COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE
POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ

COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE

Enjeux d'éthique concernant des outils numériques pour le déconfinement

Jeudi 14 mai 2020

Réponse à la saisine de Messieurs

Olivier Véran

Ministre des Solidarités et de la Santé

Cédric O

Secrétaire d'État chargé du numérique

66, rue de Bellechasse 75007 Paris – 01 42 75 66 42
www.ccne.fr – contact@comite-ethique.fr

Table des matières

1. Introduction

Le Comité national pilote d'éthique du numérique (CNPEN) a été saisi le 30 avril 2020 par le ministre des Solidarités et de la Santé et le secrétaire d'État chargé du Numérique au sujet *des questionnements éthiques liés à la conception, à la mise en œuvre et aux usages d'outils numériques* dans les différentes phases du déconfinement, en particulier en ce qui concerne *le respect de la vie privée et des libertés publiques* et les *effets structurants* que pourraient induire ces outils à moyen et long terme, notamment sur les citoyens et la société.

La réponse à cette saisine que constitue le présent avis a été élaborée dans des délais très courts compte tenu du contexte de rapidité dans lequel doivent être mises en œuvre les décisions du gouvernement. Cependant, le CNPEN avait mis en place dès le 19 mars un groupe de travail spécifique pour effectuer une veille relative aux questions éthiques soulevées par les usages du numérique dans la situation de crise créée par l'épidémie. Ceci a donné lieu à la publication le 7 avril d'un premier bulletin de *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë*, avec en particulier un accent mis sur le *suivi des personnes par des outils numériques*, puis d'un communiqué le 29 avril relatif aux *Enjeux d'éthique du numérique du suivi épidémiologique en sortie de confinement*. Le présent avis s'appuie en particulier sur ces deux documents. Il a aussi été élaboré en coopération avec le CCNE pour les sciences de la vie et de la santé qui, pour sa part a été saisi le 4 mai par le Conseil scientifique Covid-19 sur les enjeux éthiques du déconfinement.

La situation de crise amorcée par la pandémie de la Covid-19 a conduit à une amplification inédite des usages du numérique ainsi qu'à la création de nouveaux outils. Ils sont devenus essentiels à tous les niveaux, d'un point de vue sociétal, économique et sanitaire, entraînant également une exacerbation de leurs enjeux éthiques.

Sur le plan sanitaire, les outils numériques peuvent notamment contribuer à identifier les transmissions possibles entre des porteurs du virus et des personnes avec lesquelles ils ont été en situation de proximité, ceci afin de faciliter une alerte rapide des porteurs potentiels. Au niveau collectif, ces outils permettent en particulier d'étudier et de modéliser l'évolution de l'épidémie, d'identifier d'éventuels nouveaux foyers, et de contribuer à l'évaluation de l'immunité de la population dans un contexte où les connaissances relatives à la pandémie sont encore partielles. Ils prennent tout leur sens et montrent leur utilité dans le cadre d'un dispositif global qui inclut les gestes barrières, les tests, le diagnostic, l'isolement, l'accompagnement, le traitement et l'hospitalisation.

Toutefois la conception, la mise en œuvre et l'utilisation de ces outils dans le contexte de la pandémie mettent en tension d'une part, les impératifs sanitaires avec le respect des libertés fondamentales et la protection de la vie privée et des données personnelles, et d'autre part, l'urgence de leur déploiement avec les questions de souveraineté, d'expérimentation, de contrôle, et d'information loyale du public.

Dans cet avis, nous présentons d'abord un panorama d'outils numériques qui pourraient être utilisés dans les différentes phases de déconfinement et au-delà. Nous nous focalisons ensuite sur l'analyse spécifique des enjeux d'éthique relatifs aux outils numériques de traçage des personnes susceptibles de propager le virus. Comme nous l'explicitons synthétiquement en annexe, ce traçage peut être réalisé de plusieurs manières, complémentaires, en s'appuyant à la fois sur des applications de traçage numérique et des équipes sanitaires qui recueillent et échangent des informations portant sur des personnes et sur leurs contacts sociaux. Nous analysons donc les questions d'éthique relatives aux applications de traçage numérique – et tout particulièrement celles qui reposent sur l'utilisation de techniques de type Bluetooth – puis celles qui sont relatives à leur utilisation combinée avec les systèmes d'information SI-DEP et Contact Covid prévus en soutien des équipes sanitaires, tels qu'ils sont en particulier décrits dans le Décret n° 2020-551 du 12 mai 2020[1]. De ces analyses nous tirons des points d'attention et des recommandations qui visent à éclairer la conception, la mise en œuvre et les usages de ces outils numériques.

---

[1] 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

2. Les outils numériques dans le cadre de la crise Covid-19

La stratégie du gouvernement pour le déconfinement repose sur trois piliers : protéger, tester, isoler. Ces trois éléments nécessitent la mise en œuvre de moyens spécifiques à court, moyen et long termes, incluant des outils numériques variés. À titre d'exemples, des outils numériques pourraient aider à protéger les usagers des transports en commun en les informant sur l'affluence en temps réel ; à identifier les personnes à tester suite à leur contact rapproché avec des personnes infectées ; et permettre aux personnes susceptibles d'être infectées de continuer à communiquer ou d'être suivies médicalement tout en étant isolées. Par ailleurs, les outils numériques peuvent aussi contribuer, en particulier dans le cadre d'actions de recherche, à anticiper les évolutions et les conséquences de cette pandémie et à mieux prévenir de futures crises sanitaires.

Le tableau suivant présente des outils numériques qui sont utilisés, ou auxquels il serait possible de recourir, pendant les différentes phases de déconfinement et au-delà, en indiquant leurs usages en vue de **protéger (P), tester (T), isoler (I) et anticiper (A).**

Outils numériques	**P**	**T**	**I**	**A**
Applications de traçage de contacts		x	x	x
Systèmes d'information pour le recensement et le traçage de contacts par les équipes sanitaires (SI-DEP et Contact Covid)		x	x	x
Outils facilitant l'information des équipes sanitaires et leur interaction avec les personnes à tester ou à suivre		x	x	
Outils d'auto-diagnostic, outils pour la médecine de ville, télémédecine	x	x	x	
Outils d'information du public et d'expression citoyenne	x	x	x	x
Outils de modélisation pour le suivi et la prédiction de la propagation de l'épidémie	x			x
Outils d'analyse statistique de données et de prospective à long terme pour la recherche	x			x
Outils d'analyse et de visualisation pour l'imagerie médicale		x		x
Outils pour la recherche médicale (aide à la recherche de médicaments, de vaccins, etc.)	x			x
Robots pour les analyses médicales		x		

Outils numériques	P	T	I	A
Robots pour l'aide à la désinfection	x			
Robots d'aide à la livraison de repas, de médicaments	x			
Outils d'information et d'orientation des usagers des transports	x			
Contrôle automatique des autorisations d'accès aux transports	x			
Vidéosurveillance du respect des gestes barrières dans les lieux et transports publics	x			
Fabrication automatisée de produits critiques (masques, écrans protecteurs, embouts de respirateur, etc.)	x			
Outils permettant d'organiser et de poursuivre les activités économiques, sociales, éducatives et culturelles (télétravail, téléenseignement, etc.)	x		x	

Les outils numériques contribuent ainsi à concilier des objectifs sanitaires, économiques et sociaux. Toutefois leur conception, leur mise en œuvre et leur utilisation font apparaître certaines tensions éthiques. Elles sont exposées dans la suite de ce document pour ce qui concerne les applications et les systèmes d'information relatifs au traçage des contacts.

3. Enjeux éthiques des applications de traçage numérique pour le suivi épidémiologique

Introduction aux applications de traçage sur smartphone

En phase de déconfinement et plus généralement en cours d'épidémie due à une maladie particulièrement contagieuse, la réduction des chaînes de contamination est de toute première importance. Elle repose d'abord sur la prévention et la protection, notamment les gestes barrières. Elle repose aussi sur l'identification des personnes réellement infectées et donc sur des tests médicaux, et enfin, sur la prise de contact la plus rapide et efficace possible avec les personnes potentiellement contaminées. Le nombre moyen de personnes auxquelles un sujet malade transmet la maladie, appelé facteur de transmission R_0, doit être inférieur à 1 pour que l'épidémie régresse. La valeur de ce facteur de transmission résulte de plusieurs paramètres, incluant la prévention et la protection mais aussi la rapidité de l'identification des personnes potentiellement contaminées. Cette identification dépend des situations de proximité entre deux personnes dont l'une est porteuse du virus et symptomatique. Ce « traçage des contacts » peut s'effectuer soit par l'intervention directe de personnes habilitées, soit en utilisant des applications numériques permettant notamment de détecter et de mémoriser automatiquement la proximité de deux smartphones que l'on suppose être portés par deux personnes (voir annexe 1), ou encore en combinant les deux approches.

Les applications de traçage numérique constituent donc à la fois une opportunité de contribution à la diminution du facteur R_0 et un risque de fuite des données personnelles des personnes qui utilisent ces applications. Pour réduire ce risque, des protocoles préservant l'anonymat et renforçant la sécurité des applications de traçage ont été conçus, dont la majorité appartient à deux grandes classes de protocoles qualifiés de « centralisés » et « décentralisés ». L'annexe 1 en expose les grands principes selon que les informations sont principalement gérées par un serveur centralisé ou qu'elles sont principalement gérées localement sur les smartphones.

En termes de cybersécurité, les risques concernent les données stockées aussi bien sur les smartphones que sur un serveur centralisé, ainsi que les communications entre les smartphones ou entre ceux-ci et un serveur central. La circulation des données sur les réseaux, dont internet, présente également un risque de fuite.

La mise en œuvre d'une application de traçage nécessite aussi de prendre en compte les éléments de son architecture matérielle et logicielle. Le serveur central et les réseaux devront ainsi être configurés de sorte à garantir une disponibilité et une continuité de service assurant les objectifs de sécurité et de fiabilité de l'application de traçage. Ils pourraient aussi intégrer des outils d'apprentissage d'informations relatives à la durée et à l'intensité des contacts.

L'analyse des tensions éthiques induites par les choix réalisés par les concepteurs d'une application de traçage numérique nécessite d'examiner synthétiquement les techniques actuellement disponibles.

La détection de proximité peut s'effectuer en utilisant soit des techniques de localisation utilisant le GPS, le wifi ou le réseau cellulaire, voire une combinaison de plusieurs d'entre elles, soit en utilisant un protocole de communication locale tel que Bluetooth Low Energy (BLE) entre deux dispositifs numériques. La plupart des protocoles proposés en Europe utilisent cette dernière solution, éventuellement combinée à de la localisation. Faire ce choix technique nécessite d'être attentif à ses conséquences en termes de fiabilité de la détection de proximité. Notamment, l'ignorance d'un contexte protecteur des contacts (par exemple, la présence d'un mur ou la proximité entre un malade et un médecin portant un équipement de protection) augmenterait le nombre de faux positifs. Par ailleurs, l'utilisation du Bluetooth BLE par une application de traçage numérique est sujette, pour certaines marques de smartphones, à des restrictions d'utilisation de la part du fabricant et du propriétaire du système d'exploitation. Ces derniers sont alors en position de décider de favoriser, ou non, la mise en place de cette application de traçage.

Analyse des tensions éthiques propres aux applications de traçage numérique

Les choix techniques et sociétaux opérés lors de la conception, la mise en œuvre et l'utilisation d'une application de traçage sont susceptibles d'exacerber des tensions entre différents principes et valeurs éthiques qu'il s'agit de recenser, d'analyser, et qui nécessitent des arbitrages.

Choix et usages d'une application

En automatisant le traçage des contacts, en particulier dans l'espace public et dans les transports, une application sur smartphone permet d'accélérer le signalement des nouveaux cas de personnes potentiellement contaminées. Elle contribue ainsi à la réduction du facteur R_0 et au ralentissement de la propagation de l'épidémie, grâce à un confinement et un suivi médical proposés à ces personnes. À plus long terme, elle peut également contribuer au développement d'études statistiques ou de modèles prédictifs à l'échelle nationale ou internationale. On peut en outre envisager l'utilisation d'applications similaires dans le cas d'autres crises sanitaires (par exemple les épidémies de grippe saisonnière). Cependant, on pourrait craindre la pérennisation de tels dispositifs de traçage des contacts dans la population, leur usage à d'autres fins que la gestion des crises sanitaires, voire l'accoutumance de la population au recours à de telles mesures légitimées par le contexte de la pandémie actuelle.

Pour prévenir le risque d'atteinte à la vie privée que constituerait une telle pérennisation, des garanties devront être données quant au caractère temporaire et proportionné de l'utilisation des données recueillies par l'application. Le déclenchement d'une application, sa suspension ou l'ajustement de ses paramètres (mesure de la distance, niveau d'alerte, …) devront être décidés par les autorités publiques compétentes sur la base de l'évolution sanitaire de la situation.
Le critère de proportionnalité implique que les applications minimisent le volume des données collectées et garantissent l'anonymat, afin que ni l'identité de la personne contaminée ni celle de ses contacts ne puissent être accessibles, y compris à l'application elle-même. Cependant, cette anonymisation peut rendre plus difficile la nécessaire prise en charge de la personne contaminée par les professionnels du soin.
En outre, si de tels outils de traçage se révélaient insuffisamment efficaces, d'autres techniques telles que la géolocalisation pourraient être envisagées, avec des risques éventuels d'atteinte à la vie privée.

Pour pouvoir maîtriser toutes ces dimensions, les autorités publiques doivent être en mesure de faire leurs propres choix d'application. Il est particulièrement important de recourir à des dispositifs numériques de traçage conçus et déployés avec un souci d'interopérabilité, notamment européenne et internationale. Le déploiement d'applications nationales non interopérables et la multiplication d'applications proposées par des acteurs privés et/ou internationaux susceptibles d'établir des listes de contacts différentes pourraient limiter l'efficacité du traçage numérique. Cette multiplicité pourrait également conduire à une limitation de la liberté de circulation, en particulier d'un pays à un autre.

Recommandations :

3.1 Viser l'interopérabilité des applications de traçage, au niveau européen, voire international, dans le respect du RGPD2.

3.2 Veiller à la non-discrimination des personnes qui n'utilisent pas les applications volontaires de traçage, y compris dans le contexte de déplacements en Europe et à l'international.

3.3 Choisir des moyens techniques de détection de proximité qui favorisent la protection de la vie privée et des données personnelles.

3.4 Donner la possibilité aux autorités publiques compétentes d'activer ou de désactiver les applications de traçage qui ont été volontairement installées par leurs utilisateurs en en informant ces derniers.

3.5 Donner à tout moment la possibilité aux utilisateurs qui ont volontairement installé une application de traçage sur leur smartphone de la désactiver temporairement ou de la désinstaller définitivement.

3.6 Prévoir la désactivation automatique des applications de traçage après l'expiration de leur délai légal ainsi que les moyens d'en rendre compte publiquement.

Transparence

L'efficacité d'une application dépend en particulier de l'adhésion de la population à son utilisation, qui repose sur la confiance accordée à l'ensemble du dispositif de prévention et de soin mis en place. Cette adhésion ne peut se faire sans une information régulière, librement accessible, loyale et transparente. Cette information doit concerner la conception et le code de l'application, y compris leurs auteurs, la finalité de l'application ainsi que l'exploitation des données qu'elle collecte, afin que chacun puisse être assuré qu'elle ne fait que ce qu'elle est censée faire. En particulier, la publication du code source de l'application est une condition élémentaire de transparence. La loyauté de l'information suppose en outre que les termes employés pour décrire les aspects techniques ne soient pas ambigus et apportent effectivement des éléments de compréhension pour tous. Par exemple, l'utilisation des termes « centralisé » et « décentralisé », qui sont chargés de sens implicites, peut brouiller la compréhension des dispositifs techniques.
Cette information, complétée de données relatives notamment au taux de diffusion des applications dans la population et de résultats d'audits réalisés au niveau national par des tiers de confiance, doit permettre de nourrir les contrôles institutionnels et démocratiques ainsi que les débats publics.

Recommandations :

3.7 Garantir l'information régulière, librement accessible, loyale et transparente sur la conception et le code des applications de traçage, leur finalité ainsi que sur l'exploitation des données qu'elles collectent. Veiller à ce que cette information comporte des éléments de compréhension pour tous.

2 Règlement général européen sur la protection des données

3.8 Prévoir un cadre législatif et réglementaire afin d'organiser les contrôles institutionnels et démocratiques des applications de traçage et faciliter le débat public.

3.9 Soumettre les applications de traçage à l'audit par des tiers de confiance.

Consentement

Une application de traçage est conçue comme un dispositif permettant d'informer chacun d'un contact avec une personne contaminée et ainsi d'être acteur de sa propre santé et de celle des autres. Le caractère volontaire et non contraignant de son adoption peut néanmoins réduire son efficacité. Il faut aussi tenir compte du possible manque de réactivité de ces personnes ou de leur possible réticence à se soumettre à un test médical. Malgré l'impact potentiellement négatif du volontariat sur l'efficacité du dispositif, celui-ci est indispensable et doit se fonder sur un consentement libre et éclairé. Cela suppose que le refus de consentir n'expose pas la personne à des conséquences négatives, quelle qu'en soit la nature.
Ce consentement repose sur la transparence et suppose la mise en place préalable d'une politique d'information et d'acculturation des citoyens, malgré le contexte d'urgence. Cette information doit en particulier exposer les implications et les limites de l'application, en particulier pour prévenir l'illusion d'être « protégé » par son smartphone et les comportements à risque qui en résulteraient. Par ailleurs, le consentement à l'utilisation de l'application et la responsabilisation des personnes mineures ou vulnérables doivent être questionnés et faire l'objet d'un accompagnement et d'une information adaptée. Une attention particulière doit être accordée aux personnes en situation de précarité sociale, ne maîtrisant pas la langue française ou à celles qui ne pourraient pas accéder à la technologie.

Si des politiques incitatives pour l'utilisation d'une application de traçage numérique étaient mises en place, elles devraient exclure tout système susceptible d'induire des biais et de provoquer la discrimination de certaines populations, en particulier les systèmes de récompense aux usagers.

On ne saurait écarter l'éventualité de la stigmatisation ou de formes éventuelles de pression envers les personnes qui n'utilisent pas d'application, notamment par les employeurs ou les assureurs. La possession d'un smartphone et l'utilisation d'une application ne peuvent aucunement constituer des conditions d'accès à des services ou des ressources, en particulier l'accès au soin et à l'emploi. Des mesures spécifiques et gratuites doivent être prévues pour les personnes qui ne disposent pas de smartphone mais qui souhaitent participer au dispositif de traçage.

Recommandations :

3.10 Rendre disponibles et accessibles à tous les publics des informations claires et loyales relatives aux objectifs, au fonctionnement et aux limites des applications de traçage. Ces informations devront être fournies sur un site de référence national en ligne, par téléphone, sous forme de documents imprimés et sous forme radio et télé diffusée.

3.11 Déployer une pédagogie large et adaptée à toute la population sur les enjeux techniques et sociétaux de ces applications de traçage.

3.12 Garantir le consentement libre et éclairé tout comme la possibilité de ne pas consentir et ceci sans pression, contrainte, ni mise en place de système de récompense.

3.13 Permettre aux personnes de revenir à tout moment sur leur engagement et permettre l'effacement des données collectées.

3.14 Prévoir des mesures spécifiques et gratuites pour les personnes ne disposant pas de smartphone et souhaitant participer au dispositif de traçage.

Point d'attention :

3.a L'utilisation d'une application de traçage doit faire l'objet d'une codécision entre les titulaires de l'autorité parentale et le mineur de moins de 15 ans.

Expérimentation

Pour pouvoir disposer d'une application de traçage robuste et fonctionnelle, il est nécessaire de l'expérimenter au préalable et ce, en toute transparence. Pour cela, il est préférable d'agir d'abord à petite échelle, sur un échantillon de population, avant le déploiement général. Une validation insuffisante ou une expérimentation précipitée de l'application pourraient nuire à son efficacité. Par exemple, cela pourrait induire un débordement inutile du système de tests médicaux par des faux positifs (notifiés mais testés négativement par la suite). Si une application de traçage connaissait des dysfonctionnements ou se révélait inefficace, la responsabilité et la réputation des entités l'ayant commanditée, conçue ou mise en œuvre pourraient être engagées, affectant ainsi la confiance dans la gestion de la crise.

Ces expérimentations se heurtent à deux limites : d'une part le choix et la taille de l'échantillon, et d'autre part le temps nécessaire pour les conduire. Si une application est déployée, il serait donc souhaitable, pour pouvoir la corriger et l'améliorer, de poursuivre les expérimentations durant le déploiement afin de prendre en compte leurs résultats en même temps que les retours d'expérience de ce déploiement.

Recommandation :

3.15 Si une application de traçage est déployée, mener des expérimentations même si sa mise en service doit intervenir rapidement. Poursuivre ces expérimentations en parallèle de son déploiement.

4. Enjeux éthiques des interactions entre le traçage numérique et les systèmes d'information SI-DEP et Contact Covid pour le recensement et le traçage de contacts

La stratégie nationale de sortie du confinement s'appuie actuellement sur deux outils numériques[3] : SI-DEP (Système d'Information de Dépistage), un collecteur automatisé de résultats de tests diagnostiques (RT-PCR) qui permet de recenser les cas positifs, et Contact Covid, une base de données spécifique qui enregistre les patients testés positifs ainsi que leurs contacts rapprochés à des fins de suivi.[4]
Nous analysons ici les liens avérés ou potentiels entre les trois systèmes d'information que constituent SI-DEP, Contact Covid et une éventuelle application de traçage numérique. Notons d'abord que des données de SI-DEP, dont l'identité des personnes testées positives, sont traitées par Contact Covid[5]. Notons aussi qu'une application de traçage numérique enregistre tous les contacts indépendamment de leur signification, alors que SI-DEP et Contact Covid enregistrent uniquement les contacts suspicieux car le processus est déclenché par un médecin suite à un test médical ou à la présence de symptômes. Cela modifie l'évaluation de la proportionnalité et, en conséquence, les exigences d'anonymat que nous abordons ci-dessous.

Usages des systèmes d'information

Les membres des équipes sanitaires utilisateurs de SI-DEP et Contact Covid peuvent à la fois interpréter les données recueillies en contexte et expliquer les mesures sanitaires préconisées à la personne concernée ainsi qu'à ses contacts. Ceci est toutefois conditionné par le fait que ces utilisateurs des systèmes d'information soient assermentés et compétents.

Un questionnement relatif aux mesures de déconfinement opposerait l'efficacité d'une application de traçage numérique à celle des actions réalisées par des humains, notamment par les équipes sanitaires. Cette opposition conduit souvent à craindre des actions réalisées par des machines, même si elles sont peu intrusives, et à leur préférer des actions réalisées par des humains, même si elles sont plus intrusives. D'un côté, une base de données gérée par des opérateurs humains peut comporter autant, voire plus, de risques de rupture de la confidentialité que les données rassemblées par une application numérique. De l'autre côté, l'anonymat, qui est visé dans une application de traçage, ne permet pas l'accompagnement par des professionnels des personnes notifiées par l'application comme ayant été en contact avec des personnes testées positivement, du moins avant qu'elles ne se signalent elles-mêmes à leur médecin ou à une autorité de santé.

[3] LOI n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions

[4] Voir le site du ministère des Solidarités et de la Santé, consulté le 11 mai 2020 à 11h.

[5] 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

D'autres outils numériques pourraient aussi venir en soutien à l'intervention humaine à des fins de traçage. Par exemple, dans la démarche Contact Covid, la personne à laquelle il est demandé de signaler ses contacts pourrait s'appuyer le cas échéant sur l'historique de géolocalisation de son propre téléphone, voire autoriser l'agent qui l'interroge à accéder à cet historique ou à son agenda. D'autres moyens numériques pourraient, en soutien à l'intervention humaine, aider à la priorisation des appels en fonction de la fréquence de contacts ou des zones les plus atteintes, ou offrir des outils d'interaction incluant le diagnostic via les outils de télémédecine. Ces outils soulèvent également des questions de confidentialité des données personnelles.

Par ailleurs, la procédure en plusieurs étapes de Contact Covid comporte des faiblesses potentielles. Elle repose d'abord sur les appels téléphoniques, avec le risque de ne pouvoir joindre les personnes concernées. Elle repose ensuite sur un entretien avec ces personnes, dont la mémoire n'est pas certaine ou qui ne souhaiteraient pas divulguer certaines informations. En conséquence, la base de données Contact Covid est potentiellement lacunaire et incorrecte. De plus, elle peut être biaisée par des actes de malveillance, par exemple la fausse déclaration de contacts. À l'inverse, un protocole formalisé automatique donnerait rapidement la liste exhaustive des contacts de la personne testée positive. En ce qui concerne ces aspects, le recours à une application de traçage numérique pourrait compléter et renforcer utilement la procédure Contact Covid.

La complémentarité entre une application de traçage et les systèmes d'information SI-DEP et Contact Covid pourrait donc permettre une détection plus rapide, plus rigoureuse et plus robuste des cas contacts. Leur mise en relation élargirait la possibilité de suivi individuel des personnes potentiellement contaminées. Cependant, la combinaison de ces deux types d'approches peut présenter deux risques majeurs. Un croisement de deux bases de données, l'une comportant des données anonymes et l'autre non (celle de l'application et celle des systèmes SIDEP et Contact Covid), peut conduire à perdre le caractère anonyme de la première. Par ailleurs, le caractère souverain[6] d'outils numériques tels que SI-DEP et Contact Covid pourrait être compromis par leur combinaison avec une application de traçage qui échappe au contrôle des autorités nationales.

Recommandations :

4.1 Veiller à maintenir le caractère anonyme d'une base de contacts constituée automatiquement par une application numérique dans le cas de sa mise en relation avec des systèmes d'information alimentés par des professionnels assermentés et dans lesquels les informations ne sont pas anonymisées.

4.2 Veiller à ce que la combinaison éventuelle des outils SI-DEP et Contact Covid avec une application de traçage n'échappe pas au contrôle des autorités nationales.

6 La souveraineté permet d'être responsable de ses choix éthiques ; voir le rapport de la CERNA, *La souveraineté à l'ère du numérique Rester maîtres de nos choix et de nos valeurs*, Allistene, oct. 2018 ; http://cerna-ethics-allistene.org/digitalAssets/55/55708_AvisSouverainete-CERNA-2018.pdf

Point d'attention :

4.a Le croisement des deux bases de données SI-DEP et Contact Covid rend les informations de santé hautement identifiantes.

Le recours à des collaborateurs nouveaux, formés rapidement, ainsi que l'ouverture éventuelle des données médicales sensibles (état de santé de la personne, ses antécédents et ses traitements éventuels) à des acteurs qui n'y ont pas accès en conditions normales, sont susceptibles d'augmenter le risque de rupture du secret médical. La responsabilité de l'État et des divers acteurs impliqués serait engagée en cas de fuite de données ou de détournement d'usage.

Recommandation :

4.3 Former les membres des équipes sanitaires et les sensibiliser aux enjeux de la protection des données personnelles, notamment dans le contexte d'usage d'outils numériques. Veiller en particulier à la préservation du secret médical.

Anonymisation et pseudonymisation

Les données de santé nominatives contenues dans SI-DEP et Contact Covid sont pseudonymisées pour leur utilisation à des fins d'études épidémiologiques et de recherche.
De nombreuses études informatiques ont montré que la suppression de certaines données identifiantes, en particulier des noms et prénoms, éventuellement en les remplaçant par des pseudonymes, ne constitue pas une anonymisation au sens du RGPD. En effet, il existe un risque de ré-identification par croisement avec d'autres bases de données où figureraient explicitement des informations nominatives. Il convient donc d'être attentif à distinguer données « pseudonymisées » et données « anonymisées ».

Point d'attention :

4.b Des données de santé « pseudonymisées » ne sont pas des données « anonymisées », et doivent donc être considérées comme des données personnelles à protéger selon les principes imposés par le RGPD.

Protéger sans discriminer

Les données collectées par les équipes sanitaires ou par une application numérique sont des données sensibles qui pourraient être utilisées à des fins discriminatoires. Le Conseil de l'Europe souligne que *« le profilage ne doit pas entraîner de mesures discriminatoires d'aucune sorte »* en particulier sur les aspects politique, socio-économique, sexuel ou religieux[7]. De même l'OMS alerte sur le risque de stigmatisation des personnes présentant des caractéristiques perçues comme liées à la maladie[8].

[7] Conseil de l'Europe "Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel", Série des Traités Européens n° 108, 1981
[8] Article 3 du Règlement Sanitaire International de l'OMS - 2005

Recommandation :

4.4 S'assurer de la non-discrimination des personnes testées positives, ainsi que des groupes qui pourraient être identifiés dans les analyses épidémiologiques, tout en leur appliquant les mesures d'isolement requises pour limiter la propagation de l'épidémie.

5. Recommandations générales concernant les outils numériques de traçage

Pour la conception

5.1 Organiser des vérifications et des tests techniques tout au long du cycle de vie des outils numériques de traçage pour en évaluer la robustesse et la sécurité.

5.2 Faire évaluer l'efficacité des outils numériques de traçage par un organisme indépendant.

Point d'attention :

5.a À toutes les étapes de la conception et pour tous les composants techniques, veiller à respecter les cadres réglementaires français et européens, notamment le RGPD.

Pour la mise en œuvre

5.3 Définir et annoncer, pour chaque outil de traçage, une durée légale de son utilisation et de conservation des données traitées qui soit limitée et proportionnée à la durée de la pandémie. Documenter les conditions de la réversibilité de la mise en œuvre de ces outils.

5.4 Prévoir les moyens techniques et juridiques adaptés pour garantir la cybersécurité des outils numériques de traçage au vu de leur caractère intrusif et de leur usage massif.

5.5 Créer un comité de suivi unique et opérationnel pour identifier et traiter les problèmes éthiques, juridiques et sociétaux posés par les différents outils de traçage dans le contexte de la stratégie de déconfinement. Ce comité impliquera notamment des professionnels du numérique, de la santé, des sciences humaines et sociales ainsi que des parlementaires et des représentants de la société civile. Ce comité devrait s'articuler avec le Comité de contrôle et de liaison covid-19 instauré par la loi du 11 mai 2020 (art 11 VIII) chargé « *d'associer la société civile et le Parlement aux opérations de lutte contre la propagation de l'épidémie par suivi des contacts ainsi qu'au déploiement des systèmes d'information prévus à cet effet* ».

Pour les usages

5.6 Permettre aux personnes d'accéder aux données qui les concernent, de signaler une erreur, de demander une modification, de recevoir une réponse à leur requête dans un délai spécifié et d'initier un recours en cas de préjudice subi.

6. Récapitulatif des recommandations générales et spécifiques :

Pour la conception

3.1 Viser l'interopérabilité des applications de traçage, au niveau européen, voire international, dans le respect du RGPD.

3.3 Choisir des moyens techniques de détection de proximité qui favorisent la protection de la vie privée et des données personnelles.

3.4 Donner la possibilité aux autorités publiques compétentes d'activer ou de désactiver les applications de traçage qui ont été volontairement installées par leurs utilisateurs en en informant ces derniers.

3.5 Donner à tout moment la possibilité aux utilisateurs qui ont volontairement installé une application de traçage sur leur smartphone de la désactiver temporairement ou de la désinstaller définitivement.

3.6 Prévoir la désactivation automatique des applications de traçage après l'expiration de leur délai légal ainsi que les moyens d'en rendre compte publiquement.

3.7 Garantir l'information régulière, librement accessible, loyale et transparente sur la conception et le code des applications de traçage, leur finalité ainsi que sur l'exploitation des données qu'elles collectent. Veiller à ce que cette information comporte des éléments de compréhension pour tous.

3.9 Soumettre les applications de traçage à l'audit par des tiers de confiance.

3.15 Si une application de traçage est déployée, mener des expérimentations même si sa mise en service doit intervenir rapidement. Poursuivre ces expérimentations en parallèle de son déploiement.

5.1 Organiser des vérifications et des tests techniques tout au long du cycle de vie des outils numériques de traçage pour en évaluer la robustesse et la sécurité.

5.2 Faire évaluer l'efficacité des outils numériques de traçage par un organisme indépendant.

Point d'attention :

5.a À toutes les étapes de la conception et pour tous les composants techniques, veiller à respecter les cadres réglementaires français et européens, notamment le RGPD.

Pour la mise en œuvre

3.8 Prévoir un cadre législatif et réglementaire afin d'organiser les contrôles institutionnels et démocratiques des applications de traçage et faciliter le débat public.

3.10 Rendre disponibles et accessibles à tous les publics des informations claires et loyales relatives aux objectifs, au fonctionnement et aux limites des applications de traçage. Ces informations devront être fournies sur un site de

référence national en ligne, par téléphone, sous forme de documents imprimés et sous forme radio et télé diffusée.

3.11 Déployer une pédagogie large et adaptée à toute la population sur les enjeux techniques et sociétaux de ces applications de traçage.

3.12 Garantir le consentement libre et éclairé tout comme la possibilité de ne pas consentir et ceci sans pression, contrainte, ni mise en place de système de récompense.

4.1 Veiller à maintenir le caractère anonyme d'une base de contacts constituée automatiquement par une application numérique dans le cas de sa mise en relation avec des systèmes d'information alimentés par des professionnels assermentés et dans lesquels les informations ne sont pas anonymisées.

4.2 Veiller à ce que la combinaison éventuelle des outils SI-DEP et Contact Covid avec une application de traçage n'échappe pas au contrôle des autorités nationales.

4.4 S'assurer de la non-discrimination des personnes testées positives, ainsi que des groupes qui pourraient être identifiés dans les analyses épidémiologiques, tout en leur appliquant les mesures d'isolement requises pour limiter la propagation de l'épidémie.

5.3 Définir et annoncer, pour chaque outil de traçage, une durée légale de son utilisation et de conservation des données traitées qui soit limitée et proportionnée à la durée de la pandémie. Documenter les conditions de la réversibilité de la mise en œuvre de ces outils.

5.4 Prévoir les moyens techniques et juridiques adaptés pour garantir la cybersécurité des outils numériques de traçage au vu de leur caractère intrusif et de leur usage massif.

5.5 Créer un comité de suivi unique et opérationnel pour identifier et traiter les problèmes éthiques, juridiques et sociétaux posés par les différents outils de traçage dans le contexte de la stratégie de déconfinement. Ce comité impliquera notamment des professionnels du numérique, de la santé, des sciences humaines et sociales ainsi que des parlementaires et des représentants de la société civile. Ce comité devrait s'articuler avec le Comité de contrôle et de liaison covid-19 instauré par la loi du 11 mai 2020 (art 11 VIII) chargé « *d'associer la société civile et le Parlement aux opérations de lutte contre la propagation de l'épidémie par suivi des contacts ainsi qu'au déploiement des systèmes d'information prévus à cet effet* ».

Points d'attention :

4.a Le croisement des deux bases de données SI-DEP et Contact Covid rend les informations de santé hautement identifiantes.

4.b Des données de santé « pseudonymisées » ne sont pas des données « anonymisées », et doivent donc être considérées comme des données personnelles à protéger selon les principes imposés par le RGPD.

Pour les usages

3.2 Veiller à la non-discrimination des personnes qui n'utilisent pas les applications volontaires de traçage, y compris dans le contexte de déplacements en Europe et à l'international.

3.13 Permettre aux personnes de revenir à tout moment sur leur engagement et permettre l'effacement des données collectées.

3.14 Prévoir des mesures spécifiques et gratuites pour les personnes ne disposant pas de smartphone et souhaitant participer au dispositif de traçage.

4.3 Former les membres des équipes sanitaires et les sensibiliser aux enjeux de la protection des données personnelles, notamment dans le contexte d'usage d'outils numériques. Veiller en particulier à la préservation du secret médical.

5.6 Permettre aux personnes d'accéder aux données qui les concernent, de signaler une erreur, de demander une modification, de recevoir une réponse à leur requête dans un délai spécifié et d'initier un recours en cas de préjudice subi.

Point d'attention :

3.a L'utilisation d'une application de traçage doit faire l'objet d'une codécision entre les titulaires de l'autorité parentale et le mineur de moins de 15 ans.

Annexe 1 : Les différentes méthodes de suivi des contacts[9]

Dans un contexte sanitaire épidémique, imaginons qu'Alice et Bob se rencontrent et que, trois jours plus tard, il s'avère que Alice est malade. Comment peut-elle prévenir Bob, pour qu'il s'isole, se fasse tester et interrompe ainsi la chaîne de contamination ?

Un premier algorithme consiste, pour Alice, à noter dans un carnet le numéro de téléphone de Bob, ainsi que celui de toutes les personnes qu'elle a rencontrées, pour pouvoir les prévenir si jamais elle tombe malade. Mais Bob n'a pas nécessairement envie de donner son numéro à Alice, qui pourrait en faire un usage que Bob ne souhaite pas. Et s'il refuse de le donner ou s'il n'a pas de téléphone, il ne sera pas prévenu si Alice tombe malade. Cette méthode – appelons-la Carnet Contact – oblige à déclarer son identité à toutes les personnes que l'on rencontre. Elle est intrusive et potentiellement peu efficace car Bob peut ne pas souhaiter donner ses coordonnées à Alice. C'est le principe de cette méthode qui est repris par les médecins pour éviter les épidémies très violentes, comme celles de méningite : quand une personne tombe malade, un enquêteur professionnel cherche à identifier toutes les personnes avec qui elle a été en contact, pour les diagnostiquer et leur proposer éventuellement des soins. Dans le cadre de la crise sanitaire de la Covid-19, c'est le principe du protocole réalisé via le système d'information Contact Covid[10].

Pour éviter cet algorithme intrusif de par son accès à l'identité des personnes, les informaticiens en ont inventé d'autres, plus respectueux de la vie privée et des données personnelles. Par exemple, quand Alice et Bob se rencontrent, ils sont désignés par des pseudonymes – par exemple Xlthlx et Qfwfq. Une tierce personne, Zoé, reçoit alors l'information que Xlthlx et Qfwfq se sont rencontrés. Quand Alice tombe malade, elle indique à Zoé que la personne « Xlthlx » est malade ; Zoé en déduit que la personne « Qfwfq » a été en contact avec une personne contaminée. Bob, tous les jours, demande à Zoé si la personne « Qfwfq » a été en contact avec une personne contaminée ; le troisième jour, Zoé lui répond par l'affirmative. Il en déduit l'existence de risque pour lui-même. Cette méthode, dans laquelle Zoé enregistre toutes les paires de pseudonymes à l'échelle d'un pays ou d'un continent, est dite « centralisée ». C'est la base du protocole ROBERT[11], qui est utilisé en particulier dans l'application de traçage StopCovid[12].

Mais il est aussi possible de procéder autrement. Une autre méthode, à la base du protocole DP3T[13], utilisée par exemple dans les applications de traçage favorisées par les propriétaires des systèmes d'exploitation, sera déployée notamment en Allemagne et en Suisse. Elle fonctionne sur le principe suivant. Bob note dans son téléphone qu'il a été en contact avec une personne dont le pseudonyme est Xlthlx ; puis, Alice prévient tous les

[9] D'après un article à paraître dans Pour la Science en juillet 2020.

[10] Voir le site du ministère des Solidarités et de la Santé

[11] https://github.com/ROBERT-proximity-tracing/

[12] https://gitlab.inria.fr/stopcovid19/accueil

[13] https://github.com/DP-3T/

téléphones utilisant ce protocole que la personne « XIthIx » est malade, afin que Bob, parmi d'autres, sache qu'il a été en contact avec une personne contaminée. Cette méthode, dite « décentralisée » puisque Zoé n'y joue plus aucun rôle, demande de rendre publiques beaucoup d'informations. En effet, tous les téléphones qui l'utilisent contiennent l'information que la personne « XIthIx » est contaminée, alors que cette information n'est connue que d'Alice et de Zoé dans l'algorithme dit « centralisé ».

Dans le cas des protocoles dits « centralisés » ou « décentralisés », Alice peut prévenir Bob qu'elle est tombée malade depuis leur rencontre, sans que Bob n'ait besoin de communiquer à Alice, ni à personne, son numéro de téléphone ou son nom. Ces protocoles sont donc moins intrusifs que Carnet Contact. On peut aussi noter que, dans tous les cas, des attaques sont possibles, par exemple en dérobant le carnet d'adresses d'Alice dans le cas du protocole Carnet Contact, ou en menant une cyber-attaque dans le cas des deux autres types de protocoles.

Un troisième type de protocoles, qui associe des identifiants chiffrés uniques à chaque rencontre et non à chaque téléphone, est en cours de développement. Il pourrait ouvrir une troisième voie qui ne se limiterait pas au choix entre des protocoles dit centralisé ou décentralisé.[14]

14 https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE, mis en ligne le 9 mai 2020

Annexe 2 : Saisine

GOUVERNEMENT

Liberté
Égalité
Fraternité

Les Ministres

Paris, le 30 AVR. 2020

Monsieur le Directeur,

La stratégie de déconfinement, qui a été présentée le 28 avril 2020 par le Premier Ministre devant l'Assemblée nationale, repose sur trois piliers : protéger, tester et isoler. La mise en œuvre de cette stratégie va mobiliser de nombreux outils numériques qu'ils soient existants, et dont l'usage va être élargi, ou qu'ils constituent de nouveaux instruments en cours de développement.

Ces outils numériques sont mis en place dans un contexte d'urgence afin d'être disponibles rapidement dans les différentes phases de déconfinement. Néanmoins, le Gouvernement est particulièrement attaché à ce que ces outils respectent pleinement la vie privée de nos concitoyens et les libertés publiques. Au-delà de ces exigences, l'analyse de votre comité sur les enjeux éthiques de la mise en place de ces outils répondant à une nécessité impérieuse dans un contexte de crise mais également susceptibles d'avoir des effets structurants à moyen/long terme, permettrait d'éclairer les choix du Gouvernement.

Dans ce contexte, nous souhaiterions que le comité d'éthique du numérique puisse examiner les questionnements éthiques liés à la conception, la mise en œuvre, l'usage de ces outils afin que les réflexions qu'il pourra formuler puissent éclairer les travaux des semaines à venir mais aussi les débats sur l'utilisation de ces outils. Il serait particulièrement utile que le Comité pilote d'éthique du numérique nous transmette un avis d'ici au 11 mai.

Nous vous prions d'agréer, Monsieur le Directeur, l'expression de notre considération distinguée.

Olivier VERAN
Ministre des Solidarités et de la Santé

Cédric O
Secrétaire d'Etat
chargé du Numérique

Monsieur Claude KIRCHNER
Directeur du Comité national pilote d'éthique du numérique
Membre du CCNE
66 rue de Bellechasse
75007 PARIS

Personnes auditionnées

Franck Chauvin, Président du Haut Conseil de la santé publique et membre du Conseil Scientifique Covid-19
Marc Debrincat, Bruno Gazeau, Anne-Marie Ghermard de la Fédération Nationale des Associations d'Usagers des Transports
Luciano Floridi, professeur à l'université d'Oxford, membre du *Ethics Advisory Board for NHSx COVID-19 app*
Hélène Gebel, coordinatrice de l'espace de réflexion éthique du Grand Est et de la Conférence Nationale de Espaces de Réflexion Éthique Régionaux
Bruno Sportisse, Président-directeur général d'Inria

Composition du groupe de travail ayant contribué à l'élaboration de ce document

Gilles Adda
Raja Chatila
Theodore Christakis
Laure Coulombel
Camile Darche – rédactrice
Laurence Devillers
Emmanuel Didier
Karine Dognin-Sauze
Gilles Dowek
Valeria Faure-Muntian
Christine Froidevaux – co-rapporteuse
Jean-Gabriel Ganascia
Eric Germain
Alexei Grinbaum
David Gruson
Jeany Jean-Baptiste
Claude Kirchner
Caroline Martin
Tristan Nitot
Jérôme Perrin
Catherine Tessier – co-rapporteuse
Serena Villata
Célia Zolynski

Les membres du Comité national pilote d'éthique du numérique

Gilles Adda
Raja Chatila
Theodore Christakis
Laure Coulombel
Jean-François Delfraissy
Laurence Devillers
Karine Dognin-Sauze
Gilles Dowek
Valeria Faure-Muntian
Christine Froidevaux
Jean-Gabriel Ganascia
Eric Germain
Alexei Grinbaum
David Gruson
Emmanuel Hirsch
Jeany Jean-Baptiste
Claude Kirchner - directeur
Augustin Landler
Christophe Lazaro
Gwendal Le Grand
Claire Levallois-Barth
Caroline Martin
Tristan Nitot
Jérôme Perrin
Catherine Tessier
Serena Villata
Célia Zolynski

Contact presse : communication@comite-ethique.fr