Prise de position de la Commission Nationale d'Éthique (C.N.E.) sur les aides informatiques dans la lutte contre la pandémie du Coronavirus SARS-CoV-2

En provoquant la maladie potentiellement mortelle, appelée COVID-19, le Coronavirus SARS-CoV-2 s'est révélé être une menace pour la santé publique au monde entier au point que les États, l'un après l'autre, se sont résolus à prendre des mesures de lutte exceptionnelles contre sa propagation. Ces moyens mis en œuvre sont drastiques et ils sont uniques dans l'histoire en temps de paix, tant en profondeur qu'en étendue géographique. Les mesures prises jusqu'à présent ne font pas l'objet de la présente prise de position, la C.N.E. se contentant de constater ici qu'elles sont très largement acceptées pendant au moins la première période de leur application.

Parmi les moyens de lutte possibles, mais actuellement rarement utilisés en Europe, on compte le traçage informatique de rapprochements humains, un procédé aux capacités quasi infinies, mais qui déclenche des réflexes de résistance à une potentielle surveillance totale, voire totalitaire.

La discussion publique est donc lancée de savoir si ces moyens informatiques permettraient de compléter le traçage analogue et de relâcher les autres mesures pour arriver aux mêmes résultats dans l'endiguement de la pandémie. Peut-on surveiller les déplacements et contacts humains des citoyens pour, en contrepartie, protéger la santé publique et permettre de dépasser le blocage de la société provoqué par les autres mesures? La C.N.E. a considéré que cette question essentielle relève manifestement de celle pour laquelle elle a été créée et qu'elle doit donc essayer d'y apporter des réponses adaptées aux spécificités luxembourgeoises. La présente prise de position décrit le détail des réflexions de la Commission, mais commence par énoncer ses conclusions en formulant à l'égard du gouvernement un certain nombre de recommandations concrètes.

1. Recommandations au gouvernement

La C.N.E. estime que le traçage informatique doit être considéré comme un élément utile dont la prise en compte devient dès lors nécessaire. Cette conclusion positive n'est pas sans conditions. Elle oblige à établir les lignes rouges d'un cadre acceptable d'un point de vue éthique. Les éléments essentiels du cadre sont que, quel que soit le choix technique, le traçage doit être volontaire, transparent, minimaliste et limité dans le temps avec un objectif clairement défini.

A la lumière des difficultés techniques du dossier, la C.N.E. ne va pas jusqu'à recommander purement et simplement le traçage informatique par les portables intelligents (smartphones). Mais elle estime que cette méthode doit être très sérieusement considérée pour en mesurer la faisabilité, la proportionnalité et l'utilité pour la sécurité sanitaire tout en permettant une levée plus rapide des restrictions de mouvement et d'action. Le traçage informatique ne devrait pas être éliminé par pur opportunisme.

En consultant les recommandations étrangères de sources diverses[1], la C.N.E. retrouve généralement les mêmes éléments qui se répètent et qui devraient aussi guider le comportement d'un gouvernement luxembourgeois qui s'engagerait dans la voie du traçage informatique :

1.1 Caractéristiques

- Le traçage doit être volontaire. Il y a diverses raisons à cela :
  - Le cas échéant, la résistance de grandes parties de la population vis-à-vis d'une surveillance des mouvements devrait être vaincue. Or, le scepticisme des citoyens ne peut être dépassé que par leur adhésion à une nécessité et par la confiance dans des systèmes minimalistes, transparents et surtout volontaires.
  - Indépendamment des problèmes éthiques particuliers que poserait la contrainte, elle n'est pas une option réaliste. Tous n'ont pas un smartphone, nul ne peut être contraint d'en avoir un et la population multinationale de résidents et frontaliers du Luxembourg rendrait le traçage informatique obligatoire impossible en pratique.
- Le caractère volontaire d'un traçage doit être protégé.
  - Le système devra assurer un consentement libre et éclairé des personnes concernées.
  - Le système devra permettre aux personnes concernées de revenir sur leur décision et d'effacer à tout moment les données collectées sur leur appareil (réversibilité).
  - La contrainte externe devra être sanctionnée en ce sens qu'aucune personne, organisation ou entreprise n'aura le droit de soumettre ses offres, services, emplois ou quelconques prestations à la condition d'utiliser un traçage informatique.
- Le fonctionnement de l'application utilisée doit avoir une durée strictement limitée, définie d'avance et connue par les utilisateurs. La désactivation automatique doit être intégrée. Un prolongement de cette durée ne devrait être possible que par un consentement exprès renouvelé.
- Les données traitées par le portable doivent être irrémédiablement détruites sur le smartphone après la période de rétention épidémiologiquement pertinente.
- L'application doit répondre au critère d'un niveau de traitement minimal de données requis au regard des finalités poursuivies.

[1] Références : Avis n°6 du Conseil scientifique COVID-19 du 20 avril 2020 : SORTIE PROGRESSIVE DE CONFINEMENT.
(https://solidarites-sante.gouv.fr/IMG/pdf/avis_conseil_scientifique_20_avril_2020.pdf)
Lignes directrices du *European Data Protection Board* sur le traitement de données relatives à la santé à des fins de recherche ainsi que sur les outils de géolocalisation et de traçage dans le contexte de l'épidémie Covid-19.
(https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf)
Recommandations du Comité national (français) d'éthique du numérique.
(http://www.anthropotechnie.com/suivi-numerique-du-covid-10-recommandations-ethiques/)

1.2 Fonctionnement

- Pour emporter l'adhésion au système et éviter d'exacerber l'exclusion digitale de certaines catégories de la population, la facilité de chargement et d'emploi d'une application de smartphone est très souhaitable.
- Le fonctionnement de ce type d'application nécessite de diffuser des données lues par les appareils d'autres utilisateurs et d'écouter ces émissions. Seuls des identifiants pseudonymes doivent être échangés entre les équipements mobiles des utilisateurs. Les identifiants doivent être générés à l'aide de processus cryptographiques de pointe et être renouvelés régulièrement pour réduire le risque d'attaques et d'abus.
- Les données pseudonymisées collectées sur un smartphone concernent donc aussi des données relatives aux tierces personnes approchées. Ces données doivent dès lors être conservées de façon inaltérable, sauf à être supprimées par désinstallation de l'application par le propriétaire du portable.
- Le fonctionnement de ce type d'application peut nécessiter, selon l'architecture choisie, l'utilisation d'un serveur centralisé. Dans un tel cas et conformément aux principes de minimisation et de protection des données par conception, les données traitées par le serveur centralisé doivent être limitées au strict minimum.
- Les informations transmises et stockées sur un serveur central ne devraient pas permettre au responsable du traitement d'identifier les utilisateurs diagnostiqués comme infectés ou ayant été en contact avec ces utilisateurs.
- Lorsqu'un utilisateur est diagnostiqué comme infecté par le virus SARS-CoV-2, les informations concernant ses précédents contacts proches ou les identifiants diffusés par l'application de l'utilisateur ne peuvent être collectées qu'avec l'accord de l'utilisateur.
- Lorsqu'un utilisateur est diagnostiqué infecté, cette information, si elle passe par un moyen de télécommunication, ne doit pas révéler l'identité de la personne infectée.
- Lorsqu'un utilisateur est diagnostiqué infecté, les personnes avec lesquelles il a été en contact étroit doivent être concomitamment encouragées à se manifester et à passer un test du SARS-CoV-2.

1.3 Garanties

- La mise en œuvre d'un traçage informatique devrait être accompagnée par un comité *ad hoc* externe, composé de spécialistes informatiques, de la santé, de la protection des données et d'éthique, aucune autorité existante – et *a fortiori* la C.N.E. – n'étant en mesure de s'exprimer sur des applications informatiques concrètes.
- L'application de traçage devrait être certifiée par une autorité compétente, après avis de la Commission nationale pour la protection des données (CNPD)[2]. Les critères de la certification incluent l'évaluation de la sécurité, la prévention à l'abus, le souci du traitement minimal de données nécessaires au regard de la finalité poursuivie, la sécurité du stockage, l'anonymisation ou la pseudonymisation des données, les moyens d'accès contrôlé aux données, la définition des parties intervenant dans le

[2] D'autres modèles de contrôle sont imaginables à l'instar de la Commission spéciale du contrôle du Service de renseignement de l'État du Luxembourg (SREL) qui est composée de trois magistrats, à savoir le président de la Cour supérieure de justice, le président de la Cour administrative et le président du Tribunal d'arrondissement de Luxembourg.

traitement et la limitation dans le temps du fonctionnement de l'application et de la conservation des données.

- Afin de contribuer à la confiance et à l'adhésion des utilisateurs, toute l'information sur le système de traçage doit être publiquement accessible, loyale et transparente. Cette information inclut :
    - la conception, le code,
    - les moyens de traçage informatique,
    - l'appréciation de leur nécessité et de leur finalité,
    - la procédure d'exploitation des données collectées,
    - les critères d'évaluation, les avis et les conclusions du Comité *ad hoc* et de l'autorité de certification,
    - la procédure de nomination et la composition du Comité *ad hoc* et de l'autorité de certification.
- La nécessité et la proportionnalité des mesures doivent être réévaluées à intervalles réguliers par l'autorité de certification sur demande du comité *ad hoc* externe créé à cet effet.
- Les utilisateurs doivent être informés des autorités ou instances où ils peuvent signaler une erreur ou un dysfonctionnement et initier un recours. Les décisions de ces autorités doivent à leur tour être soumises à un potentiel contrôle judiciaire.
- Des échanges internationaux de données de traçage doivent être limités aux pays membres de l'Union européenne et se faire dans le respect du cadre européen de la protection des données personnelles et de la vie privée. La C.N.E. estime que la qualité de membre de l'Union européenne n'est pas une garantie implicite du respect de la protection des droits fondamentaux, dont notamment la protection des données.
- La transparence du système doit permettre un contrôle démocratique et parlementaire des mesures de traçage informatique.

2. La démarche de la Commission

Pour conclure que le traçage informatique est un moyen dont au moins la prise en compte, sinon la réalisation, est incontournable, la C.N.E. a dû peser les dangers de cette méthode contre les menaces pour la santé publique et celles que constituent les autres formes de la lutte sanitaire pour la liberté, la démocratie, la vie économique et culturelle et le bien-être au sens large. Pour cela, la C.N.E. a choisi :

- de rappeler le danger effectif pour la santé publique du COVID-19,
- de faire un bref inventaire des autres menaces découlant de l'état de crise actuel,
- de décrire en quoi un traçage informatique pourrait, dans l'absolu, effectivement circonscrire ces dangers,
- de décrire les dangers inhérents au traçage informatique et les options techniques pour les mitiger,
- de décrire les limites légales actuellement dressées par le RGPD,
- de mettre en balance les valeurs et dangers respectifs pour conclure si, oui ou non, le traçage doit être considéré comme utile, voire nécessaire et quelles en seraient les conditions.

2.1 Le danger du COVID-19 pour la santé publique

Pour apprécier si un moyen mis en œuvre est proportionnel au fléau qu'il entend combattre, il est nécessaire de prendre la juste mesure du danger effectif que ce fléau représente. Le danger du COVID-19 n'est pas à ce point évident qu'il peut se soustraire à la discussion. S'agit-il d'une « grippe comme une autre » ? Faut-il restreindre drastiquement la vie quotidienne de 100% de la population pour quelques 0,01% de décès ? Les victimes, majoritairement âgées ou à pathologie(s) pré-existante(s), ne seraient-elles pas décédées de toute façon ? Ne meurent-il pas autant de gens par une grippe saisonnière ou par les accidents de la route sans que cela ne provoque des mesures d'exception ?

Toutes ces questions sont posées à juste titre, mais les réponses sont souvent coloriées par des relents populistes ou par des « fake news ». Il s'y ajoute qu'une vision purement statistique d'une mortalité ignore les malheurs individuels et les peurs collectives qui accompagnent une pandémie.

Il est pourtant évident que la situation sanitaire actuelle est en soi totalement exceptionnelle. Des hôpitaux entiers sont occupés, et à l'étranger souvent dépassés, par le nombre de patients COVID-19. Une proportion exceptionnelle de personnel soignant est infectée par la maladie-même qu'ils sont appelés à soigner. Il y a menace de pénurie de matériel de soins, de médicaments et de matériel de protection. Des patients très gravement malades sont transportés à travers l'Europe pour leur trouver les lits de soins intensifs nécessaires. Le personnel soignant est acculé à établir des priorités extrêmement difficiles d'un point de vue éthique (voir la prise de position de la C.N.E. à cet égard[3]). La maladie elle-même n'est pas encore entièrement comprise et il n'existe encore ni remède, ni vaccin. Et surtout, il faut craindre que sans les mesures radicales prises, le nombre de personnes infectées, de patients marqués à vie par des séquelles ou de morts aurait explosé, ruinant au passage le système de santé et risquant de causer *in fine* un dommage sociétal bien pire que le blocage actuel.

Une caractéristique particulièrement pernicieuse de la crise actuelle est son étendue sur une durée inconnue. Il est donc incontestable que le fléau du COVID-19 constitue un danger immédiat et exceptionnel qui justifie des mesures elles aussi exceptionnelles sans que leur durée ne peut excéder pas le fléau qu'elles entendent combattre. Même des mesures graves peuvent en l'occurrence être parfaitement proportionnelles.

2.2 Les dangers de l'état de crise actuel

La C.N.E. n'entend pas ici juger les mesures prises par le gouvernement luxembourgeois à l'instar des politiques appliquées par la grande majorité des pays européens. Elle constate simplement que les inconvénients du confinement sont connus et débattus par le monde politique luxembourgeois et la déclaration de l'état de crise souligne en elle-même le caractère parfaitement exceptionnel de la situation. Le vœu d'un retour à la normale est incontestablement partagé à l'unanimité, quelles que soient les discussions de détail sur la façon optimale pour y arriver.

Mais dans la mesure où un traçage informatique pourrait éventuellement accélérer le déconfinement, il est nécessaire – comme pour la santé publique – de décrire à quel point le confinement est aussi un drame.

[3] « Repères éthiques essentiels lors de l'orientation des patients dans un contexte de limitation des ressources thérapeutiques disponibles pendant la crise pandémique du COVID-19 ». (https://cne.public.lu/fr.html)

Le confinement dans la forme retenue en début de crise consiste à emprisonner la population chez elle pour son plus grand bien. Cette approche est actuellement atténuée, mais risque de regagner en vigueur en cas de nouvelle vague d'infection. La liberté de circuler est alors très limitée pour tous ; pour les plus âgés, elle n'existe plus en pratique. La liberté d'association est privée de son expression physique. Il est interdit de se rencontrer entre amis, en famille, au sport, aux pratiques culturelles et religieuses. La liberté du commerce est suspendue. Il devient impossible aux familles de rencontrer et soigner leurs anciens, d'accompagner leurs mourants et leurs défunts. Il est défendu aux enfants de jouer, d'apprendre et de vivre comme un enfant. Bref, l'essentiel des droits humains et constitutionnels est en suspens.

Comme ces mesures sont justifiées par le souci de préservation de la santé publique, il est utile de rappeler qu'elles constituent en même temps une menace pour la santé publique. Car la santé ne se limite pas à l'absence de maladie. Elle inclut le bien-être mental et social qui ne dépend pas seulement des services de santé, mais aussi des droits et des libertés, de l'éducation, du contact social, du travail, de l'éducation, de la culture.

L'effondrement économique est un problème qui mérite d'être considéré à part. La séparation entre activités essentielles et non essentielles est une fiction. La vie économique est une roue qu'on ne peut mettre partiellement à l'arrêt en espérant que les parties essentielles, telles l'alimentation ou les services de santé, pourraient continuer à tourner. Lorsque les chaînes de valeurs sont interrompues, l'alimentation des parties dites essentielles est vite menacée. Pire, la destruction annoncée des entreprises et des emplois va plonger dans la misère des millions de personnes dans la seule Europe et risque d'entraîner des catastrophes sociales et sociétales, voire des politiques extrêmes. Seuls les États, par le recours à des endettements colossaux peuvent tenter de limiter les dégâts, mais ils le font au détriment des générations futures et en risquant de perdre en route leurs autres priorités, telles la lutte contre le changement climatique, contre les inégalités, contre la migration de misère et les autres calamités du siècle.

Après avoir constaté que le COVID-19 constitue un danger exceptionnel justifiant des mesures elles aussi exceptionnelles, la C.N.E. fait remarquer que le confinement met en cause les libertés les plus élémentaires autant que toutes les autres priorités sociétales et menace la santé publique sur un pan pour la protéger sur d'autres pans. Si ces mesures peuvent être levées ou allégées par des mesures moins contraignantes, il est impérieux de les considérer.

2.3 Les mérites annoncés d'un traçage informatique

Sans correctif, le SARS-CoV-2 se propage de façon exponentielle, chaque personne infectée en infectant à son tour trois autres en moyenne. L'endiguement exigerait donc d'empêcher chaque infecté de transmettre le virus. Cela est rendu très difficile parce que les personnes touchées ne présentent pas de symptômes ou ignorent leur condition avant l'éclosion des symptômes, c'est-à-dire pendant une période d'incubation allant généralement de quelques jours à deux semaines. C'est la raison pourquoi les autorités sanitaires aimeraient retracer, pour chaque personne testée positivement au Coronavirus, les contaminations potentielles pendant la période épidémiologiquement pertinente. Au tout début de l'épidémie, ce retraçage des contacts se fait par enquête et questionnements des concernés. On informe alors les contacts de la personne infectée et leur demande de se mettre en isolation et de s'observer de façon à ce qu'elles ne contaminent personne à leur tour. C'est ce qu'on appelle communément le traçage « analogue ».

On peut supposer que très peu de gens se soustraient aux questions des autorités lorsqu'ils sont en situation d'épargner la maladie à d'autres. L'énorme majorité au contraire se sentirait coupable d'avoir propagé la maladie sans avertir leurs connaissances des risques que ceux-ci encourent et font encourir à leurs proches. Mais le procédé est fastidieux, incertain et d'une efficacité limitée. Peu de gens peuvent nommer les noms et coordonnées de toutes celles qu'elles ont croisées depuis quinze jours ou plus. De plus, une fois que le virus a atteint des milliers ou des dizaines de milliers de personnes, cette enquête devient matériellement impossible pour les autorités.

D'où l'idée de compléter la mémoire défaillante et le questionnement individuel par un traçage automatisé des mouvements et contacts de chacun. Il est aujourd'hui techniquement très facile de localiser les smartphones et avec eux l'énorme majorité de la population. Un registre permanent des contacts permettrait ainsi de reconstituer pour chaque personne infectée les personnes qu'elle risque d'avoir contaminées. L'intérêt du procédé est évident et d'ailleurs peu contesté[4]. Les scientifiques et épidémiologistes concluent que du point de vue de la lutte sanitaire, le traçage doit être considéré comme utile, sinon nécessaire. Certains spécialistes considèrent le traçage informatique comme incontournable si on ne veut pas risquer de tomber d'une vague d'infections à l'autre avec à chaque fois son cortège de confinements et restrictions.

Il y a lieu de noter que la surveillance et l'obligation de déclaration des maladies contagieuses fait partie depuis toujours de la panoplie de mesures des autorités de santé. Le traçage est un procédé normal de lutte contre une pandémie. Dans sa politique de tests très étendus, le gouvernement prévoit explicitement de recourir au traçage individuel non-informatique des personnes testées positivement pour casser la chaîne de transmission. Tout porte à croire que sa variante informatique à l'aide des smartphones portables contribuerait à une efficacité accrue, surtout si le nombre de personnes touchées ne permet plus le suivi individuel par les autorités. Mais surtout, un traçage informatique tel que celui envisagé actuellement serait moins invasif pour la vie privée que le traçage analogue qui n'est pas remis en question. Ce n'est pas le procédé informatique qu'il faut craindre, mais ses excès potentiels.

Il est par ailleurs marginal de constater que toutes les personnes ne possèdent pas de smartphone et toutes ne seront pas prêtes à se soumettre au procédé. C'est le nombre qui compte et comme l'écrasante majorité en est équipée, l'utilité potentielle du procédé est facilement garantie pour une proportion suffisante de gens.

---

[4] Avis n°6 du Conseil scientifique français COVID-19 du 20 avril 2020, SORTIE PROGRESSIVE DE CONFINEMENT : « (Les…) *outils numériques offrent au public des moyens simples pour déterminer si l'on est un cas probable, être dans ce cas orienté vers des lieux de test, obtenir rapidement le résultat de son test, être suivi médicalement si l'on est positif, apprendre si l'on a été en contact avec un cas et plus généralement évaluer les risques d'infection auxquels on a été exposé. Les outils numériques ont également un rôle clé à jouer pour soutenir la logistique, notamment concernant la réalisation de tests («testing»), le rendu des résultats des tests, la gestion des ressources hospitalières. Le Conseil scientifique considère les outils numériques comme un élément très utile de la stratégie de contrôle de l'épidémie. (...) le Conseil scientifique considère que les outils numériques permettant d'améliorer l'efficacité du contrôle sanitaire doivent être déployés en France, en concertation avec les institutions européennes et les pays européens si cela est possible. Ces outils doivent s'inscrire dans une stratégie globale de lutte sanitaire, dont ils ne sont qu'un élément.* »

Pour ces raisons, le principe du traçage informatique est largement utilisé en Asie avec la Chine, Singapour et la Corée du Sud comme exemples les plus connus. Les techniques qui y sont utilisées ne sont pas identiques.

Il convient cependant de ne pas confondre l'utilité d'un traçage informatique avec une panacée. Le remède universel qui nous débarrasserait à la fois de la maladie et des restrictions n'existe tout simplement pas et les moyens informatiques ne sauraient être, même dans le meilleur des cas, qu'un accompagnement qui augmenterait l'efficacité d'autres mesures, dont le traçage analogue.

2.4 Les dangers inhérents au traçage et les options techniques pour les mitiger

La première de toutes les libertés essentielles est la liberté de mouvement. C'est ce qui rend le confinement obligatoire par les autorités publiques aussi délicat. Dans la conception occidentale de la liberté de mouvement, celle-ci n'est vraiment donnée que si elle peut s'exercer sans contrôle externe. Aucune personne n'est vraiment libre de ses mouvements si elle doit en rendre compte. Cette idée est profondément ancrée dans l'entendement que nous avons des droits de l'homme et des libertés publiques et donc aussi dans les fondements juridiques de nos sociétés.

Mais ce n'est pas le seul problème de fond. En l'occurrence, le but du traçage est de partager *in fine* des données personnelles de deux ordres :

- données sur les mouvements et rencontres avec d'autres personnes et
- données relatives à la santé.

Alors que la première catégorie relève déjà de données sensibles, la seconde touche aux données les plus sensibles qui soient.

Avant tout autre progrès dans nos réflexions, nous pouvons dès lors constater que le traçage peut porter préjudice et qu'il n'est pas souhaitable *a priori*.

Pourtant, la technique utilisée n'est pas neutre dans la juste description des inconvénients du traçage informatique. Il y a lieu de distinguer grossièrement trois options techniques :

1. **La géolocalisation** permet de positionner géographiquement un smartphone et d'en retracer en temps réel ou *ex post* les mouvements dans le temps et dans l'espace. Cela est possible grâce à un système de positionnement par satellites (p.ex. GPS) et/ou via les antennes de télécommunication. Les positions enregistrées sont stockées sur un terminal central et peuvent être extraites ultérieurement ou être consultées en temps réel. Un très grand nombre d'applications utilisées au quotidien par des millions d'utilisateurs utilisent la géolocalisation. Comme toute appréciation des moyens en présence passe par la recherche du traitement minimal, la C.N.E. peut facilement exclure la géolocalisation qui, bien que très utilisée sur des applications courantes, ouvrirait sans nécessité la voie à des abus et dangers majeurs. Il y a lieu de la mentionner ici, car beaucoup de peurs et réticences contre le traçage dans le public proviennent justement des possibilités de contrôle exorbitant qui s'ouvrent avec cette technique.

2. **Le système Bluetooth** permet à chaque smartphone d'entrer en contact bidirectionnel avec d'autres appareils à l'aide d'un échange de données à très courte distance en utilisant des ondes radio. Il devient ainsi possible pour des smartphones équipés d'une

application adaptée d'enregistrer réciproquement leur état de proximité sans que soient localisés leurs mouvements géographiques et sans forcément livrer leurs informations à un serveur central en temps réel. La puce Bluetooth du smartphone envoie des signaux et reçoit les signaux des appareils à proximité de seulement quelques mètres. Le smartphone stocke des codes aléatoires qu'il reçoit d'autres appareils et également ceux qu'il envoie aux autres, idéalement pendant une durée et à une distance qui permettent l'infection. Les codes changent en permanence à quelques minutes d'intervalle. Ces systèmes peuvent se distinguer au moment où le porteur de l'appareil est testé positivement au virus SARS-CoV-2.

a. Dans un **système centralisé**, la personne infectée choisit de transmettre l'intégralité des **codes envoyés et reçus** à un serveur central, sous contrôle de l'autorité publique. Ces données sont analysées au **niveau du serveur central** et les utilisateurs de l'application qui étaient à proximité de la personne infectée seront notifiés directement sur leurs smartphones. Cette notification ne contient pas d'information identifiable et va inviter la personne à appeler une hotline et de se faire tester à son tour.
b. Dans un **système décentralisé**, la personne infectée choisit de transmettre l'intégralité des **codes envoyés** à un serveur central, de préférence sous contrôle de l'autorité publique. Tous les autres utilisateurs de l'application téléchargent périodiquement cette liste. Ces données sont analysées au **niveau du téléphone portable** de l'utilisateur et si un contact prolongé a eu lieu, l'application va informer la personne et l'inviter à appeler une hotline et de se faire tester à son tour. Les résultats de cette analyse restent sur le téléphone portable de l'utilisateur.

Dans les deux systèmes, une autorité centrale est nécessaire et la protection des données échangées par Bluetooth se fait toujours par des moyens cryptographiques visant à préserver la confidentialité des utilisateurs. C'est le cas, par exemple, des systèmes élaborés par Apple et Google pour leur projet de traçage. Par contre, la pseudonymisation et les moyens cryptographiques couvrent uniquement l'échange des données entre appareils et l'endroit central potentiel de stockage des données. Il incombe aux fournisseurs d'applications de traçage de s'assurer que les dispositifs nécessaires en matière de sécurité et de protection des données est garantie. Dès lors, en respectant tous les critères qui assurent la protection maximale des données personnelles, un traçage par Bluetooth s'avère comme une piste à explorer. Indépendamment de savoir si une autorité centrale entre directement en contact avec les personnes qui seront averties, aucun des deux systèmes Bluetooth n'est plus invasif que ne l'est le traçage dit analogue. Par contre le système centralisé permettrait, en cas d'abus, un profilage des contacts qu'il faut dès lors éviter à tout prix.

2.5 Les limites légales actuellement dressées par le RGPD

La protection des données nominatives compte aujourd'hui parmi les expressions les plus notoires de la protection de la vie privée. La C.N.E. se doit de rappeler que cette protection s'oppose à l'État et notamment son exécutif qui détient, dans un État de droit, le monopole de la violence. En effet, l'État de droit se définit par son autolimitation à travers la loi qui donne au citoyen des droits que l'État doit respecter malgré ses intérêts éventuellement divergents. Ce rappel est nécessaire dans la mesure où les exécutifs étatiques ont une tendance à s'ériger en défenseur des droits de la personne alors qu'ils en sont en réalité les débiteurs. Il va de soi que la protection des données doit aussi pouvoir être efficacement opposée à des acteurs privés, notamment commerciaux, mais il est important de noter qu'ils ne sont pas les seuls, et même pas les premiers visés.

Quiconque retrace les mouvements et contacts d'une personne est soumis à la législation sur la protection des données personnelles dont l'expression légale européenne est aujourd'hui le *Règlement général sur la protection des données* (RGPD). Le RGPD est d'application directe dans tous les États membres de l'Union européenne et sa conformité est obligatoire depuis le 25 mai 2018. Ses principes essentiels sont bien antérieurs et découlent aussi d'un bon sens éthique :

- Le traitement de données (en ce compris la collecte et la conservation) doit être permis par la loi ou par la personne concernée (consentement).
- La collecte et le traitement de données doivent obéir à des finalités légitimes et précises lesquelles doivent rester respectées dans la durée. Cela implique
    - que seules les données nécessaires à ces finalités peuvent être traitées (minimisation) et
    - que la durée de conservation est limitée à l'accomplissement de ces finalités.
- Les données traitées doivent être correctes.
- Les données doivent être traitées en sécurité.
- Les données traitées ne doivent pas être transmises à des tiers (confidentialité).

Ces principes valent pour toutes les données, mais toutes les données ne sont pas à traiter à la même enseigne. Le RGPD distingue notamment les données biométriques et les données relatives à la santé comme étant des données « particulières » dont le traitement n'est autorisé que par exception (articles 9 et 10 RGPD). La collecte et le traitement de ces données doivent être justifiés au cas par cas au regard des objectifs recherchés. La protection des données médicales est une exigence éthique depuis l'antiquité et s'est exprimée la première fois dans le serment d'Hippocrate.

Dans tous les débats relatifs à une application informatique permettant le traçage dans le cadre de la crise du COVID-19, la protection des données est donc à juste titre mise en avant comme présentant un obstacle majeur. La population a un scepticisme profond envers les moyens de surveillance tant des États que des opérateurs privés, surtout des grandes multinationales du numérique. A observer les mœurs, on doit cependant constater que le respect des principes de la protection des données est plus audible dans les grands discours qu'il n'est sensible dans les faits. Cela se constate à plusieurs niveaux.

> - Les États ont trouvé des exceptions légales dans tous les cas où ils ont estimé judicieux de contourner ces principes. C'est le cas dans la lutte contre le terrorisme, contre la pédophilie, contre le blanchiment ou encore contre la fraude fiscale. Tous les secrets professionnels ont été affaiblis ces dernières décennies alors que la protection des données fut promue. La C.N.E. n'entend pas juger ici de la justification de ces exceptions légales, elle constate simplement qu'elles sont légions et a priori elles ne semblent pas avoir obéi à une gravité plus évidente que la crise du COVID-19.
>
> - Les pouvoirs exécutifs des États ont une propension à ignorer la législation sur la protection des données. Depuis le scandale du réseau d'espionnage ECHELON, resté sans conséquences, en passant par les révélations d'un Edward Snowden jusqu'au récent constat que même les moindres infractions des citoyens au Luxembourg sont tenues sans limites de temps dans des bases de données illégales, les exemples ne manquent pas pour illustrer que la pratique ne suit la loi que de façon très imparfaite.

Ce sont ces exemples qui sont largement à l'origine du scepticisme public envers toute surveillance informatique sournoise.

- Les citoyens eux-mêmes ne réservent que peu d'attention à la protection de leurs données. Une grande majorité d'utilisateurs de smartphone utilisent des applications qui retracent leurs faits et gestes, bien au-delà de ce que les projets d'application de traçage du COVID-19 ne prévoient.

- Les entreprises privées ressentent les règles du RGPD souvent comme une chicane administrative et elles constituent surtout un coût pour chacune d'elles.

- La presse qui s'érige souvent en avocat de la protection des données plaide quasi unanimement pour la transparence et s'oppose à tous les secrets, sauf à celui de ses propres sources.

Par ces propos, la C.N.E. n'entend en aucun cas relativiser les principes ci-avant rappelés d'une protection des données personnelles. Elle s'attend au contraire à ce qu'ils soient appliqués. Mais elle estime que la gravité de la situation actuelle ne permet pas maintenant de sanctifier dans le débat public des principes auxquels il est dérogé chaque fois qu'un argument contraire, aussi futile soit-il, peut lui être opposé. La première question est donc de savoir si les conditions légales qui s'appliqueraient à un traçage informatique en permettraient l'usage ou si le législateur – national ou européen – devrait intervenir.

Les autorités européennes compétentes pour la protection des données (*European Data Protection Board* – EDPB) se sont exprimées dès le 20 mars 2020 sur le traitement des données à caractère personnel dans le cadre de l'épidémie[5]. Le 22 avril 2020, l'EDPB adopte ses « *Lignes directrices sur le traitement de données relatives à la santé à des fins de recherche ainsi que sur les outils de géolocalisation et de traçage dans le contexte de l'épidémie Covid-19* »[6]. Les conclusions sont claires : La réglementation européenne de la protection des données permet l'usage responsable de données pour la gestion de la santé publique, tout en assurant que les droits et libertés personnelles ne soient pas sacrifiés dans le processus.[7]

Mais la légalité n'est pas tout. La C.N.E. a pris en compte les lignes directrices de l'EDPB dans ses recommandations.

[5] https://cnpd.public.lu/fr/actualites/international/2020/03/statement-edpb-corona.html
[6] https://cnpd.public.lu/fr/actualites/international/2020/04/edpb-covid19-guidance.html
[7] *"The world is facing a significant public health crisis that requires strong responses, which will have an impact beyond this emergency. Automated data processing and digital technologies can be key components in the fight against COVID-19. However, one should be wary of the "ratchet effect". It is our responsibility to ensure that every measure taken in these extraordinary circumstances are necessary, limited in time, of minimal extent and subject to periodic and genuine review as well as to scientific evaluation. The EDPB underlines that one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and more over data protection principles can play a very important role in the fight against the virus. European data protection law allows for the responsible use of personal data for health management purposes, while also ensuring that individual rights and freedoms are not eroded in the process."*

2.6 La pesée des valeurs et dangers respectifs

Les valeurs en présence ont été énoncées plus haut et s'énumèrent comme suit :

- La santé publique, la préservation du système de santé et le droit de chaque personne à voir sa vie et son intégrité physique préservées et à voir minimisé son risque personnel de devenir victime par contagion d'un virus aux dangers incontestés ;
- La liberté de mouvement et d'action qui sont autant de droits fondamentaux, humains, politiques et économiques ;
- La protection de la sphère privée, dont le droit au contrôle sur ses données personnelles.

Ces valeurs sont susceptibles d'être mises en danger de plusieurs façons :

- Le virus déclenche une épidémie qui menace les personnes, les systèmes de santé et, par ricochet, l'ordre public.
- L'état de crise avec ses restrictions d'actions et de mouvements des personnes est une attaque aux libertés fondamentales et provoque une crise économique majeure avec son cortège de dégâts sociaux.
- Le traçage informatique implique un traitement de données sensibles et est susceptible d'établir un contrôle externe sur des éléments de la sphère privée et sur le libre mouvement des personnes allant jusqu'à mettre en doute la confiance du public dans la bonne foi des autorités publiques.

En confrontant des valeurs et dangers de nature aussi fondamentale, il est essentiel de garder la mesure :

- La santé publique ne s'est pas effondrée, les ravages sanitaires ne menacent pas l'existence du pays.
- Le gouvernement n'est pas suspect de vouloir laminer les droits politiques et sa bonne foi dans la lutte sanitaire est largement reconnue par la population et par l'opposition parlementaire.
- Les adeptes du traçage des personnes contaminées ou à risque sont des scientifiques qui cherchent à protéger les personnes et qui ne complotent pas contre les libertés fondamentales.

Nous sommes en présence d'un trilemme qui interdit d'ériger chacun de ces trois pôles en principe absolu. Cela relèverait de la caricature. Mêmes des principes comme la santé publique et les autres libertés essentielles doivent au contraire être jaugés à leur juste valeur et aussi être relativisés l'un en face de l'autre. C'est ce qui a été fait sans hésitations en instaurant un état de crise. De même, le traçage informatique, s'il est envisagé, doit être traité comme un mal nécessaire et être mis en balance contre le préjudice de la maladie et contre le préjudice du confinement.

Nous avons noté plus haut que tout porte à croire que le traçage informatique serait sanitairement utile, même s'il ne constitue pas la panacée. Il y a donc un espoir réaliste qu'il pourrait aider à mitiger les restrictions de libertés que l'état de crise a imposées. Si tel est le cas, c'est-à-dire s'il peut effectivement alléger le fardeau, alors la prise en compte du traçage par les smartphones doit nécessairement être considérée parmi les moyens de lutter contre cette crise exceptionnelle. L'écarter par commodité politique ou par surévaluation des principes de la protection des données personnelles serait inacceptable. Ce serait d'autant moins acceptable qu'il n'est nullement établi que la protection des données est incompatible

avec le traçage comme le montrent les lignes de conduite que les autorités compétentes de la protection des données ont publié à travers l'EDPB.

Cette conclusion gagne actuellement l'ensemble de l'Europe où différents projets de traçage de contact sont en développement, tous prétendant respecter les droits élémentaires de la protection des données. De tels projets existent aussi à l'initiative d'experts de l'Université du Luxembourg ou de Apple et Google aux États-Unis. La *Pan-European Privacy-Preserving Proximity Tracing* (PEPP-PT), une communauté d'informaticiens européens créée à ce sujet, a acquis quelque notoriété médiatique. Il ne s'agit pas de les croire tous sur parole, mais il s'agit de les écouter.

C'est ce que font la France, la Belgique et l'Allemagne actuellement. Cette dernière a annoncé retirer son soutien à la PEPP-PT pour privilégier une approche «décentralisée» de la recherche des contacts numériques.

Le Luxembourg risque d'être entouré de pays qui chacun adopte potentiellement une solution différente. Pour un pays qui accueille des centaines de milliers de frontaliers et dont les habitants franchissent la frontière à chaque déplacement de plus de 50 kilomètres, il est évident qu'une solution européenne viendrait à point nommé. Mais ce vœu n'a rien de réaliste à court terme et, au vu des développements pervers de l'état de crise dans certains pays membres de l'Union, on doute même que cette solution soit souhaitable.

Il y a évidemment des inconvénients majeurs à avoir une moitié de la population active qui se baserait sur des systèmes de traçage reposant sur des autorités sanitaires étrangères. Cette difficulté est même de nature à mettre en question l'utilité d'un système de traçage, donc sa justification. Mais un système à architecture entièrement ouverte, décentralisé et volontaire, n'est pas mis en cause par cette difficulté, car: - rien n'interdit qu'un smartphone utilise plus d'une application et que les porteurs se conforment au mode d'emploi des deux en cas de test positif, et - rien n'interdit au Luxembourg de s'attacher à un des pays qui l'entoure, ce qui implique qu'il s'intéresse dès maintenant dans le détail aux options discutées par nos voisins.

--

L'ensemble de ces considérations amène la C.N.E. à conseiller au gouvernement d'envisager positivement le traçage informatique et faire l'analyse détaillée des moyens techniques et juridiques nécessaires à cet effet. La Commission a défini le cadre éthique et formulé ses recommandations telles qu'exprimées dès la première partie de la présente prise de position.