Les libertés publiques face au traçage numérique

François Pellegrini, Hélène Skrzypniak

Les libertés publiques face au traçage numérique

François Pellegrini, professeur d'informatique à l'université de Bordeaux[1],
Hélène Skrzypniak, maître de conférences en droit privé à l'université de Bordeaux[2]
{francois.pellegrini | helene.skrzypniak}@u-bordeaux.fr

Résumé

La stratégie « tester / tracer / isoler » mise en place par le gouvernement français pour lutter contre l'épidémie de la covid-19 sur le territoire national repose sur un triptyque d'outils numériques : SI-DEP, Contact Covid et TousAntiCovid. La très grande masse de données collectées, et notamment de données sensibles, pose des problèmes inédits en matière de préservation des droits des personnes et des libertés publiques. Pour tenter d'y remédier, le législateur et le gouvernement ont mis en place un certain nombre de garde-fous, parfois eux aussi inédits : comité de suivi, etc. Pour autant, certaines faiblesses demeurent, notamment sur l'encadrement des accès à des stocks de données très identifiantes et sensibles.

Introduction

Le contrôle des épidémies est une activité aussi ancienne que l'organisation des sociétés humaines. Les regroupements des personnes au sein des cités et agglomérations, ainsi que les échanges commerciaux à longue distance entre ces groupes humains, ont favorisé la diffusion et la dissémination de maladies autrefois limitées à des zones géographiques restreintes. Face à l'arrivée d'épidémies mortelles, les prémices des stratégies dites « tester / tracer / isoler » ont été mises en place par les médecins et autorités de l'époque. Une fois des symptômes déclarés chez une personne, son noyau familial était confiné chez lui. L'expérience que les maladies pouvaient incuber silencieusement avant que les symptômes n'apparaissent a conduit à la mise en place des premières quarantaines, en particulier pour les voyageurs lointains[3]. Ce n'est qu'avec la présomption, puis la preuve, de la transmission des maladies par des agents pathogènes, qu'ont été développées des stratégies rationnelles de lutte contre les épidémies, posant les bases des premières politiques de santé publique en la matière[4].

Avec la généralisation des déplacements à grande distance et l'anonymat des contacts dans les grandes villes, la question du traçage des contacts a pris une ampleur nouvelle. Faute de pouvoir identifier et prévenir les personnes que l'on ne connaît pas, des méthodes de suivi rétrospectif[5,6] et de

1 Univ. Bordeaux, CNRS, Bordeaux INP, LaBRI, UMR 5800 et Inria, F-33400, Talence, France

2 Univ. Bordeaux, IRDAP, Institut de Droit des affaires et du patrimoine, F-33600, Pessac, France

3 P. Debré et J.-P. Gonzalez, Vie et mort des épidémies, Odile Jacob, Paris, 2013, 285 p., ISBN 978-2738129734

4 Voir notamment l'ouvrage fondateur : J. Snow, *On the mode of Communication of Cholera*, John Churchill, New Burlington Street, London, England, 1855, 139 p. Texte intégral disponible ici : https://www.ph.ucla.edu/epi/snow/snowbook.html

5 La création des « brigades sanitaires » destinées au suivi rétrospectif et à l'alerte des cas contacts de la covid-19 a été annoncée par M. Édouard Philippe, Premier ministre, lors de sa déclaration à l'Assemblée nationale, le 28 avril 2020, sur la stratégie nationale de déconfinement suite à l'épidémie de covid-19 à compter du 11 mai 2020. Voir : https://www.vie-publique.fr/discours/274200-edouard-philippe-28042020-plan-de-deconfinement-covid . Pour leur encadrement léglslatif, v. *infra* sur l'art. 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions.

6 Le suivi rétrospectif n'est efficace que si l'information peut être recueillie et exploitée rapidement. Il est cependant souvent lacunaire. Voir notamment le cas de la recherche infructueuse du « patient zéro » du SIDA aux États-Unis : M. Worobey, T. Watts, R. McKay et al., « 1970s and 'Patient 0' HIV-1 genomes

confinement de régions entières[7] ont été mises en œuvre. C'est afin de résoudre ce problème, essentiel pour contenir la propagation des grandes épidémies, qu'ont été proposées des solutions informatisées, dites de « traçage numérique ». Il s'agit ici d'utiliser les outils numériques – et notamment les ordiphones attachés aux personnes – afin de suivre le déplacement des populations et d'identifier les « cas contacts », c'est-à-dire les individus ayant été potentiellement infectés par un cas positif.

La massification de l'usage des technologies numériques au sein de la société conduit en effet à la génération de quantités considérables de traces. Celles-ci sont inhérentes à l'usage des outils eux-mêmes (comme par exemple le « bornage » des téléphones mobiles auprès des antennes fixes des réseaux de téléphonie, nécessaire à l'établissement des connexions), ou peuvent être générées de façon volontaire par les personnes utilisant une application dédiée (applications de suivi marketing, par exemple). Il était donc naturel d'imaginer mobiliser ces outils au sein de la mise en œuvre de politiques de santé publique.

L'exploitation des traces numériques des personnes à des fins de santé publique n'est pas nouvelle. Elle a notamment été utilisée pour lutter contre l'épidémie de SRAS en 2002–2003, du MERS en 2012–2013 ou encore contre celles d'Ebola[8]. Elle n'est pas, non plus, propre au domaine de la santé. La géolocalisation des personnes est, par exemple, utilisée en France pour lutter contre les violences conjugales, au moyen des « bracelets anti-rapprochement » mis en place par la loi du 28 décembre 2019 visant à agir contre les violences au sein de la famille[9]. Ces bracelets permettent de contrôler, grâce à un système de géolocalisation en temps réel, qu'un conjoint ou ex-conjoint violent ne se trouve pas à faible distance d'une personne à protéger[10].

Dans le domaine de la santé, la mise en œuvre de la chaîne d'actions « tester / tracer / isoler » à de vastes populations a nécessité la création d'un ensemble d'outils informatisés dédiés. Ces outils manipulent par nature des données extrêmement sensibles, car relatives non seulement à la santé des personnes, mais aussi à leurs relations intimes (y compris celles habituellement cachées). Ils constituent ainsi un risque pour le droit au secret des données à caractère personnel, le droit au respect de la vie privée ou encore le secret médical. Or, si la crise sanitaire justifie la mise en place d'instruments de traçage afin de lutter contre l'épidémie, leurs impacts sur ces droits et libertés fondamentaux ne peuvent être ignorés. La légalité de ces outils supposait que soit trouvé un équilibre entre l'impératif sanitaire de lutte contre la covid-19 et le respect de ces droits et libertés fondamentaux.

C'est ainsi que, en France, le législateur et le gouvernement ont mis en place un cadre juridique permettant la création de trois principaux traitements[11] :

---

illuminate early HIV/AIDS history in North America ». Nature 539, 98–101 (2016), https://doi.org/10.1038/nature19827

7 Le cas le plus emblématique pour la covid-19 ayant été le confinement de l'ensemble de la province chinoise du Hubeï, dont la capitale est Wuhan, du 23 janvier au 8 avril 2020

8 Rapport de l'*Assembla a di Corsica*, « Epidémie, numérique, libertés publiques », 15 mai 2020

9 Loi n° 2019-1480 du 28 décembre 2019 visant à agir contre les violences au sein de la famille, JORF n° 0302 du 29 décembre 2019

10 Les modalités de mise en œuvre du bracelet anti-rapprochement ont été précisées par le décret n° 2020-1161 du 23 septembre 2020 relatif à la mise en œuvre d'un dispositif électronique mobile anti-rapprochement, JORF n° 0233 du 24 septembre 2020. Le dispositif a reçu un avis favorable de la CNIL, délib. n° 2020-073 du 16 juillet 2020 portant avis sur un projet de décret relatif au bracelet anti-rapprochement (demande d'avis n° 20010563).

11 V. art. 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, JORF n° 0116 du 12 mai 2020, https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000041865258 ; décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, JORF n° 0117 du 13 mai 2020 ; décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid », JORF

- « SI-DEP », système informatisé de suivi des examens de dépistage, permettant de détecter les personnes contaminées (appelées « cas index » en épidémiologie, le terme « patient zéro » étant réservé au premier humain porteur d'une nouvelle maladie contagieuse[12]) ;
- « Contact Covid », système de suivi manuel des contacts identifiés à partir des cas index fournis par SI-DEP et des interviews des cas index ;
- « StopCovid », application mobile personnelle permettant d'alerter les personnes inconnues avec lesquelles une personne peut avoir été en contact, une fois cette personne reconnue comme positive à la covid-19. Cette application a été par la suite renommée « TousAntiCovid »[13], cette nouvelle version conduisant à coupler, au sein de la même application, plusieurs fonctionnalités différentes : la fonctionnalité initiale de suivi de contacts de StopCovid, un portail d'informations sur l'avancée de l'épidémie et un lien vers le formulaire de saisie d'attestations de déplacements numérisées. Ces deux dernières fonctionnalités ne posant pas de questions spécifiques, nous n'en parlerons pas ici. L'ajout à cette application d'un nouveau traitement de « cahier de rappel numérique », basé sur des QR codes à scanner par l'usager à l'entrée des lieux publics, est envisagé pour le tout début de l'année 2021[14]. Les modalités de ce traitement n'étant pas encore connues, nous n'en parlerons pas non plus dans la suite de ce texte.

L'objectif de cette contribution est de présenter comment l'outillage numérique de la stratégie « tester / tracer / isoler » a été encadré, sur les plans technique et juridique, afin de garantir une protection élevée des libertés fondamentales des personnes, en particulier quant à la protection de leurs données à caractère personnel et au secret médical. Un quatrième traitement de masse, « Vaccin Covid », a été récemment créé pour organiser la campagne de vaccination et éventuellement détecter les effets indésirables des vaccins contre la covid-19, créés et homologués dans l'urgence[15]. Nous ne l'aborderons pas ici, car il ne relève pas du domaine du traçage des personnes.

I. Conception fonctionnelle et technique de la chaîne des traitements

A. Les garanties techniques entourant SI-DEP et Contact Covid

Les applications SI-DEP et Contact Covid sont deux maillons essentiels de la chaîne « tester / tracer / isoler ».

---

n° 0131 du 30 mai 2020.

12 Le gouvernement a toutefois fait le choix de désigner sous le terme de « patient zéro » la personne « testée comme positive ou confirmée positive par l'établissement de santé qui a posé le diagnostic » (art. 1 du décret n° 2020-551 du 12 mai 2020, préc.).

13 La mise en place de cette nouvelle application n'a pas donné lieu à un nouveau texte et, à ce jour, le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid » est toujours en vigueur. Ses dispositions s'appliquent à la nouvelle version de « StopCovid » dénommée « TousAntiCovid ».

14 Avis du 15 décembre 2020 du comité de contrôle et de liaison covid-19 sur le projet de décret modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid », publié le 12 janvier 2021, https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/etat-des-lieux-et-actualites/article/avis-du-15-decembre-2020-sur-le-projet-de-decret-modifiant-le-decret-no2020-650

15 Décret n° 2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la covid- 19

La première, dont les terminaux sont déployés au sein des laboratoires d'analyse médicale, vise à centraliser de façon fiable les résultats des tests biologiques effectués. Dans le cas de résultats positifs, elle permet également aux laboratoires de fournir aux personnes infectées, maintenant considérées comme des « cas index », un code à usage unique. Ce code permettra aux cas index d'informer de leur état les contacts inconnus enregistrés par le biais de leur application personnelle StopCovid, qui devront alors se considérer comme des « cas contact » et agir en conséquence.

La deuxième, mise en œuvre au sein des équipes péri-médicales[16], permet à ces équipes d'effectuer les opérations d'identification manuelle des cas contacts connus, par interrogation des cas index sur leurs activités récentes et les personnes qu'elles ont fréquentées les jours précédents.

Tant SI-DEP que Contact Covid sont des applications centralisées. En effet, chacune d'entre elles est articulée autour d'une base de données unique, stockée de façon centralisée, et accédée au moyen d'interfaces permettant d'effectuer des requêtes d'interrogation et d'introduire des données nouvelles. L'architecture de ces applications étant centralisée, les seuls mécanismes pouvant être mis en œuvre pour limiter les accès consistent en des systèmes d'authentification des accédants, afin que seules les personnes ayant à en connaître puissent effectivement consulter les données de la base. Or, dans le cas de Contact Covid, le nombre de personnes accédantes est potentiellement très important. Qui plus est, parce que les contacts entre personnes peuvent avoir lieu au cours de déplacements, aucune restriction géographique ne peut être mise en place pour compartimenter les accès des personnes autorisées selon un critère géographique, ni selon aucun autre critère. Les possibilités de consultation des accédants ne peuvent donc pas être fonctionnellement limitées a priori ; elles ne peuvent que faire l'objet d'analyses *a posteriori* des journaux applicatifs pour détecter éventuellement des comportements d'utilisation de la base qui ne correspondraient pas aux missions des accédants.

Tant SI-DEP que Contact Covid contiennent des données extrêmement sensibles : l'une sur l'état sanitaire de chacune des personnes testées, notamment au cours du temps, et l'autre sur l'ensemble des personnes ayant été déclarées comme ayant été en contact avec les cas index, assorties d'informations relatives à la proximité de ces contacts. Plusieurs centaines de milliers de personnes sont fichées dans ces bases.

Pour autant, l'émoi populaire autour d'un fichage généralisé des personnes par le « gouvernement » n'a absolument pas concerné ces traitements, alors même que la base centralisée de Contact Covid contient des données d'identification nominatives détaillées et immédiatement exploitables. Il faut sans doute chercher cette différence de traitement médiatique dans le fait que les traitements SI-DEP et Contact Covid sont peu visibles en tant que tels et utilisés par des « médecins », considérés comme liés par le secret médical, alors que l'application StopCovid est directement placée au sein des ordiphones des personnes, qui relèvent du niveau de l'intime, et ne fait pas l'objet d'une supervision par des personnels médicaux en tant que tels[17].

B. Les garanties architecturales et techniques entourant l'application StopCovid / TousAntiCovid

1 Le suivi de contacts non connus

La problématique du traçage manuel de contacts, tel qu'effectué au sein du traitement Contact Covid, est qu'il ne concerne par nature que les personnes que l'on connaît et dont on peut fournir les coordonnées. Pouvoir alerter les personnes que l'on ne connaît pas suppose donc la collecte de

16 Car pas nécessairement constituées de professionnels de santé mais pilotées par eux

17 Notamment parce qu'aucune information nécessitant leur appréciation n'est directement accessible

données supplémentaires, par le biais de nouveaux traitements visant les interactions au sein des différents lieux publics.

Tel est le cas par exemple des « cahiers de rappel » mis en place dans les restaurants[18]. Ces bases de données à caractère personnel, majoritairement mises en œuvre sous forme papier, et dont les responsables de traitement sont les restaurateurs eux-mêmes, collectent sur la base du volontariat les coordonnées de tous les clients ayant fréquenté les établissements, ici encore de façon nominative et en clair. Elles nécessitent donc un encadrement adapté[19].

Ces traitements sectoriels ne peuvent cependant pas être généralisés à l'ensemble des lieux publics, et surtout ceux pour lesquels les débits de circulation sont essentiels et ne peuvent être freinés, comme par exemple les transports en commun. Un enregistrement manuel des personnes est inenvisageable, et poserait des problèmes de collecte et de conservation des données insurmontables.

Un autre moyen pour déterminer rapidement si des personnes ont pu être en contact, consiste à traiter *a posteriori* des masses de données de géolocalisation, telles que celles produites par les opérateurs téléphoniques lors du « bornage » des téléphones mobiles, afin de détecter les contacts entre personnes sur la base de leur proximité géographique pendant une période donnée. C'est ainsi qu'en Israël, l'ensemble des données de géolocalisation collectées par les opérateurs téléphoniques a été confié au service de sécurité intérieure, le Shin Beth, pour effectuer de tels calculs[20]. Outre que les résultats n'ont pas été pertinents (la précision de la localisation n'étant pas assez bonne et les « faux positifs » étant très nombreux, comme par exemple dans le cas des habitants de deux appartements mitoyens n'ayant aucun contact physique entre eux), le traitement centralisé de telles masses de données très sensibles et identifiantes peut être considéré comme largement disproportionné vis-à-vis du problème à résoudre[21].

2 Le suivi numérique de contacts pseudonymes

Les applications mobiles de la famille de StopCovid visent donc à pouvoir alerter a posteriori des personnes que l'on ne connaît pas, sans révéler d'informations directement identifiantes sur ces personnes auprès des tiers participant au traitement. Parce qu'il s'agira au final d'identifier des personnes, les informations les concernant, bien que chiffrées, seront toujours bien des données à caractère personnel, intégralement soumises aux lois « informatique & libertés ». Pour autant, leurs concepteurs ont mis en œuvre un ensemble de solutions techniques afin que les données échangées soient les moins identifiantes possibles. Le principe général de ces applications ayant été largement décrit par ailleurs, nous nous contenterons d'en résumer ici les caractéristiques saillantes.

Lorsqu'elles sont activées, ces applications échangent entre elles, via des technologies de communication de proximité (notamment la technologie Bluetooth, initialement conçue pour l'interconnexion à courte portée entre équipements et périphériques sans fil), des identifiants chiffrés uniques. Ces identifiants sont renouvelés régulièrement au cours du temps, afin qu'on ne puisse

18 Ces cahiers de rappel ont été mis en œuvre par arrêtés préfectoraux pris, dans les départements concernés, dans le courant du mois d'octobre 2020. Voir par exemple, pour le Rhône, l'AP n° 69-2020-10-09-003 du 9 octobre 2020 portant prescription de diverses mesures pour freiner l'épidémie de COVID-19 dans le département du Rhône et la Métropole de Lyon, https://www.rhone.gouv.fr/content/download/42944/237951/file/ap_mesures_diverses_octobre_2020_v7.pdf

19 Voir notamment les recommandations de la CNIL à ce sujet : https://www.cnil.fr/fr/covid-19-et-les-cahiers-de-rappel-les-recommandations-de-la-cnil [consulté le 31 déc. 2020]

20 Sur la mise en œuvre précipitée de ce dispositif et les contrôles mis en place par la suite, voir par exemple : T.O.I. Staff, « High Court says virus mass surveillance can't continue without Knesset oversight », Times of Israel, 19 mars 2020 [consulté le 31 déc. 2020]

21 Tel est le constat auquel est parvenu le comité de supervision de ce traitement. Voir par exemple : J. Maltz, « Israel to Scale Back Shin Bet Tracking of Coronavirus Patients », Haaretz, 16 déc. 2020

réidentifier une personne à travers un identifiant permanent. Chaque application conserve donc localement, au sein de l'ordiphone de son usager, une liste d'identifiants des personnes avec qui elle est restée en contact à courte distance. En l'absence de contamination, les données de contact plus anciennes qu'une durée de prescription prédéfinie sont supprimées, au fil du temps, de la mémoire des ordiphones.

Dans le cas de l'application StopCovid, qui met en œuvre le protocole ROBERT[22], si un usager est déclaré positif, il se voit remettre un code d'activation à usage unique par son laboratoire d'analyse. Ce code permettra d'activer, sur son application StopCovid, la transmission, de son ordiphone à un serveur centralisé, des identifiants de ses contacts récents. Ce serveur sert de relais passif pour répercuter l'alerte aux contacts en question. En effet, à intervalles réguliers, chaque application StopCovid active se connecte à ce serveur pour récupérer les identifiants pseudonymes des contacts détectés comme positifs. L'application qui reconnaît dans cette liste un identifiant qu'elle a généré par le passé sera ainsi à même d'alerter son usager qu'il a été en contact avec une personne ultérieurement testée comme positive. L'usager devra alors se rapprocher d'un professionnel de santé et/ou d'un laboratoire pour se faire tester à son tour.

Comme on le voit, le protocole ROBERT repose sur l'existence d'un serveur centralisé pour répercuter les alertes. Cependant, à la différence des traitements SI-DEP et Contact Covid, les données hébergées sur ce serveur sont extrêmement peu identifiantes. Ré-identifier ces données demanderait des efforts disproportionnés, et les personnes qui s'alarment à grand bruit de ce que le « gouvernement » pourrait faire avec elles semblent oublier que des données de géolocalisation et de contact des personnes, bien plus identifiantes (notamment concernant les appels passés et les SMS échangés), sont déjà présentes dans les bases de données centralisées des opérateurs téléphoniques, sans parler de celle de Contact Covid.

Pourtant, c'est sur la base de telles craintes que l'Allemagne a dû renoncer à la mise en œuvre d'un système , analogue à StopCovid, basé lui aussi sur le protocole ROBERT, pour choisir un protocole sans serveur central proposé par Apple et Google. Les préjugés anti-étatiques de technologues libertaires a au final conduit des États à renoncer à leur souveraineté sur le contrôle de jeux de données de santé considérables.

3 Problématiques d'usage

Comme on le voit, à la différence des bases de données des applications SI-DEP et surtout Contact Covid, qui doivent être centralisées de par la nature des opérations à réaliser, les architectes de l'application StopCovid ont fait en sorte de minimiser la centralisation des données : seuls sont présents sur le système central des identifiants pseudonymes, non rattachables directement à une personne. Un avantage de cette solution centralisée est que, dès le moment où le serveur est arrêté, le traitement prend fin de façon définitive. Les conditions d'arrêt du traitement sont donc garanties et facilement contrôlables.

L'une des questions débattues lors de la conception de ce dispositif concerne sa nécessité. En effet, faute de l'adoption du dispositif par une population suffisamment nombreuse, il a été envisagé que le traitement puisse ne pas être opérant en termes d'influence sur le cours de l'épidémie et que, à ce titre, faute de nécessité, il doive être abandonné. Au cours de la deuxième vague de l'épidémie, en octobre 2020, une campagne de promotion a été effectuée autour de l'application renommée « TousAntiCovid », qui a conduit à un nombre de téléchargements bien plus significatif que lors de la première vague de mars 2020. Pour autant, l'efficacité du dispositif ne pourra être mesurée qu'à l'aune

22 Équipes Inria PRIVATICS et Fraunhofer AISEC, « ROBERT: ROBust and pricacy-presERving proximity Tracing », v1.1, 31 mai 2020, https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_1.pdf

de son nombre d'activations et du nombre de personnes qu'elle aura permis d'alerter, qui ont effectivement été dans une situation à risque et ont pris les mesures adéquates.

Les premiers retours d'usage ont également conduit à s'interroger sur le repositionnement de l'usage de l'application. Alors qu'elle avait majoritairement été pensée pour le cas des transports en commun[23], la généralisation du port du masque dans ceux-ci a conduit à ce qu'ils ne soient plus des lieux majeurs de propagation, à l'exception des endroits où il est enlevé et où les contacts sur des surfaces souillés sont fréquents[24]. De fait, elle semble majoritairement utile dans les lieux de convivialité où le masque n'est pas porté (période des repas, moments de convivialité, etc.).

Ces doutes entourant l'efficacité de cet instrument de lutte contre l'épidémie n'est pas sans conséquence juridique. Plus précisément, la question se pose de savoir si un outil numérique dont le risque sur la protection de données à caractère personnel est avéré, alors que son utilité dans la lutte contre l'épidémie reste hypothétique, peut être considéré comme un outil légitime et donc licite. La réponse à la question ne peut être donnée sans une analyse approfondie des différentes garanties juridiques entourant la mise en œuvre de ce traitement.

II. **L'encadrement juridique des techniques de traitement**

Si la crise sanitaire justifie la mise en place d'instruments de traçage afin de lutter contre l'épidémie, leurs effets sur les droits et libertés fondamentaux des individus – que sont notamment la liberté d'aller et venir, le droit au respect de la vie privée ou la confidentialité des données à caractère personnel et sensibles – ne sauraient être ignorés. Les protections constitutionnelle et conventionnelle de ces droits[25] exigent que les atteintes qui leur seraient portées soient non seulement justifiées par un intérêt légitime mais aussi nécessaires et proportionnées à l'objectif poursuivi, à savoir, ici, l'impératif sanitaire[26].

Afin de répondre à ces exigences, le gouvernement et le législateur français ont strictement encadré la mise en place de l'application TousAnticovid (A) et des traitements SI-DEP et Contact Covid (B). L'analyse des garanties encadrant ces instruments de traçage permettra d'apprécier si l'exigence de proportionnalité est respectée.

---

23 Y. Shen, C. Li, H. Dong et al., « Community Outbreak Investigation of SARS-CoV-2 Transmission Among Bus Riders in Eastern China », JAMA Intern Med. 2020;180(12):1665-1671, doi:10.1001/jamainternmed.2020.5225

24 C'est par exemple le cas des toilettes des avions de ligne. Voir à ce sujet : S. Bae, H. Shin, H. Koo et al., « Asymptomatic Transmission of SARS-CoV-2 on Evacuation Flight », Emerging Infectious Diseases 2020;26(11):2705-2708, doi:10.3201/eid2611.203353

25 La valeur constitutionnelle de la liberté d'aller et venir a été reconnue par le Conseil constitutionnel dans sa décision du 12 juillet 1979 (Cons. const., 12 juill. 1979, n° 79-107 DC). Cette liberté se rattache également à l'article 4 de la DDHC ainsi qu'à l'article 5 de la CESDH. Le droit au respect de la vie privée est, quant à lui, rattaché à l'article 2 de la DDHC (Cons. const., 23 juill. 1999, n° 99-416 DC, cons. 45. V. aussi : Cons. const., 25 mars 2014, n° 2014-693, cons. 10). Il est également consacré par l'article 8 de la CESDH et 7 de la Charte des droits fondamentaux de l'U.E. Enfin, la protection des données à caractère personnel et des données sensibles résulte des articles 6 et 9 du règlement (UE) 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 (RGPD) ; v. aussi la décision du Conseil constitutionnel du 22 mars 2012 : « la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée ; que par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionné à cet objectif » (cons. const., 22 mars 2012, n° 2012-652 DC).

26 Voir : L. Cluzel-Métayer, « La datasurveillance de la Covid-19 », RDSS, 2020, p. 918.

A. Les garanties encadrant TousAntiCovid

Les garanties sont à la fois d'ordre technique (1) et juridique (2).

1 Les garanties techniques

Quelques exemples étrangers. Nombreux sont les pays à avoir adopté des applications numériques dans la lutte contre la covid-19[27]. Si les objectifs sont communs, les techniques utilisées sont plurielles et leurs impacts sur les droits et libertés des individus sont d'inégale importance. L'exemple de la Corée du Sud est à cet égard très révélateur des dérives qui peuvent en résulter. La stratégie mise en œuvre par le gouvernement sud-coréen pour tenter d'endiguer l'épidémie repose sur la géolocalisation des personnes infectées et de leurs contacts, en agréant un ensemble de sources de données numériques très diverses : pour identifier ces personnes, le gouvernement traque les téléphones portables, exploite les historiques des cartes bancaires et des cartes de transports, et visionne les vidéos des caméras de surveillance. Des SMS révélant leur nationalité, âge, lieu de travail, localisation actuelle sont ensuite envoyés aux personnes dont l'historique des données cellulaires indique qu'elles se trouvaient à proximité d'une personne infectée. Les données collectées sont rendues publiques et alimentent automatiquement une carte virtuelle mise à jour en temps réel afin d'identifier les lieux où circulent les personnes positives. La presse internationale s'est alors fait écho des dérives que cette surveillance a engendrées[28], des personnes identifiées positives – parfois sur la base de fausses informations – étant victimes de véritables campagnes de dénigrement[29].

La technique de la géolocalisation a également été développée à Taïwan : l'installation d'un logiciel de traçage sur les téléphones des personnes testées positives est imposée afin de contrôler le respect de leur mise en quarantaine. Si la personne s'éloigne de son domicile ou éteint son téléphone, elle est contactée dans les 15 minutes par les services de police qui peuvent prononcer des amendes s'ils constatent que le confinement n'est pas respecté. Les contrevenants risquent également la publication de leur identité[30].

La Pologne a adopté une stratégie assez similaire : l'installation d'une application téléphonique de géolocalisation est imposée aux personnes infectées ainsi qu'à celles revenant de l'étranger. Cette application envoie de manière aléatoire – et plusieurs fois par jour – des SMS leur demandant de se géolocaliser au moyen d'un auto-portrait (« *selfie* »). La personne a vingt minutes pour envoyer sa photographie. En l'absence de réponse, l'application prévient les forces de l'ordre, qui sont alors chargées de vérifier si la personne concernée respecte la quarantaine et, le cas échéant, peuvent la sanctionner d'une amende pouvant aller de 500 zlotys (110 euros) à 5000 zlotys (1100 euros).

---

27 Pour les exemples étrangers : v. F. Mattatia « Suivi des populations pour lutter contre une épidémie et protection des données personnelles », JCP A, 4 mai 2020, 2136. V. aussi : A. Cherif, « Tracking du Covid-19 : comment font les autres pays », La Tribune, 9 avr. 2020 ; M. Mahjoubi, « Traçage des données mobiles dans la lutte contre le Covid-19. Analyse des potentiels et des limites », note parlementaire, version 1.0 du 6 avr. 2001 : https://medium.com/@mounir/traçage-des-données-mobiles-dans-la-lutte-contre-le-covid-19-e718b1e15dfb [consulté le 3 déc. 2020].

28 Lesquelles ont amené les autorités coréennes à revoir les modalités de traçage numérique : aujourd'hui le gouvernement ne révèle plus l'âge, le sexe, la nationalité ou le lieu de travail d'un patient. Il ne révèle pas non plus les noms des lieux que le patient a récemment visités si toutes les personnes rencontrées ont déjà été identifiées. En outre, il supprime de la vue du public toute information qu'il divulgue au bout de deux semaines.

29 Pour une illustration : C. Sang-Hun, « In South Korea, Covid-19 Comes With Another Risk: Online Bullies », The New-york Times, 19 sept. 2020, consultable sur : https://www.nytimes.com/2020/09/19/world/asia/south-korea-covid-19-online-bullying.html [consulté le 3 déc. 2020].

30 M. Mahjoubi, « Traçage des données mobiles dans la lutte contre le Covid-19. Analyse des potentiels et des limites », préc., p. 37.

En France. Ces différentes techniques, particulièrement attentatoires à la liberté d'aller et venir, au respect à la vie privée et au secret médical, ont été écartées par le gouvernement français.

Géolocalisation vs Bluetooth. Ainsi, comme il l'a été précisé[31], l'application TousAntiCovid – comme son aînée StopCovid – repose sur la technologie Bluetooth. L'usage qui est fait de cette technologie s'avère beaucoup moins intrusif et plus respectueux des droits et libertés fondamentaux des individus, pour plusieurs raisons. En premier lieu, la technologie Bluetooth ne vise pas à localiser les personnes. Il ne s'agit pas, en effet, de cartographier le déplacement des individus mais de retracer les contacts entre les appareils à proximité équipés de l'application. Autrement dit, il ne s'agit pas d'identifier les personnes mais de localiser les proximités relatives des équipements mobiles, les uns par rapport aux autres, sans enregistrer les lieux fréquentés. Ce faisant, elle se révèle être beaucoup plus respectueuse de la vie privée que la technologie de géolocalisation.

Confidentialité. Ensuite, la technologie Bluetooth enregistre ces « contacts » entre les appareils via des codes pseudonymes, qui changent régulièrement[32]. La France a ainsi fait le choix d'une technologie visant à préserver la confidentialité de l'identité des personnes utilisant son application. Le gouvernement français garantit qu'il est impossible d'identifier les utilisateurs de l'application, ni même le lieu et le moment où ils ont croisé un autre appareil ayant activé l'application[33] : d'une part le téléchargement et l'utilisation de l'application ne requièrent pas la fourniture de données directement identifiantes (telles que nom, numéro de téléphone, adresse électronique, etc.) et, d'autre part, l'application téléchargée, et donc son utilisateur, n'est identifiée par le serveur central que par un pseudonyme, c'est-à-dire une donnée non identifiante par elle-même. Contrairement à ce qui a été mis en place dans d'autres pays, aucune personne ni aucune organisation n'a donc accès à une liste de personnes qui se déclarent positives[34] ou à une liste des interactions sociales entre les utilisateurs[35]. La technique choisie se veut ainsi plus respectueuse du droit à la vie privée et du secret médical.

Volontariat. Enfin, le traçage numérique par Bluetooth n'est pas automatique : l'application TousAntiCovid doit être activée par les titulaires du téléphone portable. Contrairement à certains pays qui ont opté pour une application obligatoire (Chine, Corée du Sud, Israël ou Pologne), la stratégie française repose sur le volontariat : les personnes sont libres d'installer et de désinstaller l'application à tout moment[36]. En outre, aucune conséquence négative n'est attachée à l'absence de téléchargement ou d'utilisation de l'application[37]. Rien de comparable donc aux techniques développées en Pologne ou à Taïwan : pas de contrôle des services de police et, a fortiori, pas de sanction en cas de non utilisation de l'application. L'application ne vient donc pas restreindre la liberté d'aller et venir des citoyens.

La technologie choisie par le gouvernement français offre ainsi plusieurs garanties pour les droits et libertés fondamentaux des individus. La protection de ces droits ne peut toutefois être effective que si le droit vient strictement encadrer ces techniques afin, notamment, d'en prévenir tout détournement. Les garanties techniques ont ainsi été consolidées par des garanties juridiques.

2 Les garanties juridiques

La mise en place de l'application StopCovid par le gouvernement s'est accompagnée d'un dialogue avec les instances nationales, au premier rang desquelles le Parlement et la Commission nationale de

31 V. *supra*.

32 Les identifiants pseudonymes (« crypto-identifiants ») sont supprimés au bout de 15 jours (v. « TousAntiCovid », dossier de presse, 22 octobre 2020, p. 13).

33 « TousAntiCovid », dossier de presse, préc., p. 12-1.

34 Celles-ci sont enregistrées dans SI-DEP

35 « TousAntiCovid », dossier de presse, préc., p. 13

36 Art. 1, III, du décret n° 2020-650 du 29 mai 2020, préc.

37 V. sur ce point : CNIL, délib. n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » (demande d'avis n° 20006919).

l'informatique et des libertés (CNIL). L'Assemblée nationale et le Sénat se sont prononcés, le 27 mai 2020, en faveur du déploiement de l'application. La CNIL a quant à elle été saisie pour avis à deux reprises sur le projet de décret relatif au traitement de données StopCovid[38]. Après avoir constaté que les préconisations formulées dans sa délibération du 24 avril[39] avaient été prises en compte, et sous réserve de quelques observations, la Commission a estimé que l'application pouvait être légitimement déployée pour accompagner la gestion de la crise sanitaire[40]. Plus précisément, après avoir relevé les différentes garanties prises par le gouvernement pour respecter les législations européenne et française relatives à la protection des données à caractère personnel, la CNIL a considéré que les atteintes portées au droit au respect de vie privée étaient proportionnées à l'objectif poursuivi[41].

Sans revenir sur l'ensemble des exigences contenues dans la législation relative à la protection des données à caractère personnel[42], nous relèverons ici les principales garanties juridiques prises par le gouvernement français afin de concilier impératifs sanitaires et respect des droits et libertés des individus. Celles-ci sont contenues dans le décret du 20 mai 2020 relatif au traitement de données dénommé « StopCovid »[43].

Licéité des traitements. Ces garanties concernent, d'abord, la licéité des traitements. Pour être licite, un traitement doit reposer sur l'un des fondements énumérés par les articles 6 et 9 du RGPD[44]. S'agissant de l'application téléphonique, deux fondements étaient envisageables : le consentement – puisque l'application repose sur le volontariat – et l'intérêt public – dans la mesure où l'application vise à lutter contre l'épidémie de la covid-19[45]. Possible, le consentement n'était toutefois pas le fondement le plus opportun[46]. Pour être efficace, les textes européens et français exigent en effet que celui-ci soit éclairé, libre, spécifique et univoque[47]. Or, dans un contexte de risque sanitaire, il n'est pas du tout certain que ces conditions puissent être réunies (en raison notamment de la peur de la maladie, des pressions sociales ou bien encore de comportements abusifs que pourraient adopter certaines personnes en exigeant, par exemple, l'installation de l'application pour accéder à un lieu[48]). Il faut donc saluer le choix du gouvernement français d'avoir choisi, pour base légale du traitement, l'existence d'un intérêt public[49]. Comme le relève la CNIL, « *la lutte contre l'épidémie de COVID-19 constitue une mission d'intérêt général dont la poursuite incombe en premier lieu aux autorités publiques. En conséquence,* […] *la mission d'intérêt public* […] *constitue la base légale la plus appropriée pour le développement par l'autorité publique de l'application StopCovid* […]. *Le choix de cette base légale permet en outre de concilier en toute sécurité juridique le caractère volontaire de l'utilisation de cette*

38 CNIL, délib. n° 2020-046 du 24 avril 2020, préc. et délib. n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » (demande d'avis n° 20008032).

39 CNIL, délib. n° 2020-046 du 24 avril 2020, préc.

40 CNIL, délib. n° 2020-056 du 25 mai 2020, préc. Voir aussi : CNIL, 15 juill. 2020, déc. MED-2020-015, mettant en demeure le ministère des solidarités et de la santé.

41 S'agissant de la version 2.0 de « TousAntiCovid », v. CNIL, communiqué de presse, 23 octobre 2020.

42 Contenue dans le RGPD et la loi française « Informatique et Liberté » (LIL) (loi n° 78-17 « informatique & libertés » du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

43 Décret n° 2020-650 du 29 mai 2020, préc. Comme indiqué précédemment, la mise en place de la nouvelle application « TousAntiCovid » n'a pas donné lieu à l'adoption d'un nouveau texte et le décret du 29 mai 2020 est aujourd'hui toujours en vigueur.

44 Repris aux art. 5 et 6 de la LIL

45 V. en ce sens : CNIL, délib. n° 2020-046 du 24 avril 2020, préc.

46 *Id.*

47 Art. 4 du RGPD, repris à l'art. 5 de la LIL

48 N. Metallinos, « Covid-19 : l'état d'urgence sanitaire à l'épreuve du droit de la protection des données à caractère personnel », CCC, n° 5, mai 2020, étude 9.

49 Art. 1er, I du décret n° 2020-650 du 29 mai 2020, préc.

application et les éventuelles incitations des pouvoirs publics à une telle utilisation, afin de promouvoir son utilisation la plus large possible[50] ».

Limitation des finalités. Une deuxième garantie concerne, ensuite, les finalités des traitements. Il s'agit d'un principe cardinal de la protection des données à caractère personnel[51], en vertu duquel ces données ne peuvent être utilisées que pour un objectif précis et déterminé à l'avance. Toute utilisation non conforme à ces finalités est interdite. Les finalités de l'application déployée par le gouvernement français sont contenues à l'article 1er du décret. Les trois principales sont :

- informer la personne qui utilise l'application des risques qu'elle ait été contaminée ;
- sensibiliser sur les symptômes de la maladie et les gestes barrières à adopter ;
- orienter les personnes vers les services compétents pour leur prise en charge[52].

Contrairement à certaines applications étrangères, TousAntiCovid n'a pas pour finalité de localiser, de surveiller et/ou de punir. Sa finalité essentielle est d'informer ou, plus précisément, d'informer, de prévenir et de conseiller. L'application ne saurait, par exemple, être utilisée pour surveiller le respect des mesures de confinement, de réaliser un suivi du nombre de personnes infectées ou bien encore, d'identifier les zones dans lesquelles ces personnes se sont déplacées. À cet égard, l'application développée par les autorités françaises apparait moins attentatoire aux droits et libertés fondamentaux des individus que certains instruments développés à l'étranger[53].

Limitation de la durée du traitement. Les autorités françaises ont également pris soin de limiter la durée d'exploitation et de conservation des données à caractère personnel. TousAntiCovid n'a pas vocation à persister à la fin de l'épidémie et prendra fin dans un délai ne pouvant excéder six mois après la cessation de l'état d'urgence sanitaire[54]. En outre, les données de l'historique de proximité enregistrées par l'application sur le téléphone mobile ne sont conservées que quinze jours à compter de leur enregistrement par cette application. Précisons, à cet égard, que les études scientifiques tendent à démontrer qu'au-delà de quinze jours, le risque de contagiosité par contact avec une personne contrôlée positive est quasi nul. En choisissant de limiter la durée de conservation à quinze jours, le gouvernement limite ainsi cette durée à ce qui est strictement nécessaire à l'objectif poursuivi.

Droit à l'information. Des garanties ont aussi été apportées pour assurer le droit à l'information. Lors du téléchargement de l'application, les personnes sont ainsi informées des principales caractéristiques du traitement et de leurs droits[55]. Ce dispositif est complété par des informations publiées sur le site du ministère des solidarités et de la santé[56].

Utilité de l'application. Ces quelques points relevés permettent de comprendre comment la France a tenté de concilier impératifs sanitaires et respect des droits et libertés fondamentaux afin de répondre à l'exigence de proportionnalité. Si la démarche adoptée peut être saluée, il reste à l'éprouver. Or, comme le rappellent les lignes directrices du Contrôleur européen des données à caractère personnel (EDPS)[57], la proportionnalité d'une mesure qui limite des droits fondamentaux s'apprécie, non

50 CNIL, délib. n° 2020-046 du 24 avril 2020, préc.

51 *Id.*

52 La dernière : adapter, le cas échéant, la définition des paramètres de l'application permettant d'identifier les contacts à risque de contamination grâce à l'utilisation de données statistiques anonymes au niveau national

53 V. *supra*

54 Art. 3 du décret n° 2020-650, 29 mai 2020, préc.

55 Art. 4 du décret n° 2020-650, 29 mai 2020, préc.

56 Voir : https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/tousanticovid

57 EDPS, « Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux », 19 déc. 2019

seulement, au regard des garanties prises pour limiter les atteintes à ces droits mais, aussi, en considération des bénéfices sociaux qui découlent de la mesure. En d'autres mots, pour être proportionnée, une mesure doit être nécessaire ; pour être nécessaire, elle doit être utile et, pour être utile, la mesure doit être efficace. Or on peut, aujourd'hui encore, légitimement douter de l'efficacité de l'application. À cela, plusieurs raisons. D'abord parce que, pour être efficace, une application de traçage doit être utilisée par un nombre important de la population estimé, selon les sources, entre 20 % et 60 %[58]. Il est peu de dire que ce taux peine à être atteint : l'application StopCovid n'avait été téléchargée que par à peine plus de 3 % de la population. Si TousAntiCovid semble avoir eu davantage de succès, seuls 10 % de la population avaient téléchargé la nouvelle version de l'application au 1er novembre dernier[59]. Malgré les modifications effectuées par le gouvernement[60] et la communication autour de l'application, cet outil suscite toujours la méfiance ou, à tout le moins, l'indifférence de la population. Ensuite, au-delà du taux de téléchargement, l'efficacité de l'application dépend des profils des personnes qui la téléchargent. Plus précisément, une efficacité optimale suppose que ce soient les personnes les plus exposées qui adhérent en nombre à l'application, c'est-à-dire les personnes les plus âgées et les jeunes enfants porteurs asymptomatiques[61]. Or on pourrait penser que, précisément, ce public est peut-être le moins à même à se tourner vers l'outil numérique. Enfin, on ne peut ignorer les imperfections de fonctionnement de l'application, et notamment l'absence de détection malgré la proximité[62]. Dans ce contexte, et comme l'ont rappelé la CNIL et la Commission nationale consultative des droits de l'homme (CNCDH), il est essentiel d'effectuer des évaluations régulières de l'efficacité de l'application[63]. Aujourd'hui, s'agissant de l'application TousAntiCovid, ces évaluations se font toujours attendre[64]. Elles ont en revanche été mises en place pour les traitements SI-DEP et Contact-Covid[65], autres instruments de traçage numérique dont la mise en œuvre a été entourée de garanties visant à préserver les droits et libertés fondamentaux.

B. **Les garanties entourant SI-DEP et Contact-Covid**

Ces garanties sont issues de la législation relative à la protection des données à caractère personnel (1) et de dispositions spécifiques visant à protéger le secret des informations (2).

---

58 M. Mahjoubi, « Traçage des données mobiles dans la lutte contre le Covid-19. Analyse des potentiels et des limites », préc., p. 33. Le chiffre le plus souvent cité reste toutefois celui de 60 % avancé par le réseau européen eHealth (eHealth Network, 15 avr. 2020, Mobile applications to support contact tracing).

59 Déclaration de Cédric O à l'AFP le mardi 3 novembre 2020 (sur cet entretien, voir notamment, Sciences et Avenir avec AFP , « TousAntiCovid : Cédric O vise au moins 15 millions de téléchargements d'ici un mois », Sciences et Avenir, 3 nov. 2020, consultable sur : https://www.sciencesetavenir.fr/sante/e-sante/tousanticovid-cedric-o-vise-au-moins-15-millions-de-telechargements-d-ici-un-mois_148911 [consulté le 3 déc. 2020].

60 V. *supra*.

61 L. Pailler, « StopCovid : la santé publique au prix de nos libertés ? – Brèves observations sur l'application de traçage numérique », D., 2020, p. 935

62 *Id.*

63 V. en ce sens : CNIL, délib. n° 2020-056 du 25 mai 2020, préc.

64 CNIL, délibération n° 2021-004 du 14 janvier 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19, §§ 34–43, https://www.cnil.fr/sites/default/files/atoms/files/deliberation-n2021-004.pdf

65 La loi du 11 mai 2020 a en effet porté création d'un comité de contrôle et de liaison covid 19 (CCL Covid) chargé, notamment, par des audits réguliers, d'évaluer, grâce aux retours d'expérience des équipes sanitaires de terrain, l'apport réel des outils numériques à leur action et de déterminer s'ils sont, ou pas, de nature à faire une différence significative dans le traitement de l'épidémie. Il a également pour mission de vérifier, tout au long de ces opérations, le respect des garanties entourant le secret médical et la protection des données à caractère personnel (v. particulièrement l'art. 11, VIII, de la loi n° 2020-546 du 11 mai 2020, préc.).

1 Les garanties issues de la législation relative à la protection des données à caractère personnel

Licéité du traitement. Comme il l'a été souligné[66], les traitements SI-DEP et Contact Covid exploitent des données d'une extrême sensibilité. Sont en effet traitées non seulement des données révélant l'identité des personnes (nom, prénom, sexe, date et lieux de naissance, etc.) ainsi que leur vie privée (données relatives aux relations – contacts – de la personne concernée, aux lieux qu'elle a fréquenté : régions, états, établissements, ou encore aux personnes avec qui elle cohabite) mais aussi, celles relatives à leur santé : caractère positif du test covid, date de prélèvement, existence de symptômes, date de leur apparition, situation médicale de la personne (hospitalisée ou à domicile), identité du médecin traitant, etc. Ces dernières données correspondent à ce que la législation relative aux données à caractère personnel qualifie de « données sensibles ». Le traitement de telles données est en principe interdit[67]. Toutefois, le règlement européen et la législation française prévoient des exceptions à cette interdiction, au titre desquelles figurent des « motifs d'intérêt public dans le domaine de la santé publique[68] ». Comme pour l'application TousAntiCovid, c'est donc l'existence d'un intérêt public – la lutte contre la covid-19 – qui fonde la licéité de ces deux traitements de traçage[69]. L'existence d'un fondement licite ne saurait toutefois suffire à conclure en la licéité de ces fichiers.

Finalité du traitement. Comme tous traitements de données à caractère personnel, la licéité de SI-DEP et Contact Covid supposait, aussi, que soient respectés les différents principes de la législation sur les données à caractère personnel. À cet effet, la loi du 11 mai 2020[70] portant création de ces systèmes d'information, puis son décret d'application du 12 mai 2020[71], ont précisé les conditions d'exploitation des données traitées. Afin de garantir une utilisation strictement proportionnée au but poursuivi, ce sont d'abord les finalités du traitement qui ont été précisées[72]. Le traitement de ces données ne peut avoir que pour seules fins :

- l'identification des personnes infectées et des personnes présentant un risque d'infection ;
- l'orientation des personnes infectées et des personnes susceptibles de l'être vers des prescriptions médicales d'isolement ;
- la surveillance épidémiologique aux niveaux national et local ; ainsi que
- la recherche sur le virus et les moyens de lutter contre sa propagation.

Durée de conservation des données. Le gouvernement a également pris soin de limiter la durée de conservation des données traitées, laquelle a été fixée à trois mois après leur collecte[73]. Compte tenu des difficultés qu'il peut y avoir à recueillir des informations auprès de la personne « cas index », qui peut se montrer rétive à divulguer certaines données, ce délai ne paraît pas déraisonnable. Il semble correspondre au cycle d'une enquête sanitaire[74]. Une réserve peut toutefois être émise à l'égard des données relatives aux personnes considérées « à risque » : lorsque le dépistage s'avère finalement négatif, la conservation de ces données pendant trois mois ne paraît pas proportionnée aux finalités

66 V. *supra*.

67 Art. 9, §1 RGPD et art. 6 I de la LIL

68 Art. 9, §2, i) RGPD et art. 6 II de la LIL

69 Art. 1er, I du décret n° 2020-551 du 12 mai 2020, préc.

70 Loi n° 2020-546 du 11 mai 2020, préc.

71 Décret n° 2020-551 du 12 mai 2020, préc.

72 Art. 11, II de la loi n° 2020-546 du 11 mai 2020, préc.

73 Art. 5, I et 11, I du décret n° 2020-551 du 12 mai 2020, préc.

74 L. Pailler, « La surveillance sanitaire de la population aux fins de lutter contre la covid-19 (commentaire de l'article 11 de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions) », Lettre juridique, n° 827, 11 juin 2020

poursuivies. Sans intérêt pour la lutte contre l'épidémie, ces données devraient être effacées immédiatement[75]. Notons qu'au délai de trois mois s'ajoute une date butoir : la durée de conservation ne peut excéder six mois à compter de la fin de l'état d'urgence[76].

Pour autant, il existe une tentation croissante, dans les milieux scientifiques, de conserver, à des fins de recherche, le stock de données extrêmement précieux que constitue l'analyse jour par jour de la propagation d'une épidémie de cette nature[77]. Cette volonté s'oppose frontalement aux limites fixées par le législateur. Une solution respectueuse de la législation relative aux données à caractère personnel consisterait à anonymiser ces données. Se poseraient alors les questions de la pertinence, pour l'analyse épidémiologique, de données ayant subi un traitement visant à les rendre effectivement anonymes[78], ainsi que du risque résiduel de réidentification attaché à des données décrivant des réseaux relationnels corrélés à une information géographique résiduelle.

Droit des personnes concernées. Afin de se conformer aux exigences de la législation sur les données à caractère personnel, les textes français reconnaissent également le droit à l'information des personnes dont les données sont traitées[79], le droit d'accès à celles-ci et le droit de rectification[80]. En revanche, des limites sont apportées au droit d'opposition et d'effacement. Ainsi, s'il est prévu que les personnes à risque de contamination peuvent s'opposer au traitement des données recueillies auprès du cas index et obtenir l'effacement des données les concernant, cette possibilité est exclue « lorsque prévalent les intérêts impérieux de santé publique[81] ». Or, en pratique, cette circonstance pourra souvent être retenue, notamment lorsque le risque que ces personnes aient été contaminées est élevé[82]. Ces limites ne constituent toutefois pas une atteinte à la législation sur les données à caractère personnel, qui prévoit expressément la possibilité de telles dérogations aux droits des individus[83].

Minimisation des données. Si les instruments français de lutte contre la covid-19 apparaissent ainsi conformes à la législation relative à la protection des données à caractère personnel, une réserve peut toutefois être émise à l'égard du principe de minimisation des données. Prévu à l'article 5.1.c du RGPD, ce principe exige que le traitement ne porte que sur des données « strictement adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités » poursuivies. Or, on peut légitimement s'interroger sur la pertinence de certaines informations recueillies et conservées dans SI-DEP et Contact Covid. Outre les informations relatives aux personnes testées négatives, déjà évoquées, on citera, à titre d'exemple, celles concernant la spécialité du médecin à l'origine de l'inscription sur les registres[84] : peu utile pour la lutte contre l'épidémie, une telle information peut en effet, selon la spécialité du médecin, révéler des informations sur une pathologie particulière de la personne concernée et porter ainsi une atteinte injustifiée à sa vie privée[85]. Pour cette raison, elle ne

75 *Id.* Également en ce sens : N. Metallinos, « Contact Covid et SI-DEP – Quel encadrement pour les outils numériques du dépistage Covid-19 », CCC, juillet 2020, comm. 59.

76 Art. 11, I, al. 1 de la loi n° 2020-546 du 11 mai 2020, préc.

77 En témoigne la tension entre le conseil national de l'Ordre des médecins et le conseil scientifique auprès du gouvernement, au sujet de l'allongement de la durée de conservation des données à des fins de recherche épidémiologique. Voir : https://www.conseil-national.medecin.fr/publications/communiques-presse/fichiers-sidep-amelipro

78 Et non pas seulement pseudonymes

79 Voir notamment l'art. 12 du décret n° 2020-551 du 12 mai 2020, préc.

80 Voir l'art. 7, II et l'art. 13 du décret n° 2020-551 du 12 mai 2020, préc.

81 Art. 7, I, al. 1er du décret n° 2020-551 du 12 mai 2020, préc.

82 L. Pailler, « La surveillance sanitaire de la population aux fins de lutter contre la covid-19 (commentaire de l'article 11 de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions) », art. préc.

83 Art. 21 du RGPD et art. 56 de la LIL

84 Art. 2, II, 1°, d) du décret n° 2020-551 du 12 mai 2020, préc.

85 Voir N. Metallinos, « Contact Covid et SI-DEP – Quel encadrement pour les outils numériques du dépistage Covid-19 », art. préc.

devrait pas figurer dans les registres. Lors de l'examen du projet de décret relatif à ces deux traitements, la CNIL avait d'ailleurs fait état de ses réserves et inquiétudes face à l'ampleur et à la grande sensibilité de certaines données, demandant aux autorités françaises de faire preuve de plus de rigueur dans la définition des données traitées[86]. Ces observations n'ont cependant pas été intégralement suivies.

D'autres inquiétudes concernent le secret des informations recueillies. Des garanties ont certes été posées ; elles ne sont toutefois pas pleinement satisfaisantes.

2 Les garanties protégeant le secret des informations

Volontariat. Au titre de ces garanties, il faut d'abord relever que le traitement Contact Covid repose sur le volontariat : le patient peut refuser de révéler l'identité des personnes avec lesquelles il a été en contact, tandis que la personne contactée peut refuser de participer à l'enquête. Pas plus, les médecins ne sont-ils obligés à révéler ces informations, et aucune conséquence négative, telles que des sanctions professionnelles, la condamnation à une amende ou à l'isolement, n'est attachée au refus de participer aux enquêtes sanitaires. Qui plus est, dans le cas où le cas index aura accepté de révéler les personnes avec lesquelles il était en contact, il peut exiger que son identité ne soit pas communiquée aux personnes susceptibles d'être à risque de contamination. Ces règles ont le mérite de protéger non seulement le droit au respect de la vie privée mais aussi le secret médical.

Obligations. En revanche, une telle liberté de choix n'existe pas s'agissant du traitement SI-DEP. Les médecins, les responsables des services et des laboratoires de biologie médicale ont en effet l'obligation d'inscrire sur le registre les informations permettant d'identifier la personne infectée. En outre, elles ont l'obligation de transmettre les cas positifs à la covid-19 à l'autorité sanitaire. Le cas échéant, cette inscription peut intervenir sans le consentement du patient. La mise en place de SI-DEP a ainsi amené le législateur à consacrer de nouvelles dérogations au secret médical. L'obligation faite au personnel de santé de transmettre à l'autorité sanitaire des informations relatives à une maladie n'est pas inédite : elle est prévue à l'article L. 3113-1 du code de la santé publique pour une série de maladies telles que le choléra, la peste, la rage ou encore la rougeole[87]. L'obligation de transmission des informations n'est donc pas une dérogation nouvelle au secret médical mais l'extension d'une pratique existante à une nouvelle maladie : la covid-19[88].

En revanche, l'obligation de transmettre les informations permettant l'identification de la personne infectée constitue une brèche inédite au secret médical[89]. Celle-ci est d'autant plus remarquable que les informations ainsi révélés sont partagées par un nombre conséquent de personnes.

Partage des informations. L'article 11, III de la loi du 11 mai 2020[90] énumère ainsi, à la Prévert, les personnes autorisées à prendre connaissances de ces informations sensibles : le service de santé des armées, les communautés professionnelles territoriales de santé, les établissements de santé, sociaux et médico-sociaux, les équipes de soins primaires mentionnées à l'article L. 1411-11-1 du code de la santé publique, les maisons de santé, les centres de santé, les services de santé au travail mentionnés

86 Délibération n° 2020-051 du 8 mai 2020 portant avis sur un projet de décret relatif aux systèmes d'information mentionnés à l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire

87 Art. D. 3113-6 du code de la santé publique

88 L. Pailler, « La surveillance sanitaire de la population aux fins de lutter contre la covid-19 (commentaire de l'article 11 de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions) », art. préc.

89 Le système de traitement mis en place pour lutter contre la Covid-19 se distingue ici des autres fichiers nationaux relatifs à des maladies infectieuses : certes la déclaration est aussi obligatoire mais, d'une part, elle ne concerne que le cas index et non les cas contacts et, d'autre part et surtout, les données relatives aux patients infectées font l'objet d'une anonymisation qui rend l'identification de la personne impossible.

90 Loi n° 2020-546 du 11 mai 2020, préc.

à l'article L. 4622-1 du code du travail et les médecins prenant en charge les personnes concernées, les pharmaciens, etc. À ces acteurs s'ajoutent les agents des « brigades sanitaires », c'est-à-dire l'ensemble des personnes mobilisées par le gouvernement pour tracer les personnes testées positives à la covid-19 et leurs contacts[91].Certes, le législateur soumet l'ensemble de ces personnes au secret professionnel[92] ; il n'en reste pas moins que la multiplication des catégories de personnes manipulant ces informations sensibles accroît, par la même occasion, les risques de divulgation. Ces risques sont d'autant plus importants que les mesures la sécurité entourant ces fichiers apparaissent lacunaires.

Sécurité des traitements. Comme l'indique la CNIL[93], l'encadrement des accès à des données de santé est essentiel au regard des exigences prévues par la législation relative aux données à caractère personnel. L'article 9.2.g du RGPD, relatif aux traitements de données sensibles justifiés pour des motifs d'intérêt public importants, exige, notamment, que lesdits traitements respectent « l'essence du droit à la protection des données » et prévoient « des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ». À cet égard, la CNIL a rappelé que les mesures de traçabilité constituent l'« une des pierres angulaires[94] » de la sécurité des traitements de données. Elle préconise, plus précisément, la mise en place d'une matrice d'habilitation définissant les droits d'accès en lecture et en écriture selon les profils des personnels habilités. Selon la Commission, il s'agit d'« un élément central de la sécurité du traitement ». Or, le ministère de la santé a indiqué à la CNIL « qu'en raison des contraintes opérationnelles rencontrées », il n'entend pas paramétrer les dispositifs de façon à limiter les accès aux seuls besoins des utilisateurs[95]. Cette posture apparaît très critiquable au regard des exigences de confidentialité de ces données sensibles. Autre lacune relevée par la CNIL : Contact Covid est accessible avec de simples identifiants et mots de passe. Ces modalités d'authentification des personnes n'apparaissent pas conformes aux préconisations de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S)[96] et aux recommandations de la Commission concernant l'accès à des données de santé. En présence de données aussi sensibles, et dont le partage est aussi large, de telles lacunes sont difficilement acceptables.

On le constate, malgré les garanties que le législateur et le gouvernement ont mises en place, les instruments de traçage recèlent de véritables risques pour les droits et libertés fondamentaux des individus. Ces risques sont en réalité inhérents à ces outils numériques. Ainsi, si, dans l'abstrait, l'encadrement de ces traitements permet de considérer que les ingérences dans les droits et libertés des personnes concernées sont nécessaires et proportionnés à la lutte contre la covid-19[97], les conditions concrètes de leur mise en œuvre ne sont pas pleinement satisfaisantes. Dans sa dernière délibération, en date du 14 janvier 2021[98], la CNIL a ainsi relevé un certain nombre de mauvaises pratiques et fait plusieurs recommandations pour y remédier. Il faut espérer que celles-ci seront suivies d'effets. Il s'agit d'une condition indispensable au maintien de l'équilibre – fragile – entre respect des droits et libertés fondamentaux et exigences sanitaires.

---

91 Art. 3, I du décret n° 2020-551 du 12 mai 2020, préc.

92 Art. 11, III de la loi n° 2020-546 du 11 mai 2020, préc.

93 CNIL, délib. n° 2020-051 du 8 mai 2020, préc.

94 *Id.*, p. 12

95 *Id.*, p. 8

96 Depuis 2012, la PGSSI-S assemble des référentiels d'exigences, des guides de bonnes pratiques et propose un cadre commun de niveau de sécurité des SI du secteur de la santé.

97 L. Pailler, « La surveillance sanitaire de la population aux fins de lutter contre la covid-19 (commentaire de l'article 11 de la loi du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions) », art. préc.

98 CNIL, délibération n° 2021-004 du 14 janvier 2021, préc.