COVID-19 : tracé(e)s pour cause de pandémie

Depuis le début de la pandémie des traitements de données à caractère personnel à grande échelle ont été mis en œuvre. Ceux-ci recouvrent essentiellement trois grandes finalités et fonctionnalités :

- Le « contact tracing » pour retrouver des contacts ayant croisé une personne potentiellement infectée afin de les alerter et les inviter à se faire dépister et le cas échéant se mettre en quarantaine ;

- La géolocalisation des personnes infectées par le virus, éventuellement en combinaison avec des fonctionnalités permettant l'évaluation de leur état de santé au cours de la période de quarantaine, afin de faire respecter les mesures prises par le gouvernement pour limiter la propagation ;

- Les « cartes de mobilité » anonymisées basées sur des agrégats géographiques[1] et des données épidémiologiques des autorités afin de prédire la propagation du virus.

Ces solutions reposent donc toutes sur le traitement de données de localisation des smartphones et des données de santé avec ou sans procédé d'anonymisation.

Au niveau de l'Union européenne, la Commission a émis une première recommandation destinée à harmoniser l'utilisation de ces applications face à la pandémie[2].

Cette recommandation concerne la mise en place d'une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise du COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées.

Elle prévoit d'ores et déjà une finalité de dimension européenne puisqu'elle propose que « les Etats membres (représentés au sein du réseau « Santé en ligne », en lien avec le comité de sécurité sanitaire, le réseau de surveillance épidémiologique, l'ECDC et, si nécessaire, l'ENISA) échangent les meilleures pratiques sur l'utilisation des données de mobilité, partagent et comparent leurs modélisations et prévisions sur la propagation du virus, et surveillent les effets des mesures destinées à limiter cette propagation[3]. ».

Dans ce contexte et à l'aune de cette recommandation, il est légitime de s'interroger sur les conditions dans lesquelles de telles applications peuvent s'inscrire dans le cadre juridique de la

[1] Code postal par exemple.

[2] Recommandation (UE) 2020/518 de la Commission européenne du 8 avril 2020 concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées, JOUE du 14/04/2020.

[3] Article 19 de la recommandation (UE) 2020/518.

protection des données personnelles, que chacun connaît désormais sous le nom du RGPD[4]. De plus, au vu de la nature des données qui sont susceptibles d'être exploitées, il faut également citer une réglementation spéciale au niveau européen qui régit le volet « données personnelles » des communications électroniques. Le texte de référence en la matière est la directive dite « ePrivacy[5] ».

Ces textes génériques sont complétés par des dispositions spécifiques relatives, d'une part, à la surveillance épidémiologique et, d'autre part, au domaine de la santé (même si celui-ci reste principalement de la compétence souveraine des Etats membres). La recommandation fait ainsi état de :

- La décision du Parlement européen et du Conseil qui établit des règles spécifiques en matière de surveillance épidémiologique, de surveillance des menaces transfrontières graves sur la santé, d'alerte précoce en cas de telles menaces et de lutte contre celles-ci[6] ;
- La directive relative à l'application des droits des patients en matière de soins de santé transfrontaliers[7].

La Commission européenne a annoncé qu'elle interviendrait de nouveau, en tant que de besoin, afin de compléter sa recommandation « par des orientations supplémentaires [...], notamment en ce qui concerne les implications, sur le plan de la protection des données et du respect de la vie privée, de l'utilisation d'applications mobiles d'alerte et de prévention. ».

Dans la foulée a ainsi été publié le 15 avril 2020, le document intitulé « Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States », qui pose les principales exigences que doivent respecter les Etats membres pour ces applications nationales :

- Etre volontaires ;
- Etre approuvées par l'autorité sanitaire nationale ;
- Préserver la confidentialité (les données personnelles sont cryptées) en toute sécurité ;
- Etre supprimées dès qu'elles ne sont plus nécessaires.

A l'aune de ces textes et de ces recommandations de la Commission européenne qui viennent fixer un équilibre entre le droit d'exploiter les données personnelles et les libertés individuelles et collectives, au premier chef desquelles figurent le droit au respect de la vie privée et la liberté d'aller et venir de façon anonyme dans une démocratie. Il est légitime de s'interroger sur les conditions juridiques que ces traitements de données personnelles d'envergure nationale doivent respecter, tout particulièrement leur base légale (**1**) et l'identification du(des) responsable(s) de traitement (**2**).

Ces questions sont d'autant plus prégnantes que parmi les données personnelles, objets de ces traitements, des données de santé seront collectées. Or, en raison de leur particulière sensibilité,

---

[4] Il s'agit du règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, désigné dans les termes suivants : « règlement général sur la protection des données » ou « RGPD ». La France a mis à jour la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite loi Informatique et Libertés – LIL) à l'aune du RGPD.

[5] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques.

[6] Décision no 1082/2013/UE du Parlement européen et du Conseil du 22 octobre 2013 relative aux menaces transfrontières graves sur la santé et abrogeant la décision no 2119/98/CE (JO L 293 du 5.11.2013, p. 1).

[7] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).

pouvant révéler l'intimité de la personne, le traitement de cette catégorie de donnée est par principe interdite sauf exceptions expressément prévues par les textes.

I. Identification de la base légale justifiant la création de solutions de tracing sanitaire ou de géolocalisation

A ce jour, il est envisagé un débat au Parlement sur le sujet du tracing. En outre, le premier ministre auditionné le 1er avril 2020 par la mission d'information de l'Assemblée nationale a confirmé que de tels dispositifs de tracing n'existent pas en France et ne peuvent être rendus obligatoires car « ils ne seraient pas légalement permis ». On pourrait peut-être, a-t-il précisé, en créer sur la base « d'un engagement volontaire », c'est une question « qui est à ce stade encore ouverte pour mieux tracer la circulation du virus. ».

1.2 Insuffisance du consentement ?

Le volontariat ou plus exactement le consentement des personnes est généralement proposé comme prérequis pour les solutions traitant des données de localisation sans procédé d'anonymisation.

Le texte de référence en la matière est la directive européenne dite « ePrivacy[8] » qui dispose que, sauf anonymisation, le traitement de données de localisation est soumis au consentement préalable des personnes concernées[9] et qu'il n'est possible d'y déroger que par des « mesures législatives » des Etats membres pour des raisons de « sécurité publique[10] ».

Le RGPD comme source de droit commun de la protection des données personnelles prévoit également le consentement comme base légale possible d'un traitement de données à caractère personnel.

Le consentement figure également comme exigence dans la boîte à outils établie par la Commission européenne[11].

Cependant faire reposer la légalité de ces traitements sur le seul consentement des utilisateurs, nous semble être une base juridique fragile ne garantissant pas de façon satisfaisante les exigences de protection des données personnelles.

En effet, le consentement doit, pour constituer la base légale d'un traitement de données à caractère personnel, être éclairé, spécifique, univoque et libre[12] :

- Eclairé, c'est-à-dire répondre aux exigences d'information du RGPD[13] notamment concernant les destinataires des données, les durées de conservation, les droits des personnes dont le droit de retirer son consentement à tout moment et d'introduire une réclamation auprès de la CNIL, ainsi que les éventuelles finalités ultérieures ... ;

---

8 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques.

9 Article 5 et 9 directive 2002/58/CE.

10 Article 15 directive 2002/58/CE.

11 SG-02 Voluntary character App should be consent-based with full information of intended processing of data.

12 Articles 4 et 7 du RGPD.

13 Articles 13 et 14 du RGPD.

- Spécifique à la finalité qui doit être déterminée, explicite et légitime ;

- Univoque et libre, c'est-à-dire que le refus de consentir ne doit pas exposer la personne à des conséquences négatives.

Or, le citoyen français ne se sentira-t-il pas stigmatisé en ne consentant pas à donner sa localisation face à la pression sociale et à la campagne médiatique qui sera faite autour de l'intérêt pour le bien de tous du recours à la solution de tracing ?

Si ce risque s'avère plausible, le consentement ne semble pas dès lors suffisamment solide pour constituer à lui seul la base légale du traitement.

A défaut de réel consentement possible dans les faits, un texte législatif ou réglementaire comportant d'importantes garanties pour les droits et libertés des personnes serait recommandé pour les traitements utilisant des données de localisation non anonymisées ayant les finalités précitées de « contact tracing » et de géolocalisation des personnes infectées.

Une base légale autre que celle du consentement pourrait être relative à la mission d'intérêt public ou relevant de l'exercice de l'autorité publique. Cependant, cette mission d'intérêt public ne peut pas être présumée par l'organisme qui met en œuvre le traitement de données de santé.

Pour fonder valablement le traitement envisagé dans le cas d'une application de tracing, cette mission doit donc avoir une base juridique dans le droit auquel l'organisme est soumis. Le RGPD n'impose pas de niveau de norme particulier. Il peut être défini dans des règlements européens, des lois, des décrets, etc.

En France, le gouvernement pourrait utiliser l'article 31 de la loi Informatique et Libertés (LIL) et introduire un texte réglementaire poursuivant l'intérêt national ou la sécurité publique.

Selon l'article 31 de la LIL[14] , les traitements de données personnelles comportant des données de santé et intéressant la sécurité publique sont autorisés par décret en Conseil d'Etat pris après avis motivé de la CNIL. Une autre option pourrait consister dans le choix d'un décret d'application des textes qui confient la compétence de gestion des menaces sanitaires graves au ministre chargé de la santé (cf. article L3131-1 du code de la santé publique).

Toutefois, en raison du risque d'atteinte aux libertés fondamentales, un texte de loi contrôlé par le Conseil constitutionnel peut paraître indispensable, à tout le moins une habilitation du gouvernement à agir par voie d'ordonnance délimitant le périmètre de son intervention.

Le recours à la loi n'est pas imposé par la Constitution française, qui ne contient pas, à la différence de celle de certains autres Etats européens, de dispositions explicites au sujet de la protection des données personnelles. En outre, la LIL permet comme on vient de le voir leur création sans recourir à une loi, y compris dans le domaine de la sécurité.

Cet état du droit pourrait être changé en prenant appui sur l'article 34 de la Constitution, suivant lequel la loi fixe les règles relatives aux garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques, ainsi que la procédure pénale. Ainsi, un rapport parlementaire a pu

[14] Extraits de l'art. 31 de la LIL « I.-Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :
1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;
II.-Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission. Cet avis est publié avec le décret autorisant le traitement. ».

déjà recommander que seule la loi puisse autoriser la création d'un fichier de police[15], mais ces recommandations n'ont pas été suivies d'effet.

Ces dispositions légales, outre les finalités du traitement en cause, devront définir ses caractéristiques (données traitées, durées de conservation, destinataires, etc.).

« En règle générale, plus l'incidence sur les libertés individuelles est importante, plus les garanties correspondantes prévues dans la législation applicable devraient être solides.
Les législations de l'UE et des États membres qui existaient avant la flambée de COVID-19 et celles que les États membres adoptent spécifiquement pour lutter contre la propagation d'épidémies peuvent, en principe, servir de base juridique pour le traitement des données des personnes si elles prévoient des mesures permettant de surveiller les épidémies et si elles satisfont aux autres exigences énoncées à l'article 6, paragraphe 3, du RGPD[16]. ».

En dehors de tout texte légal, qui pourra prévoir le consentement des personnes concernées, il reste bien entendu la base légale relative la sauvegarde des intérêts vitaux. Comme l'explique la CNIL, la base légale relative à la sauvegarde des intérêts vitaux peut être retenue comme fondement, par exemple lorsque le traitement est nécessaire pour suivre la propagation d'épidémies ou dans les cas d'urgence humanitaire.

Il n'en restera pas moins nécessaire de veiller, conformément au RGPD, à une pondération quant au traitement de données de santé dans ce contexte, en préconisant que des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés des personnes concernées soient prévues.

La recommandation de la Commission européenne relative à la boîte à outils insiste sur le fait qu'en l'absence de dispositions législatives dans un Etat membre, « il convient de spécifier clairement les finalités et les moyens du traitement des données, ainsi que les données à traiter et les personnes chargées du traitement. » Elle indique aussi que « toute ingérence dans ces droits devant être conforme aux exigences prévues par la loi, les législations des États membres qui établiraient ou autoriseraient des restrictions à l'exercice de certains droits fondamentaux devraient respecter les principes généraux du droit de l'Union énoncés à l'article 6 du traité sur l'Union européenne, les traditions constitutionnelles de ces États membres et leurs obligations en vertu du droit international. ».

---

[15] BATHO et BÉNISTI, Rapport d'information no 4113 sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, Assemblée nationale, 2011.

[16] Communication de la Commission du 16 avril 2002, Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données, C(2020) 2523 final.

Illustration des enjeux à l'aune d'un traitement de données de localisation utilisé hors crise sanitaire: la localisation des appels d'urgence

L'article L33-1 f) du code des postes et communications électroniques consacre le principe de l'acheminement gratuit des appels d'urgence[17] par les opérateurs qui doivent dans le même temps fournir aux services d'urgence l'information relative à la localisation de l'appelant.

L'article D98-5 dudit code fait peser sur les opérateurs des obligations relatives aux conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications et sur la sécurité et l'intégrité des réseaux et services. Ils doivent notamment mettre en œuvre *« une politique de sécurité relative au traitement des données à caractère personnel* » et prendre *« les mesures nécessaires garantissant que seules des personnes autorisées puissent avoir accès aux données à caractère personnel dans les cas prévus par des dispositions législatives et réglementaires »* et de veiller à ce que *« les données à caractère personnel stockées ou transmises soient protégées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites ».*

L'article D98-8 du même code précise les conditions de mise en œuvre, complété par une instruction relative à la mise en service de la plateforme de localisation des appels d'urgence[18] (PFLAU).

En pratique, les opérateurs organisent ce service au sein d'une association qui les regroupe et gère une plateforme mutualisée appelée PFLAU afin de permettre aux éditeurs de logiciels de régulation médicale d'appliquer des méthodes d'intégration standardisées.

Des mesures juridiques notamment au travers d'un dispositif contractuel permet d'obliger les parties prenantes, dont les établissements de santé sièges de SAMU qui reçoivent les appels d'urgence, à respecter des obligations de sécurité et de confidentialité des données personnelles dans la mise en œuvre de ce dispositif.

Cet exemple est intéressant dans la mesure où il illustre un cas dans lequel la prise en charge sanitaire des personnes, dans le contexte de l'urgence mais hors crise sanitaire, justifie la transmission des données de localisation sans droit d'opposition des personnes concernées mais dans le respect de règles répartissant les droits et obligations des acteurs publics et privés intervenant dans la chaîne de cette transmission de données, sous le contrôle du ministère chargé de la santé.

Une autre question interpelle sur la conformité de telles applications de tracing aux règles de protection des données personnelles : comment respecter les conditions qui encadrent l'exploitation des données de santé ?

---

[17] Art. D98-8 du code des postes et communications électroniques : « On entend par appels d'urgence les appels à destination des numéros d'appel d'urgence des services publics chargés :
. de la sauvegarde des vies humaines ;
. des interventions de police ;
. de la lutte contre l'incendie ;
. de l'urgence sociale. ».

[18] Instruction n°DGOS/R2/2015/184 du 2 juin 2015.

1.2 Licéité du traitement des données de santé à caractère personnel

Tout traitement de donnée de santé doit non seulement avoir une base légale mais en plus être justifié par une des exceptions au principe d'interdiction de traitement des données de santé. Le RGPD apporte des précisions dans ses considérants sur les conditions dans lesquelles il peut être dérogé au principe d'interdiction de traitement des données de santé à caractère personnel : « Certains types de traitement peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation (...)[19] ».

Les traitements envisagés pourraient donc collecter des données de santé révélant les personnes positives au COVID-19 « (...) pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel[20]. ».

Ces exigences telles que le secret professionnel sont importantes à rappeler tant qu'il n'est pas certain que les données qui seront collectées seront anonymisées.

Il est précisé dans les présentations des solutions relayées par la presse, et également par la Présidente de la CNIL, que les données de localisation seront « anonymisées ». Le terme « anonymisation » est cependant à préciser car il est souvent employé dans une approche vulgarisée et non dans son acception juridique et technique. Si les données sont anonymisées, elles sortent juridiquement du champ d'application du RGPD.

L'anonymisation est cependant difficile à atteindre à l'ère du Big Data et des fortes capacités technologiques à procéder au croisement des données et à la réidentification des personnes.

Rappelons en effet que l'anonymisation n'est juridiquement reconnue que s'il est techniquement démontré par le responsable de traitement que la ré-identification des personnes est impossible.

Pour répondre à cette exigence, les techniques d'anonymisation retenues doivent résister à trois risques essentiels :

- « L'individualisation, qui correspond à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données ;
- La corrélation, qui consiste dans la capacité de relier entre elles, au moins, deux enregistrements se rapportant à la même personne concernée ou à un groupe de personnes concernées (soit dans la même base de données, soit dans deux bases de données différentes). Si une attaque permet d'établir (par exemple, au moyen d'une analyse de corrélation) que deux enregistrements correspondent à un même groupe d'individus, mais ne permet pas d'isoler des individus au sein de ce groupe, la technique résiste à l'«individualisation», mais non à la corrélation ;

---

[19] Considérant 46 du RGPD : « Le traitement de données à caractère personnel devrait être également considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique. Le traitement de données à caractère personnel fondé sur l'intérêt vital d'une autre personne physique ne devrait en principe avoir lieu que lorsque le traitement ne peut manifestement pas être fondé sur une autre base juridique. **Certains types de traitement peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation**, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine. ».

[20] Art. 9-2 i RGPD.

• L'inférence, qui est la possibilité de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs[21]. ».

Les traitements à grande échelle reposant sur des données de localisation anonymisées pourraient être mis en œuvre sans le consentement des personnes concernées sous réserve de faire l'objet d'une Analyse d'Impact relative la Protection des Données (AIPD), qui au regard de l'envergure du traitement et de sa finalité devra à notre sens être déposée auprès de la CNIL pour consultation.

Cette AIPD devra apporter la preuve de la robustesse des techniques d'anonymisation mises en place et être régulièrement actualisée et éprouvée sous le contrôle des autorités compétentes dont la CNIL et l'ANSSI.

Dans le même sens, la Commission européenne recommande aux autorités publiques de vérifier « auprès des fournisseurs de données la méthode appliquée pour anonymiser les données et qu'elles procèdent à un contrôle de plausibilité sur l'emploi de cette méthode[22] ».

Quels que soient les choix qui seront opérés concernant la nécessité de recourir à un texte législatif ou réglementaire, les textes en vigueur et la récente recommandation de la Commission européenne imposent au gouvernement de mener une réflexion, même en temps de crise, sur les conditions permettant de garantir et de veiller à un équilibre entre la finalité du traitement poursuivi et les libertés fondamentales en jeu. Il lui appartient également d'identifier à qui sera confiée la lourde tâche de maintenir cet équilibre complexe et fragile et d'en déterminer quelle en sera la durée.

II. Identification du responsable de tels dispositifs

Ces dispositifs à grande échelle ayant une envergure nationale et le cas échéant européenne[23], il semble indéniable que la responsabilité de leur mise en œuvre relève de la compétence des autorités sanitaires ou d'organismes à but non lucratif agissant pour leur compte.

En France, la compétence de gestion des menaces sanitaires graves relève du ministre chargé de la santé qui « peut, par arrêté motivé, prescrire dans l'intérêt de la santé publique toute mesure proportionnée aux risques courus et appropriée aux circonstances de temps et de lieu afin de prévenir et de limiter les conséquences des menaces possibles sur la santé de la population[24]. ».

A noter qu'il était déjà précisé dans l'article L3131-1 du code de la santé publique (avant sa modification par la loi du 23 mars 2020) que « Le représentant de l'Etat dans le département et les personnes placées sous son autorité sont tenus de préserver la confidentialité des données recueillies à l'égard des tiers ».

La CNIL elle-même insiste sur la compétence des autorités sanitaires pour justifier que ces dernières puissent collecter des informations dont des données de santé à caractère personnel dans le cadre du COVID-19.

---

[21] Avis 05/2014 du G29 du 10 avril 2014 sur les Techniques d'anonymisation.

[22] Point 20 2) de la recommandation (UE) 2020/518.

[23] Extrait de la boîte à outils de la Commission européenne du 15 avril 2020 : « Public Health authorities should align on the protocol for data exchange of crossborder contact chains, namely about infected individuals that may have been in contact with individuals from another country. ».

[24] Article L3131-1 du code de la santé publique modifié par la loi n°2020-290 du 23 mars 2020 : « En cas de menace sanitaire grave appelant des mesures d'urgence, notamment en cas de menace d'épidémie, le ministre chargé de la santé peut, par arrêté motivé, prescrire dans l'intérêt de la santé publique toute mesure proportionnée aux risques courus et appropriée aux circonstances de temps et de lieu afin de prévenir et de limiter les conséquences des menaces possibles sur la santé de la population. ».

Sur son site Internet, la CNIL énonce ainsi que « **des données de santé peuvent être collectées par les autorités sanitaires**, qualifiées pour prendre les mesures adaptées à la situation. L'évaluation et la collecte des informations relatives aux symptômes du coronavirus et des informations sur les mouvements récents de certaines personnes relèvent de la responsabilité de ces autorités publiques[25]. ».

La Commission Européenne dans le document du 15 avril précise que « ces applications ne devraient être développées et mises en œuvre qu'en étroite coordination avec et sous la supervision des autorités de santé publique compétentes. Les autorités de santé publique coordonneront le processus de recherche des contacts locaux conformément aux directives internationales qui définissent quels contacts doivent être suivis et quelle doit être la gestion de ces contacts. ».

Qui au sein des autorités sanitaires ?

Au sein du ministère chargé de la santé a été mise en place en décembre 2019[26] la délégation du numérique en santé (DNS[27]). Cette nouvelle délégation travaille en lien avec les directions du ministère (direction générale de l'organisation des soins, direction de la sécurité sociale, direction du numérique, etc.) et autres acteurs concernés (en particulier la Caisse nationale d'assurance maladie) pour définir et mettre en œuvre la stratégie du numérique en santé, notamment sur le volet de la sécurité des systèmes d'information manipulant des données de santé.

La DNS, dont le bras armé est l'agence du numérique en santé (ANS), a notamment pour mission de proposer annuellement une feuille de route et d'identifier les moyens nécessaires à sa réalisation. La mise à disposition d'un bouquet de services (dont relève le dossier médical partagé, le dossier pharmaceutique, ou encore les messageries sécurisées de santé) au profit des professionnels de santé et d'un espace numérique de santé pour tout citoyen font d'ores et déjà partie de la feuille de route du numérique en santé présentée par la ministre chargée de la santé, le 25 avril 2019, dans le cadre de la stratégie « Ma Santé 2022 » portée par le gouvernement actuel. Il pourrait être envisagé de confier la tâche du développement d'une application COVID 19 à l'un de ces acteurs.

Conclusion

In fine, comme l'a rappelé la Présidente de la CNIL, Madame Marie-Laure Denis, lors de son audition devant la commission des lois de l'Assemblée nationale le 8 avril dernier, c'est l'évaluation 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[28].».

Cette crise fournit à l'Union européenne l'occasion de démontrer sa capacité à resserrer les rangs et produire les lignes directrices à suivre pour que chaque Etat membre mette en oeuvre les conditions garantissant l'équilibre entre santé publique et atteinte aux libertés fondamentales.

Le gouvernement français va devoir faire des choix conformes aux recommandations de la Commission européenne et veiller, à l'issue de la crise sanitaire, à prendre des mesures pour faire en sorte que, dès que le traitement n'est plus strictement nécessaire, celui-ci soit effectivement arrêté et

---

[25] https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles

[26] Décret du 20 décembre 2019.

[27] Elle succède à la délégation à la stratégie et aux systèmes d'information de santé (DSSIS).

[28] Audition commission des lois Assemblée nationale Propos liminaires de Madame Marie-Laure Denis, Présidente de la CNIL, 08 avril 2020, https://www.cnil.fr/sites/default/files/atoms/files/propos_liminaire-audition_commission_des_lois-assemblee_nationale-8-04-2020.pdf

que les données à caractère personnel concernées soient irréversiblement anonymisées ou à terme détruites.

Cependant, les données seront effectivement fortement utiles pour mener des recherches et améliorer les connaissances scientifiques. Il faut donc s'attendre à une finalité secondaire concomitante au tracing, celle de la recherche scientifique. A cet égard, la Commission européenne l'a anticipé et indique qu'il faudra tenir compte de l'avis de comités d'éthique et d'autorités chargées de la protection des données, pour apprécier leur valeur scientifique pour servir l'intérêt public. Si elle est validée par ces acteurs, la Commission considère que l'intérêt scientifique « l'emporte sur les conséquences pour les droits concernés, sous réserve de garanties appropriées ». Il y a fort à parier que ce soit le cas et il est donc recommandé que cette réutilisation soit dès lors prise en compte « by design » dans les applications de tracing notamment en veillant à la qualité de la donnée (structuration de la donnée, interopérabilité[29] des systèmes d'information) et au respect des droits des personnes concernées (information loyale et régulièrement mise à jour des personnes concernées).

Au regard de ces impératifs et en fonction de la base légale retenue, le droit d'opposition des citoyens pourrait être écarté par le texte encadrant lesdits traitements. Les exigences à mettre en œuvre en matière de protection de la vie privée et des données personnelles seront alors plus grandes et complexes dans leur déploiement et modalités de contrôle.

Une fois la crise passée, il apparaît important que les décideurs s'interrogent sur le rôle des institutions européennes et des autorités de contrôle nationales en matière de protection des données personnelles. La santé restant un domaine relevant prioritairement de la souveraineté nationale, ne faudrait-il pas envisager des prérogatives plus importantes au niveau des instances européennes ? Le respect des libertés individuelles étant un enjeu majeur pour conserver la confiance des citoyens dans le numérique mis en avant pour gérer la crise, les autorités nationales de protection des données personnelles ne devraient-elles pas se voir attribuer plus de moyens ?

Florence EON-JAGUIN
Avocate associée – Ex-directrice juridique
de l'Agence du Numérique en Santé (ANS)
Cabinet Withlaw - withlaw-avocats.fr

Nicolas SAMARCQ
CEO et fondateur de Lexagone
Créateur et animateur du groupe « données de santé » de l'AFCDP
Lexagone SAS - lexagone.fr

[29] Recommandation de la Commission du 2 juillet 2008 sur l'interopérabilité transfrontalière des systèmes de dossiers informatisés de santé.