peut donner lieu à une situation explosive sachant que le taux de mortalité se situe entre 0,5 et 1 %. Si rien n'est fait, une très grande partie de la population sera rapidement infectée, les services de santé complètement saturés et la maladie causera la mort de plusieurs centaines de milliers de personnes en France. Cette stratégie peut d'emblée être exclue.

Une deuxième stratégie, encore défendue par certains pays, mais de moins en moins, consiste à construire une immunité collective : pour éviter la saturation du système de santé, on met en place des mesures de distanciation – fermeture des écoles ou télétravail – sans aller jusqu'au confinement, pour aplatir la courbe épidémique et mieux gérer la crise sanitaire. C'est cette stratégie d'atténuation que nous envisagions en amont, lorsque nous anticipions une situation pandémique ; nous pensions alors qu'il était impossible de tout stopper. Mais les modèles ont montré qu'elle ne permettait pas d'empêcher la totale saturation de nos systèmes de santé et, du coup, un nombre de morts très élevé.

C'est pour cela que nous sommes entrés dans la stratégie du confinement : il ne s'agit plus d'aplatir la courbe, mais d'éteindre purement et simplement la transmission de l'épidémie.

Avec quelques semaines de recul, nous pouvons mesurer l'impact du confinement, indéniablement positif : si rien n'avait été fait, une personne infectée aurait transmis le virus en moyenne à trois autres ; avec le confinement, nous sommes descendus à un peu moins d'une personne. Nous sommes à une étape charnière ; nous devons maintenir l'effort dans la durée, afin de passer d'une stagnation à une décroissance forte. Il s'agit de limiter au maximum le nombre d'admissions en réanimation, mais aussi, plus généralement, de réduire le nombre total de cas d'infections au Covid-19 en France pour envisager sereinement le déconfinement. Mais nous ne sommes pas sortis d'affaire.

Le risque associé à cette stratégie de confinement est celui d'une seconde vague épidémique ; celle-ci pourrait survenir au moment du déconfinement si la population n'a pas développé d'immunité collective. Il faudrait que 66 % de la population soit immunisée pour éviter une seconde vague. Or, du fait même du confinement, il est très probable que le chiffre actuel soit très inférieur à ce seuil. Le relâchement des mesures de contrôle risque donc de faire repartir rapidement l'épidémie et nous serions contraints de remettre en place un confinement. Jusqu'à récemment, l'alternative, telle que présentée dans les travaux de modélisation, était la suivante : soit mettre en place une stratégie d'immunité collective, ce qui conduirait à une crise sanitaire majeure ; soit alterner entre phases de confinement et de déconfinement, ce qui aurait un coût dramatique pour la population française.

La connaissance du niveau d'immunité atteint par la population est un paramètre clé : les enquêtes sérologiques seront essentielles. En tout état de cause, la sortie du confinement devra s'accompagner de mesures de contrôle très fortes : il faudra continuer à ralentir la propagation du virus tout en trouvant des solutions supportables. Nous pouvons nous inspirer de ce qui a été fait à Singapour, en Corée du sud, à Hong Kong ou à Taïwan, et aussi envisager l'apport de l'outil numérique, tout en gardant à l'esprit qu'il n'existe pas de solution miracle.

Dans les pays qui, comme la Corée du sud, sont parvenus à contenir l'épidémie, le numérique a constitué un apport important ; cependant, de nombreuses autres mesures de distanciation sociales y ont été mises en œuvre, soutenues par une bonne adhésion des populations.

Ces pays s'appuient également sur une stratégie simple : il s'agit d'identifier tous les cas et leurs contacts afin de les isoler. Cette stratégie a montré son efficacité pour des virus comme le syndrome respiratoire aigu sévère (SRAS) ou Ebola, pour lesquels quasiment toutes les personnes infectées développent des symptômes sévères et sont donc faciles à repérer, et pour lesquels la transmission démarre une fois que les symptômes se sont déclarés, ce qui permet d'isoler rapidement la personne avant qu'elle en ait infecté d'autres. Or le Covid-19 se caractérise par une très forte proportion de personnes infectées ne présentant pas de symptômes, mais aussi par une transmission susceptible de démarrer avant le début des symptômes ; on en déduisait que l'approche fondée sur l'identification des cas laisserait beaucoup trop de personnes infectées dans la nature et ne serait pas efficace.

Cependant, on observe que les pays qui ont déployé cette stratégie à grande échelle ont obtenu des résultats. Les options stratégiques dont nous disposons sont essentiellement des mesures de distanciation sociale – fermeture des écoles, télétravail – ; si nous nous contentons de ces outils, nous devrons bientôt réinstaurer un confinement. Ne serait-il pas judicieux de mettre en place, en parallèle, cette stratégie d'identification des cas et de suivi des contacts ? C'est la question qui agite toute la communauté scientifique. Encore faut-il trouver un système réellement efficace dans lequel les personnes présentant des symptômes ont la possibilité d'être orientées vers les bonnes structures pour être testées et obtenir leurs résultats rapidement, avant que des enquêtes épidémiologiques soient lancées sur le terrain. Les structures habituellement dévolues à ce type d'enquêtes ne suffiront pas ; il faut donc augmenter notre capacité, déployer des équipes en nombre suffisant et les soutenir par des outils numériques adéquats, par exemple une application.

Il faut trouver un équilibre entre ces différentes options ; ce n'est pas à moi de le déterminer, mais il est clair qu'à cette heure, la seule mesure capable d'éteindre l'épidémie est le confinement. C'est seulement si l'on parvient à renforcer la stratégie fondée sur l'identification et le suivi que l'on peut espérer faire pencher la balance, et éventuellement relâcher les mesures de distanciation sociale. Il ne faut pas s'attendre à ce que l'outil numérique soit suffisant, mais il peut s'avérer précieux.

Mme la présidente Yaël Braun-Pivet. Avez-vous une idée du taux d'adhésion de la population de Singapour à l'application ? Il se dit qu'il faudrait que la proportion de la population la téléchargeant volontairement s'élève au moins à 60 % pour que la mesure soit efficace.

M. Simon Cauchemez. Singapour a lancé une application de ce type, mais il existe aussi des modèles européens, allemand et britannique notamment. Une publication récente de la revue *Science* a montré, par des sondages effectués dans plusieurs pays européens – en particulier la France – que le taux d'adhésion à un tel dispositif serait assez fort, mais nous ne pouvons pas en être certains. C'est un élément déterminant : un outil numérique n'est parfaitement efficace que si tout le monde l'utilise – or nous savons que ce n'est pas le cas. Il doit en fait être intégré à un système plus large ; pour que l'épidémie s'éteigne, il ne suffira pas que les gens utilisent une application sur leur téléphone. Il faudra faire intervenir des personnes sur le terrain afin de mener le travail d'investigation, notamment pour répondre aux

enjeux de fracture numérique. Tout cela déterminera l'intensité des mesures de distanciation propres à éviter une reprise épidémique.

M. Jean-François Eliaou. Je m'interroge sur l'utilité d'un tel procédé, d'abord compte tenu des problèmes qu'il pose sur le plan législatif et juridique, au regard des libertés.

Sur le plan épidémiologique, certaines des hypothèses de départ présidant à la mise en œuvre de la mesure sont incertaines. D'abord, quelle est la probabilité qu'une forte proportion de la population soit immunisée ? Les prévisions sont un peu pessimistes à ce sujet, puisque des travaux italiens ont montré que même dans des zones très fortement infectées, l'immunisation est relativement faible. Il faut également prendre en compte la possibilité de contamination présymptomatique.

Enfin se pose la question de l'adhésion : le recours à l'outil numérique est fondé sur le volontariat, et la fracture numérique fait que tout le monde ne pourra pas être impliqué dans l'opération ; or les populations les plus fragiles sont souvent les plus susceptibles d'être contaminées.

En tant qu'épidémiologiste et au vu de tous ces éléments, êtes-vous satisfait de ce type d'approche, et que pensez-vous des biais qui lui sont inhérents ?

Mme Alexandra Louis. Nous avons bien compris que ces technologies ne peuvent être l'alpha et l'oméga de la sortie de crise, mais que nous apprennent les courbes étrangères d'évolution de l'épidémie quant à l'intérêt de leur utilisation ?

Le fait que seule une partie limitée de la population puisse accéder à ces technologies ne risque-t-il pas de mettre en échec un tel dispositif ? Et ne serait-il pas plus judicieux d'harmoniser sa mise en œuvre à l'échelle européenne ?

Enfin, comment pourrait-on utiliser ces données issues des enquêtes sérologiques et les articuler avec les autres mesures pour lutter efficacement contre le virus ?

Mme Laurence Vichnievsky. J'émets une réserve consubstantielle s'agissant des atteintes que l'on envisage de porter aux libertés individuelles. Quelle serait d'ailleurs l'utilité véritable de la collecte de données personnelles, alors que l'on ignore encore largement quelles sont les personnes qui sont ou qui ont été infectées ? Même les personnes qui présentent des symptômes ne sont pas systématiquement testées, seule une infime partie de la population a été dépistée. Un plan est envisagé dans les établissements d'hébergement pour personnes âgées dépendantes (EHPAD), mais aucun dépistage à grande échelle n'est prévu pour l'instant. J'émets donc des réserves très conséquentes quant à la proportionnalité d'un tel dispositif, et je me demande si les gestes barrières classiques ne restent pas une meilleure réponse.

Mme Cécile Untermaier. Je m'interroge pour ma part sur l'utilité complémentaire de cette application. Qu'apportera-t-elle ? Et quelle est sa fiabilité technique ? L'Allemagne a avancé sur l'élaboration de son outil ; avez-vous pu étudier ses préconisations et ses objectifs ? Est-ce selon vous le modèle qu'il faudrait pour la France ?

M. Raphaël Schellenberger. Quelle est la durée pendant laquelle il est raisonnable de conserver des données numériques ? Avec la CNIL, nous avons évoqué une durée de soixante-douze heures. Or le temps d'incubation du virus – entre une semaine et quinze jours

– est particulièrement long ; est-ce vraiment compatible avec le respect des libertés numériques ?

M. Simon Cauchemez. La première fois qu'un collègue m'a parlé de cette approche, j'avoue lui avoir gentiment ri au nez, tant ce montage paraissait fou… Mais face à la réalité dramatique de l'alternative – laisser filer l'épidémie pour créer une immunité de groupe, au risque d'une crise sanitaire majeure, ou bien alterner des périodes de confinement et de déconfinement jusqu'à l'arrivée d'un vaccin –, j'ai réfléchi au modèle coréen et à l'apport possible des technologies, et j'y ai vu une lueur d'espoir. Il y a certes de nombreux défis à relever, mais il faut considérer le numérique comme un outil complémentaire, susceptible de renforcer les autres dispositifs. À la question de savoir si cette approche me satisfait, je répondrais donc qu'elle ne peut être totalement écartée.

Les Français doivent avoir en tête les différentes options. Si nous voulons échapper au confinement, nous devons être capables de mettre en œuvre une approche efficace d'identification et de suivi. La fracture numérique est un vrai problème, et l'outil numérique ne pourra éviter le déploiement large d'équipes sur le terrain. Certaines caractéristiques du virus, notamment la possibilité de contamination présymptomatique et les nombreuses personnes asymptomatiques, nous faisaient penser que le modèle coréen ne serait pas efficace ; mais force est de constater qu'il donne des résultats et que nous devons nous en inspirer. Encore faut-il avoir un dispositif d'une réelle efficacité. Le numérique peut aider à la renforcer.

Le seul exemple dont nous disposons sur l'usage de ces technologies est celui des pays asiatiques, où le contexte est très différent du nôtre. Les tentatives européennes en la matière n'ont pas encore été validées sur le terrain. Si peu de gens utilisent l'outil numérique, l'impact des mesures d'identification et de suivi sera réduit et, sans nécessairement aller jusqu'au confinement, il faudra renforcer les mesures de distanciation sociale. De notre capacité à mettre en œuvre un dispositif efficace d'identification des cas et de suivi des contacts – d'ailleurs pas uniquement fondé sur l'outil numérique – dépendra la décision d'atténuer ou non les mesures de distanciation sociale.

Dans le cadre de ce dispositif, ce sont les tests d'amplification en chaîne par polymérase (PCR), qui permettent de détecter les personnes infectées au moment de leur réalisation, qui seront utilisés. Quant aux tests sérologiques, ils permettront de savoir qui a été infecté par le passé, et donc d'évaluer la situation en matière d'immunité collective ; peut-être aurons-nous une heureuse surprise, ce qui autoriserait à prendre des mesures de contrôle après confinement plus légères que prévu. La sérologie permettra aussi tester les médecins, afin de déterminer ceux ne présentant plus de risque pour leurs patients.

La collecte des données personnelles n'a pas d'utilité dans un contexte où il n'y a pas de dépistage à grande échelle et où le virus circule fortement. C'est seulement une fois que nous aurons réussi à éteindre la vague épidémique, lorsqu'il n'y aura plus que quelques cas sur le territoire national, et que la stratégie consistant à tester la population de manière intensive pour identifier tous les cas pourra être mise en œuvre, que l'utilisation des outils numériques prendra son sens ; cela permettra d'éviter que l'épidémie ne redémarre – c'est la stratégie qui était utilisée au début de l'épidémie, par exemple pour traiter le cluster des Contamines-Montjoie.

Il faut replacer cette application dans un dispositif bien plus large, qui va de l'identification des cas jusqu'au traçage des contacts, et dont nous espérons qu'il nous

permettra d'échapper à un nouveau confinement. S'il recueille une bonne adhésion au sein de la population et si toute la chaîne se met en place, il peut avoir un impact important. Il reste à savoir si nous parviendrons à mettre en place ce système dans le contexte français et dans les délais impartis mais, hormis un nouveau confinement, je ne vois pas d'alternative.

Concernant la durée de conservation des données personnelles, si une personne est détectée au début des symptômes, soixante-douze heures me paraissent un délai raisonnable pour essayer d'identifier les contacts auxquels elle a pu transmettre le virus. Dans les cas de détection plus tardive, ce délai risque en revanche de ne pas permettre une telle identification.

M. Rémy Rebeyrotte. La Corée du sud a connu le SRAS et MERS-CoV ; elle a quinze ans d'expérience et une autre culture. Mais en France, j'ai l'impression que, pour le moment, toute allusion au déconfinement ou à une solution alternative au confinement, se traduit immédiatement par un relâchement des comportements. Les mesures s'additionnent-elles ? Dans une culture comme la nôtre, l'introduction de tels outils, qui peuvent être interprétés comme des solutions de substitution, ne risque-t-elle pas de remettre en cause les autres mesures en place, pourtant indispensables ?

Mme Danièle Obono. Vous avez indiqué que le confinement restait le seul moyen permettant vraiment d'éteindre la transmission. Avez-vous une idée de la proportion de la population qui doit être confinée pour que le virus cesse de circuler ? En effet, le confinement est actuellement généralisé mais pas total, puisqu'une partie de la population active continue à se rendre au travail ; cette situation ne contribue-t-elle pas à fausser l'effet du confinement ? Par ailleurs, à quel niveau de dépistage de la population faudra-t-il arriver pour que cette technologie devienne un complément efficace ?

M. Raphaël Gauvain. Vous estimez que l'utilisation de cette application numérique est importante pour assurer le déconfinement. Pourriez-vous être plus précis ? Est-ce important pour éviter la succession de phases de confinement et déconfinement ? Est-ce une nécessité absolue sur le plan opérationnel ou un élément parmi d'autres ?

M. Antoine Savignat. Vous nous avez expliqué que les seules mesures efficaces sont la distanciation et le confinement, mais également que le confinement a un effet pervers, en ce qu'il n'immunise pas une proportion suffisante de la population. Est-ce à dire que l'on ne pourra en sortir que lorsqu'on aura la certitude d'avoir éradiqué le virus ?

Une application de *tracking* a-t-elle la moindre utilité tant que l'on n'est pas en mesure de tester la population et de connaître les porteurs du virus ?

M. Xavier Breton. En matière de *tracking* toujours, à l'étranger, il semble qu'il faille être à deux ou trois mètres d'une personne pendant un certain temps – trente minutes dans certains cas – pour être identifié comme situé dans une zone à risques. À quelle distance et au bout de combien de temps y a-t-il selon vous risque de contamination ?

Mme la présidente Yaël Braun-Pivet. Compte tenu du tableau dressé et des limites de ces applications, considérez-vous qu'il faille aller plus loin et rendre ces dernières obligatoires ? Faut-il impérativement confiner toute personne suspectée d'être atteinte du Covid-19 ou ayant été en contact avec le virus, et le vérifier numériquement ? Au regard de vos vingt ans d'expérience, comment pouvons-nous sortir de cette crise sanitaire ? Les solutions technologiques font-elles partie de la palette ?

M. Simon Cauchemez. Monsieur Rebeyrotte, les pays d'Asie, comme la Corée du Sud, ont une grande expérience, liée au SRAS ou au MERS-CoV. La définition d'une stratégie est un enjeu majeur. Nous n'avions pas la même perspective il y a trois ou quatre mois. Il s'agit bien d'une guerre et, pour éviter les alternances de confinement et déconfinement, nous devons innover et impliquer massivement non seulement les développeurs, mais toute la société. Va-t-on y réussir dans le contexte français ? Je ne sais pas, mais nous devons essayer.

Vous avez raison, la priorité actuelle n'est pas de penser et de communiquer sur le déconfinement, mais bien sur le confinement, même si les parlementaires doivent réfléchir aux implications de plus long terme. À chaque fois qu'une stratégie de sortie est évoquée, on crée effectivement du relâchement… Cela étant, on ne peut imaginer rester confinés pendant un an ou dix-huit mois, dans l'attente d'un vaccin. La réflexion sur les outils du déconfinement est donc indispensable.

Quelle proportion de la population doit être confinée ? Pour évaluer l'impact de la fermeture des écoles, nous avions l'habitude de comparer la transmission de la grippe pendant les vacances et hors vacances scolaires. Nous pouvons également le faire pour le télétravail. Mais l'actuel confinement est inédit et nos modèles mathématiques trouvent donc leur limite. Nous savons qu'il faut réduire drastiquement les contacts pour diminuer efficacement la transmission, mais nous ne savons pas déterminer exactement la proportion de population à confiner. Nous pouvons seulement dire que ces trois semaines de confinement ont sans doute permis de réduire la transmission du virus d'environ deux tiers, ce qui était notre objectif en fin de confinement.

Monsieur Gauvain, les applications sont importantes, mais sont-elles vraiment indispensables ? Il y a quatre mois, la plupart des spécialistes vous auraient assuré que la détection des cas et le suivi des contacts représentaient un effort énorme, voire impossible en France. Mais, désormais, il faut maximiser autant que possible l'efficacité du processus, qui peut d'ailleurs également échouer si la logistique des tests ou le rendu des résultats ne sont pas bons. Les applications sont un moyen parmi d'autres pour l'améliorer.

Nous savons que nous ne disposons pas, actuellement, des moyens nécessaires pour assurer un suivi correct des contacts à grande échelle. Nous devons donc, me semble-t-il, recourir à une stratégie qui combine un renforcement considérable des équipes qui travaillent sur le terrain, notamment auprès des populations qui n'ont pas accès au numérique, et le déploiement d'une application. Si celle-ci est réellement utilisée, et je crois, à titre personnel, qu'elle peut susciter une adhésion forte de la population, elle peut représenter un élément important du dispositif.

La stratégie d'identification des cas et de suivi des contacts n'a de sens qu'une fois l'épidémie éteinte, lorsque l'on est en mesure de détecter très rapidement les personnes contaminées et de retrouver celles avec lesquelles elles ont été en contact.

La question des modalités de mise en œuvre du traçage est complexe. Quel type de contact est susceptible de transmettre le virus ? Il est difficile de le dire. Si ces outils sont développés et utilisés, il sera important d'évaluer leur impact sur l'épidémie en situation réelle. Si l'on s'aperçoit, par exemple, que tous les contacts positifs sont identifiés par des équipes de terrain et non par l'application, sans doute faudra-t-il revoir son utilisation. De même si, à l'inverse, son efficacité est avérée.

Faut-il rendre le dispositif obligatoire ? Je me garderai bien de faire des recommandations en la matière ; je peux simplement vous éclairer sur le niveau d'efficacité requis pour atteindre l'objectif fixé : la réduction des éléments de transmission de deux tiers. En tant que scientifique, ce que je peux dire, c'est que l'utilisation massive des outils numériques sera importante, qu'elle soit obligatoire ou fondée sur le volontariat. Il reviendra aux autorités d'apprécier l'approche qui doit être privilégiée, en sachant que si l'on ne parvient pas à contrôler l'épidémie, on risque d'être confronté à une seconde vague et de devoir imposer un nouveau confinement.

Mme la présidente Yaël Braun-Pivet. Nous vous remercions pour vos propos très éclairants.

La réunion se termine à 13 heures

Membres présents ou excusés

Présents. - Mme Caroline Abadie, Mme Bérangère Abba, M. Pieyre-Alexandre Anglade, Mme Laetitia Avia, M. Erwan Balanant, M. Ugo Bernalicis, M. Florent Boudié, Mme Yaël Braun-Pivet, M. Xavier Breton, M. Vincent Bru, M. Éric Ciotti, M. Éric Diard, Mme Coralie Dubost, Mme Nicole Dubré-Chirat, M. Jean-François Eliaou, M. Christophe Euzet, M. Jean-Michel Fauvergue, Mme Isabelle Florennes, M. Raphaël Gauvain, M. Philippe Gosselin, M. Guillaume Gouffier-Cha, M. Dimitri Houbron, M. Sacha Houlié, M. Sébastien Huyghe, Mme Élodie Jacquier-Laforge, Mme Catherine Kamowski, Mme Marietta Karamanli, M. Guillaume Larrivé, M. Philippe Latombe, Mme Marie-France Lorho, Mme Alexandra Louis, M. Olivier Marleix, M. Jean-Louis Masson, M. Fabien Matras, M. Stéphane Mazars, Mme Emmanuelle Ménard, M. Ludovic Mendes, M. Jean-Michel Mis, M. Paul Molac, M. Pierre Morel-À-L'Huissier, Mme Danièle Obono, Mme Valérie Oppelt, M. Didier Paris, Mme George Pau-Langevin, M. Stéphane Peu, M. Jean-Pierre Pont, M. Bruno Questel, M. Rémy Rebeyrotte, Mme Maina Sage, M. Hervé Saulignac, M. Antoine Savignat, M. Raphaël Schellenberger, M. Jean Terlier, Mme Cécile Untermaier, M. Arnaud Viala, Mme Laurence Vichnievsky, M. Guillaume Vuilletet

Assistaient également à la réunion. - M. Didier Baichère, Mme Paula Forteza