Audition commission des lois Assemblée nationale
Propos liminaires de Madame Marie-Laure Denis, Présidente de la CNIL

Mercredi 8 avril 2020

[Seul le prononcé fait foi]

Madame la présidente,

Mesdames et Messieurs les députés,

Mesdames et Messieurs,

Je vous remercie d'auditionner la CNIL, dans le cadre de vos travaux de suivi de la crise sanitaire sans précédent que nous traversons actuellement.

Pour cette audition, - je suis accompagnée de Jean Lessi, secrétaire général, Gwendal Le Grand, son adjoint, qui pourront intervenir et apporter des précisions.

Je le disais à l'instant, nous vivons une crise sanitaire sans précédent, à l'échelle planétaire. En ces moments extrêmement difficiles pour tous, aux multiples répercussions dans notre vie personnelle et professionnelle, je voudrais avoir une pensée pour tous ceux qui sont dans la souffrance et la détresse ; mais aussi pour tous ceux qui sont engagés quotidiennement sur

le terrain pour soigner, accompagner les victimes, porter assistance ou encore informer la population.

Je tiens à le rappeler en préambule car toutes nos réflexions et toutes nos décisions ne peuvent être prises, quel que soit leur niveau de technicité, sans avoir en tête ce contexte.

Qu'il me soit permis, avant d'entrer dans le vif du sujet du recours au traçage numérique dans un contexte de crise sanitaire, de vous dire quelques mots sur les enjeux plus généraux de protection des données personnelles.

Ces enjeux sont nombreux pour deux raisons bien différentes.

D'une part, parce que la **continuité d'activité repose en partie sur des outils numériques consommateurs en données personnelles**, massivement utilisés (télémédecine, télétravail, cours à distance pour les élèves, etc.). Ce n'est pas le cœur de cette audition, mais je tenais à vous assurer que la CNIL entend jouer tout son rôle pour accompagner ces usages, par exemple en publiant des conseils pratiques très précis pour appuyer la cybersécurité des employeurs ou salariés ayant recours au télétravail.

D'autre part – c'est la deuxième série d'enjeux de protection des données - **les données personnelles sont vues comme une ressource pour répondre directement aux défis sanitaires** (recherche en santé, protection des personnes vulnérables, et, je m'y arrêterai bien sûr, accompagnement des stratégies de confinement et/ou de déconfinement au moyen d'outils localisant la personne ou retraçant son exposition).

Sur tous ces aspects, la CNIL s'est mobilisée pour accompagner les **pouvoirs publics et les organismes publics ou privés.**

En matière de recherche en santé, la législation permet la mise en place de programmes de recherche et plusieurs projets ou études sont déjà lancés. La CNIL a d'ailleurs publié un communiqué indiquant la marche à suivre pour pouvoir mettre en œuvre rapidement des projets de recherche portant sur le Covid-19.

La majorité des projets peuvent être mis en œuvre sans autorisation dès lors qu'ils sont conformes à une des méthodologies de référence. Il suffit alors de faire une simple déclaration à la CNIL.

Pour ceux des projets qui nécessitent une autorisation, par exemple les études pour lesquelles les patients ne peuvent pas être informés individuellement de l'usage fait de leurs données, nous avons publié une adresse mail dédiée pour pré-instruire les demandes. Dès que les dossiers sont complets, les autorisations peuvent être accordées rapidement, parfois même en quelques heures

La CNIL a déjà délivré depuis le début de la crise une dizaine d'autorisations à des acteurs comme l'AP/HP, l'Inserm, l'institut Pasteur, le CHU de Lille…

Ces études visent par exemple à tester des traitements, à étudier les facteurs de mortalité des patients âgés, ou encore à analyser l'évolution des formes graves de l'infection.

En dehors de la recherche en santé également, les données personnelles sont vues comme des ressources. La CNIL a ainsi pris contact avec les trois principaux niveaux de collectivités territoriales, représentées par Régions de France, l'ADF et l'AMF afin de faire connaitre aux élus de terrain sa disponibilité pour répondre aux questions se rapportant à la gestion de la crise sanitaire. Des questions très concrètes nous ont été posées sur les conditions dans lesquelles les données détenues par les collectivités

pouvaient être utilisées pour toucher au mieux les populations afin de leur porter assistance, en particulier les personnes les plus vulnérables.

J'en viens à la question qui a plus particulièrement justifié la demande d'audition, à savoir les outils localisant la personne ou retraçant son exposition, dont l'usage éventuel est l'un des fils rouge du débat public.

Dans quel état d'esprit la CNIL aborde-t-elle le débat autour de ces outils ? Je tenais à vous faire part de deux convictions.

La première, sur laquelle je voudrais particulièrement insister sur ce point devant la représentation nationale, c'est que **les textes qui protègent les données personnelles ne s'opposent pas à la mise en œuvre de solutions de suivi numérique, individualisé ou non, pour la protection de la santé publique. Ces textes imposent, essentiellement, de prévoir des garanties adaptées d'autant plus fortes que les technologies sont intrusives, j'y reviendrai.**

Du fait de l'urgence, la tentation peut exister de s'affranchir du cadre. Cependant, **mettre en avant un cadre respectueux de la vie privée et des données personnelles est tout à fait nécessaire pour, tout à la fois, asseoir la confiance, créer les conditions d'une acceptabilité sociale de toute technique potentiellement intrusive et garantir la sécurité. J'y insiste : il n'y a pas à se demander s'il faut s'affranchir du cadre, ou prendre des libertés avec celui-ci, parce que le cadre juridique que l'Europe et la France se sont donné comporte en lui-même, en son propre sein, les solutions permettant de répondre à la situation.**

La deuxième conviction dont je souhaitais vous faire part concerne le recours aux technologies numériques : **il faut se garder de penser qu'une application va tout résoudre, même si les nouvelles**

technologies peuvent contribuer à une sortie sécurisée du confinement, dans le cadre de la stratégie globale. J'appelle régulièrement à la vigilance contre la tentation du «solutionnisme technologique». Il faut explorer, à fond, les opportunités des technologies, mais aussi leurs limites intrinsèques et leurs risques pour l'identité humaine et les droits des personnes.

Si la technologie et le traitement des données peuvent nous être d'un grand secours dans la gestion de cette crise sanitaire, **il est aujourd'hui difficile, faute de recul suffisant, d'évaluer les bénéfices effectifs qui pourraient être tirés de l'utilisation de tels dispositifs, d'autant plus que les usages peuvent varier tant au niveau des données collectées que des finalités poursuivies**.

C'est aussi dans cette optique que la CNIL a le souci de s'entourer d'une double expertise. **La première**, qui est notre cœur de métier, c'est de se donner les moyens de **connaître et de comprendre, d'un point de vue technique, l'ensemble des dispositifs utilisés, des projets envisagés ou des solutions imaginées dans le monde pour lutter contre la pandémie** : nos ingénieurs, juristes et autres experts, au contact des innovateurs, en lien avec nos homologues, réalisent une veille continue depuis mi-mars. La seconde expertise nécessaire peut paraître moins naturelle mais elle est non moins nécessaire : **c'est la compréhension de l'intérêt de santé publique de telle ou telle solution envisagée, qui est essentielle pour permettre de mesurer la légitimité, la proportionnalité, la pertinence des traitements de données mis en œuvre.** C'est ainsi à ce titre notamment que le collège de la CNIL a, par exemple, auditionné la

semaine dernière le président du Conseil scientifique, le professeur Jean-François Delfraissy.

C'est sur la base de ces travaux de veille que j'en viens à un rapide tour d'horizon des exemples étrangers et les grandes tendances que nous observons en termes d'utilisation des données personnelles au service des stratégies de lutte contre la pandémie.

Les technologies utilisées sont multiples : caméras thermiques, reconnaissance faciale, utilisations de drones afin de diffuser des messages aux personnes ne respectant pas les mesures de confinement, collecte d'informations sur les médias sociaux, suivi de la localisation permettant de surveiller la position des personnes via leurs ordiphones, applications de « suivi de contacts » (ou « *contact tracing* »).

Je concentrerai mon propos sur ces dernières technologies, à savoir celles qui se fondent sur l'analyse de données de localisation des individus – par rapport à des personnes déjà exposées, à leur domicile, à des périmètres de confinement, à leur exposition au virus, etc. Les différents Etats à travers le monde ont recours aux données de localisation pour trois séries de finalités.

Tout d'abord, il apparaît que de nombreuses autorités souhaitent utiliser les données de localisation afin de pouvoir **cartographier la propagation du virus,** prédire les prochaines zones à risques ou encore aider les autorités à prévoir les prochains besoins médicaux urgents.

Par ailleurs, les données de localisation sont également utilisées afin de **faire respecter les mesures prises par les gouvernements** pour

endiguer la propagation du virus, telles que les consignes de distanciation sociale ou encore les obligations de confinement.

Enfin, certains pays utilisent ou ont l'intention d'utiliser les données pour **faire du suivi de contacts** (*« contact tracing »)*, c'est-à-dire retrouver les contacts des personnes potentiellement exposées afin de les avertir et éventuellement les inviter à se faire dépister. Pour ce faire, certains pays vont même jusqu'à recouper les données de localisation avec d'autres données (données sur les tests et les diagnostics, données détenues par les douanes et l'immigration afin de reconstituer les antécédents de voyage des personnes suspectées d'infection, etc.) et prendre, dans certains cas, des mesures individuelles.

Pour atteindre ces trois finalités, à des degrés divers, on peut distinguer schématiquement deux séries de techniques : la localisation « individuelle » et la localisation « collective ».

La première tendance trouve des illustrations principalement au Moyen-Orient et sur le continent asiatique, mais aussi en Europe. Il peut s'agir de dispositifs imposés aux citoyens, ou de dispositifs reposant sur le volontariat des personnes.

En Israël, un système basé sur les données de localisation des téléphones mobiles vise à détecter les personnes potentiellement exposées et leur envoyer des SMS pour leur demander de se mettre en quarantaine.

En Chine, les opérateurs de téléphonie mobile ont partagé des données de localisation sur les utilisateurs qui étaient passés par le Hubei avec plusieurs agences gouvernementales pour reconstruire les mouvements de porteurs potentiels du virus ainsi que des personnes susceptibles d'avoir été en contact avec eux.

En Corée du Sud, le gouvernement a ordonné à des personnes en quarantaine d'installer une application pour vérifier le respect du confinement. Les données de localisation détenues par les opérateurs de télécommunications ont également été utilisées pour identifier personnes exposées. Le résultat est exploité par les autorités mais aussi par des sites web gérés par l'Etat, qui permettent notamment aux personnes d'avoir une information sur les nouveaux cas locaux afin qu'ils puissent éviter les endroits où le virus était actif.

Ce peuvent être également des dispositifs fondés sur le volontariat

Comme à Singapour, qui a notamment développé une application, dont l'usage est basé sur le volontariat et sur la technologie Bluetooth. Cette application vise à identifier les personnes potentiellement exposées et identifier qui doit être testé.

Plus proche de nous, **la Pologne** a utilisé une application permettant de faciliter la vérification du respect des obligations de confinement pour les personnes soumises à une quarantaine obligatoire à leur retour d'un voyage à l'étranger. L'application utilise la géolocalisation et la reconnaissance faciale afin que les utilisateurs mis en quarantaine confirment par une photo géolocalisée qu'ils respectent bien leur obligation de confinement.

La seconde tendance, celle du recours aux données de localisation agrégées, est constatée dans de nombreux pays européens. Plus particulièrement en Italie, en Autriche, et en Allemagne, plusieurs opérateurs de télécommunications ont déclaré avoir fourni des

données « anonymisées » pour surveiller les déplacements des personnes et s'assurer du respect des mesures de confinement.

En Belgique, le ministre de la santé publique a autorisé les opérateurs de télécommunications à transmettre des « cartes de mobilité » anonymisées et basées sur des agrégats géographiques (comme le code postal) à un tiers privé. Croisées avec les données épidémiologiques des autorités, ces données sont censées permettre de prédire la propagation du virus.

De son côté, le gouvernement britannique travaille également avec les opérateurs de télécommunications pour analyser les données de localisation présentées comme « anonymes » afin de voir si la population respecte ses directives en matière de distanciation sociale ainsi que les nouvelles restrictions en matière de transport.

Par ailleurs de l'autre côté de l'Atlantique, aux Etats-Unis, le gouvernement serait en pourparlers actifs avec Facebook, Google et un large éventail d'entreprises technologiques et d'experts de la santé, sur la façon dont ils peuvent utiliser les données de localisation agrégées pour suivre la propagation du SARS-CoV-2.

En outre, plusieurs applications de suivi de contacts, dont le fonctionnement varie, sont actuellement en cours de développement (notamment les applications « Waze for COVID-19 », de l'OMS, et « Safe Paths » développée par une équipe de chercheurs du MIT et de Harvard).

En France, l'opérateur de télécommunications Orange a annoncé partager des données de localisation anonymisées avec plusieurs partenaires, dont notamment des chercheurs de l'institut français de la recherche médicale (INSERM) afin de permettre aux épidémiologistes de modéliser la propagation de la maladie.

Après ce rapide tour d'horizon des solutions constatées, quelle première analyse « informatique et libertés » en tirer ?

Je rappellerai tout d'abord que le cadre juridique encadre strictement l'usage des données de localisation des résidents européens, dans un souci de garantir la maîtrise maximale des personnes sur leurs données.

Deux textes sont applicables aux traitements de données de localisation.

D'une part, la directive de 2002 sur la protection de la vie privée dans les communications électroniques, dite « ePrivacy » pose un cadre très strict. On déduit de ses articles 5 et 9 que, sauf anonymisation, **le traitement de données de localisation, que ce soit via les opérateurs télécoms ou des applications installées par le téléphone (par des opérations de lecture d'informations localisées sur le terminal), est soumis au consentement**. Il n'est possible de déroger au consentement, par des « mesures législatives » des Etats membres, que dans certaines hypothèses limitativement énumérées à l'article 15 de cette même directive, parmi lesquelles figurent la « sécurité publique » entendue largement, susceptible de couvrir cette situation. En France, compte tenu de l'impact d'un tel dispositif et de l'article 34 de notre Constitution, il faudrait vraisemblablement une loi pour mobiliser ces exceptions.

D'autre part, le RGPD, applicable à tout traitement de données personnelles, notamment de *contact tracing*, offre un cadre juridique lui aussi exigeant. Il s'applique lorsque les données de localisation ne sont pas traitées de manière anonymisée. Les exigences découlant du RGPD sont, schématiquement, de trois ordres.

La première est que tout traitement de données doit avoir **une base légale**. Pour les dispositifs dont nous parlons, le consentement est la base légale qui vient immédiatement à l'esprit, mais le RGPD en prévoit d'autres, tels que « l'obligation légale », la mission d'intérêt public de l'organisme qui traite les données ou, dans certains cas particuliers, la sauvegarde des intérêts vitaux des personnes – concrètement, il faut donc, dans la généralité des cas, soit que les données soient anonymes, soit le consentement, soit un texte qui, en France, devrait être une loi.

La deuxième exigence du RGPD concerne plus spécifiquement **le traitement des données de santé susceptibles d'être collectées dans de nombreux dispositifs mis en œuvre pour gérer la crise sanitaire.** Le traitement de telles données est en principe interdit, sauf certaines exceptions. Parmi ces exceptions figurent le consentement de la personne ; les nécessités de sa prise en charge sanitaire ; l'intérêt public dans le domaine de la santé publique ; pour les seules personnes dans l'incapacité d'exprimer leur consentement, la sauvegarde de leurs intérêts vitaux ; la recherche peut également constituer une autre exception au principe du consentement.

La troisième exigence du RGPD, c'est, vous le savez, **l'application de toute une série de principes de fond et de garanties** que les Etats doivent respecter même lorsqu'ils ont des raisons légitimes de limiter certains droits et/ou certaines obligations : la proportionnalité, la sécurité, etc. L'objectif de ces règles est clair : c'est de maximiser la maîtrise des personnes sur leurs données – y compris, voire surtout, lorsque la base légale n'est pas le consentement.

Au regard de ce cadre juridique double, ePrivacy et RGPD, je peux synthétiser le faisceau de recommandations que le collège de la CNIL pourrait émettre à ce stade – non pas sur un projet en particulier, mais sur la manière d'aborder la problématique, sur le questionnement. Au-delà de la nécessité de disposer d'un fondement juridique adéquat pour traiter des données de localisation dans le cadre de la lutte contre le Coronavirus, un tel traitement devrait notamment respecter les principes suivants et assurer une maîtrise par les personnes sur leurs données.

En premier lieu, le **principe de définition et limitation des finalités : si l'on met en place un tel traitement, on doit savoir exactement pourquoi on le fait**. Or les comparaisons internationales montrent que ces finalités sont diverses. *A fortiori*, il faudra garantir, si un dispositif était mis en œuvre que les données ne pourront pas être traitées ultérieurement à des fins sans rapport avec la gestion de la crise sanitaire.

Une fois posé l'objectif poursuivi, il faudra pouvoir exposer pourquoi le recours aux données de localisation ou d'interactions est **adéquat, nécessaire et proportionné**. Adéquat : il faut que l'instrument mis en place apparaisse réellement utile pour traiter la crise sanitaire. Nécessaire : l'utilisation de telles données ne doit pas être une solution de confort. Il faut réellement qu'on en ait besoin pour juguler la crise et qu'il n'y ait pas d'alternatives efficaces. Proportionné : comme l'a rappelé le Comité européen à la protection des données (CEPD), les solutions les moins intrusives doivent toujours être privilégiées. Par exemple, les autorités publiques devraient **d'abord privilégier le traitement des**

données de localisation anonymisées, par rapport à un suivi individuel qui s'avère plus intrusif.

La proportionnalité pourra aussi être évaluée au regard du **caractère temporaire**, uniquement lié à la gestion de crise, de tout dispositif envisagé. C'est un point essentiel, et il ne signifie pas seulement que l'application ne sera utilisée que pendant la crise : **la durée de conservation des données** est une garantie très importante. Après la crise, les données devront en principe être détruites, ou sinon conservées un temps limité et de façon protégée, pour ne servir qu'à des finalités complémentaires de recherche ou de gestion d'éventuels contentieux. Le RGPD prévoit un cadre juridique qui a pleinement vocation à s'appliquer.

Il faut également respecter le principe de minimisation des données traitées : elles devront se limiter à ce qui est nécessaire. Par exemple, certaines applications de suivi des contacts ne traitent pas d'informations nominatives mais associent les données *via* un identifiant unique généré lors de l'installation de l'application.

Il faut donc concevoir **des dispositifs permettant d'assurer une maîtrise des personnes sur leurs données. D**ans les cas où un suivi individuel serait nécessaire, il devra, en l'état du droit, reposer sur une démarche volontaire de la personne concernée. C'est d'ailleurs le cas pour certaines applications de suivi de contacts existantes. Mais il faut bien s'entendre sur les mots : pour constituer un « consentement » valide au sens du RGPD, le « volontariat » doit en respecter toute les conditions, à savoir être éclairé (informé), spécifique à la finalité, univoque et libre – c'est-à-dire que le refus de consentir ne doit pas exposer la personne à des conséquences négatives. J'y insiste, parce que les comparaisons

internationales montrent que le volontariat a parfois des contreparties qui en limitent la liberté. A défaut de réel consentement, un texte comportant d'importantes garanties, qui en France ne pourrait être qu'une loi, devrait intervenir.

De plus, il faut privilégier le stockage des données en local, sur le terminal de l'utilisateur, lorsque cela est possible. D'une manière générale, les applications qui s'appuient sur des données Bluetooth, qui sont chiffrées directement sur le téléphone sous le contrôle de son utilisateur, apportent plus de garanties que celles qui s'appuient sur un suivi géolocalisé (GPS) continu des personnes.

Enfin, d'un point de vue plus technique, un tel dispositif devra, comme tout traitement, **respecter le principe de transparence, assurer la sécurité des données et respecter les droits des personnes prévus par le RGPD. S'agissant de l'exigence d'information:** il est crucial que les gouvernements et les acteurs privés soient transparents sur les dispositifs mis en œuvre et impliquant le traitement de données à caractère personnel. Les citoyens doivent savoir quelles données les concernant sont susceptibles d'être traitées, par qui, pour quelles finalités, dans quelles conditions et avec qui leurs données sont partagées.

En résumé :

Si un suivi individualisé des personnes était mis en œuvre, il faudrait d'abord, à droit constant, qu'il soit basé sur le volontariat, avec un consentement réellement libre et éclairé - et le fait de refuser l'application n'aurait aucune conséquence

préjudiciable. Ensuite, la CNIL veillerait notamment à ce que ce dispositif soit mis en place pour une durée limitée.

En revanche, si un dispositif de suivi des personnes était mis en place sur d'autres bases, notamment de manière obligatoire, alors il nécessiterait une disposition législative et devrait, en tout état de cause, démontrer sa nécessité pour répondre à la crise sanitaire ainsi que sa proportionnalité en tenant compte des mêmes principes de protection de la vie privée, et en étant réellement provisoire. A ce jour, les pouvoirs publics français me semblent toutefois, en l'état de leur réflexion, ne pas envisager le recours à un tel dispositif.

Pour terminer, je souhaite souligner que le niveau européen est évidemment un niveau pertinent de réflexion voire de réaction.

Les autorités de protection des données travaillent en réseau au sein du Comité européen à la protection des données. Elles s'organisent avec une montée en charge progressive :

- Le CEPD a très rapidement publié, le 19 mars dernier, des premiers éléments d'analyse afin de guider les responsables de traitement qui souhaitaient collecter des données de santé (dans un cadre employeur/employé notamment) ainsi que des données de localisation pour lutter contre la propagation du virus.
- Plus récemment, le comité s'est organisé afin de fluidifier l'échange d'informations relatives au COVID 19 (création d'un groupe de contact au sein même du CEPD).

o Par ailleurs, le CEPD qui habituellement se réunit en plénière une fois par mois, a désormais mis en place des réunions hebdomadaires à distance avec ses membres.

La priorité sera donnée à l'élaboration d'orientations concernant l'utilisation des données de localisation et l'anonymisation des données. La CNIL pilotera avec le CEPD, et avec certains de ses homologues cette réflexion. Deux autres priorités sont le traitement des données de santé à des fins scientifiques et de recherche et le traitement des données par les technologies utilisées pour permettre le télétravail.

o Je me garderai de conclure ce propos, même de manière très provisoire, tant il est délicat d'apporter des réponses précises par rapport à l'éventuelle mise en place d'un dispositif dont les contours sont nécessairement flous à ce stade. Le collège de la CNIL est pleinement conscient de l'urgence qu'il y a à conjuguer l'efficacité sanitaire et le respect des libertés fondamentales afin d'apporter les réponses les plus adaptées à la crise sanitaire sans précédent que nous affrontons. A droit constant, en ayant donc recours aux instruments juridiques existants, un dispositif numérique de suivi et individualisé des personnes peut-être mis en place – en étant qu'un des éléments d'une réponse sanitaire plus globale – à condition qu'il soit nécessaire et proportionné, et assorti de garanties particulièrement fortes pour protéger les données de ses utilisateurs.

C'est seulement en gagnant le pari de la confiance – indissociable du respect de la vie privée – que nos concitoyens pourraient être susceptibles d'adopter un tel dispositif de façon suffisamment massive pour en assurer l'efficacité sanitaire.

La CNIL assurerait la pleine effectivité de ses missions d'accompagnement et ses contrôles si les pouvoirs publics décidaient de la mise en œuvre d'un tel dispositif.