N° 673

SÉNAT

SESSION ORDINAIRE DE 2020-2021

Enregistré à la Présidence du Sénat le 3 juin 2021

RAPPORT D'INFORMATION

FAIT

au nom de la délégation sénatoriale à la prospective (1) sur les **crises sanitaires** *et* **outils numériques** *:* **répondre** *avec* **efficacité** *pour* **retrouver** *nos* **libertés***,*

Par Mmes Véronique GUILLOTIN, Christine LAVARDE et M. René-Paul SAVARY,

Sénateurs

(1) Cette délégation est composée de : M. Mathieu Darnaud, *président* ; MM. Julien Bargeton, Arnaud De Belenet, Mmes Catherine Conconne, Cécile Cukierman, M. Ronan Dantec, Mme Véronique Guillotin, M. Jean-Raymond Hugonet, Mmes Christine Lavarde, Catherine Morin-Desailly, Vanina Paoli-Gagin, MM. René-Paul Savary, Rachid Temal, *vice-présidents* ; Mme Céline Boulay-Espéronnier, MM. Jean-Jacques Michau, Cédric Perrin, *secrétaires* ; M. Jean-Claude Anglars, Mme Catherine Belrhiti, MM. Éric Bocquet, François Bonneau, Yves Bouloux, Patrick Chaize, Patrick Chauvet, Philippe Dominati, Bernard Fialaire, Mme Laurence Harribey, MM. Olivier Henno, Olivier Jacquin, Roger Karoutchi, Jean-Jacques Lozach, Cyril Pellevat, Alain Richard, Stéphane Sautarel, Jean Sol, Jean-Pierre Sueur, Mme Sylvie Vermeillet.

SOMMAIRE

Pages

PREMIÈRE PARTIE :
LE NUMÉRIQUE, UN PUISSANT ANTIVIRUS

I. LES MULTIPLES USAGES DU NUMÉRIQUE FACE À LA CRISE

Omniprésent dans nos vies, le numérique a été omniprésent dans la crise sanitaire. La hausse spectaculaire de certains usages a permis d'assurer la continuité de la vie économique et sociale, alors que la moitié de l'humanité était confinée, et l'exploitation des données a contribué à faire avancer la recherche scientifique à une vitesse inédite. Toutefois, c'est son utilisation dans le cadre de dispositifs de gestion de crise, et plus particulièrement de contrôle des restrictions sanitaires, qui pose les questions les plus difficiles – et constitue l'objet du présent rapport.

A. ASSURER LA CONTINUITÉ DE LA VIE ÉCONOMIQUE ET SOCIALE

La crise sanitaire a, tout d'abord, donné lieu à une augmentation spectaculaire du recours au numérique pour assurer **la continuité de la vie économique et sociale** : télétravail, enseignement à distance, télémédecine, maintien des liens familiaux et amicaux, e-commerce, *streaming* vidéo, etc. Il s'agit là d'un phénomène majeur, et parfois même d'un basculement, certaines pratiques nouvelles étant appelées à demeurer une fois la crise terminée.

Ces évolutions générales, qui posent de très nombreuses questions d'ordre politique, économique, technique ou encore juridique, sont toutefois **hors du champ du présent rapport**.

B. FAIRE PROGRESSER LA RECHERCHE SCIENTIFIQUE

De façon plus spécifique, le numérique a également joué **un rôle déterminant dans la recherche sur le Covid-19**, afin de mieux connaître le virus, son génome, ses modes de propagation ou encore ses conséquences sur la santé, afin aussi de développer traitements et vaccins.

La **recherche médicale en général** s'appuie depuis longtemps sur un recours intensif au numérique, avec l'exploitation de grandes bases de données et la mobilisation de techniques d'intelligence artificielle. Si la crise du Covid-19 présente à cet égard une spécificité, ce n'est pas dans le recours au numérique, mais dans l'ampleur sans précédent de la mobilisation des chercheurs et des financements engagés. Ces sujets **n'entrent donc pas non plus dans le champ du présent rapport**.

Il y a toutefois **une exception : la modélisation épidémiologique**, **située aux confins de la recherche médicale et de la surveillance sanitaire**, et à ce titre abordée dans les développements qui suivent. En effet, la crise du Covid-19 a marqué une évolution majeure, en particulier du fait de **l'ampleur et la diversité des données collectées et utilisées pour affiner les modèles épidémiologiques**, qui sont parfois les mêmes que celles qui sont susceptibles de servir au contrôle du respect des mesures sanitaires, et qui en tout état de cause appuient très directement les décisions politiques.

Les exemples sont multiples. Parmi ceux qui seront détaillés dans les parties suivantes, on peut notamment citer l'analyse des données des opérateurs téléphoniques (**antennes GSM**) ou des géants du numérique (**géolocalisation**) pour étudier l'évolution de la mobilité et le respect des règles de confinement, l'analyse des **eaux usées** pour détecter la présence du virus, ou encore l'analyse des **recherches *Google*** portant sur les symptômes du Covid-19 pour prédire l'évolution de la maladie.

Précisons enfin que la recherche scientifique ne se limite pas à la recherche médicale : durant la crise sanitaire, **les sciences humaines, économiques et sociales ont-elles aussi eu recours à l'analyse de données** pour étudier l'impact du Covid-19 sur la société dans son ensemble – par exemple sur les inégalités entre les femmes et les hommes ou entre les différentes catégories socio-professionnelles.

C. GARANTIR LE RESPECT DES MESURES SANITAIRES

La grande spécificité de la crise du Covid-19, et le cœur du présent rapport, concerne le recours aux nouvelles technologies dans le cadre de la gestion de la crise sanitaire, en particulier pour assurer ou contrôler le respect des restrictions sanitaires : applications de *contact tracing*, de *tracking* ou de géolocalisation, pass et passeport sanitaires, utilisation de drones ou de caméras thermiques, etc. – sans compter les immenses perspectives – et les risques associés – qu'ouvrent les technologies numériques pour l'avenir.

De fait, **la gravité de la crise sanitaire** a conduit les gouvernements du monde entier à recourir à de telles solutions, parfois très intrusives, afin de freiner la progression de l'épidémie ou d'accompagner le déconfinement. Par rapport aux outils classiques de gestion d'une crise sanitaire – ou d'une crise comparable (catastrophe naturelle ou industrielle, etc.) – les outils numériques peuvent théoriquement permettre **un ciblage précis, individuel et en temps réel des mesures ou des contrôles, même si la plupart n'ont eu ni cette finalité, ni cet effet.**

Plusieurs typologies permettent d'appréhender les solutions mises en œuvre, dans leur grande diversité. On peut, par exemple, les classer :

- en fonction de leurs finalités : informer la population, protéger les personnes vulnérables, permettre la levée des restrictions, repérer voire sanctionner les contrevenants, etc. ;

- en fonction de leur degré *d'intrusivité* : certains outils reposent sur l'identification précise des personnes, leur géolocalisation et le croisement de données personnelles voire sensibles (dont les données médicales) afin de faire respecter des règles, tandis que d'autres sont anonymes, ne collectent ou ne conservent pas les données, ne débouchent sur aucune conséquence automatique ni mesure contraignante, et ne visent qu'à informer ou rendre des services ;

- **en fonction de leur caractère obligatoire ou facultatif**, avec une large gamme de nuances entre ces deux modèles ;

- **en fonction de la nature et de l'ampleur des données collectées** ;

- **en fonction des acteurs responsables de leur mise en œuvre ;**

- **en fonction des technologies utilisées ;**

- **et bien sûr selon leur efficacité.**

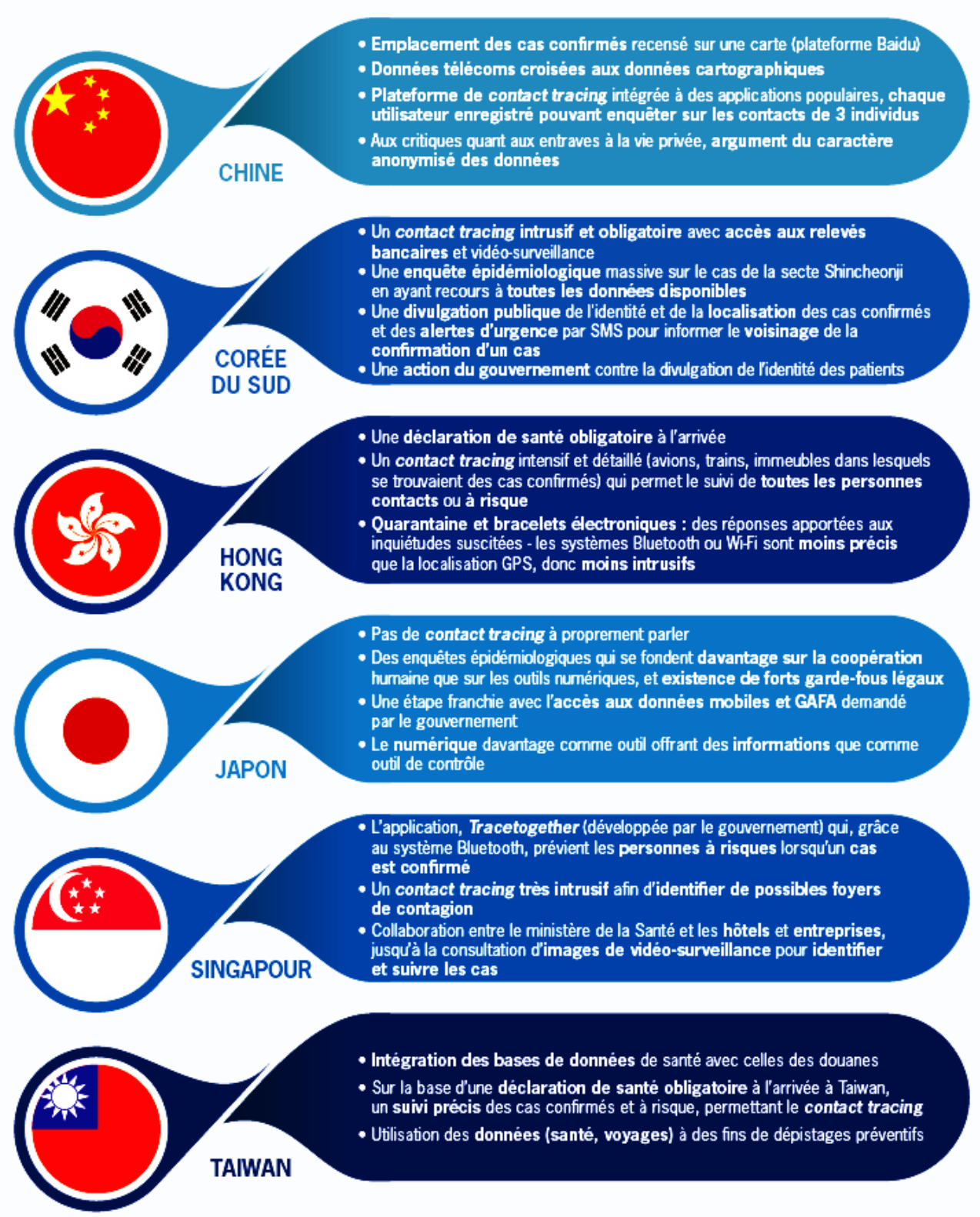
II. DÈS LE DÉBUT DE LA CRISE, LE NUMÉRIQUE A CONSTITUÉ L'UN DES PILIERS DE LA STRATÉGIE DES PAYS D'ASIE ORIENTALE

A. SIX PAYS AUX STRATÉGIES DISTINCTES

Si l'épidémie de Covid-19 a d'abord touché les pays d'Asie orientale, la situation s'est inversée dès le début de l'année 2020 : alors que l'Europe, les États-Unis puis l'Amérique du Sud étaient touchés de plein fouet, **ces pays réussissaient à freiner de façon spectaculaire la progression de l'épidémie, quand ils ne parvenaient pas l'arrêter complètement, grâce à un ensemble de mesures vigoureuses**, pour certaines éprouvées lors des épidémies précédentes (H5N1 en 1997 puis en 2007, SRAS en 2003, MERS en 2012). Ces mesures se sont appuyées sur la discipline de la population, et des facteurs culturels en général, mais aussi sur **un recours intensif aux outils numériques, y compris les plus intrusifs**.

Pourtant, tous ces pays ne sont pas des régimes autoritaires, loin s'en faut. Si le cas de la Chine peut être mis à part, celui des cinq autres pays étudiés ci-dessous montre qu'il est **possible, lorsque la population y adhère, de s'appuyer sur les technologies numériques** pour lutter contre l'épidémie, avec une très grande efficacité.

La stratégie numérique de six pays d'Asie orientale



Source : Institut Montaigne, avril 2020

L'infographie ci-dessus, tirée de la **note de l'Institut Montaigne sur la réaction des pays d'Asie orientale**[1], permet de mesurer l'importance, dès le début de l'année 2020, du volet numérique de leur stratégie. D'autres travaux conduisent aux mêmes conclusions, parmi lesquels on peut citer **l'étude rétrospective de la gestion des six premiers mois de l'épidémie**[2] **publiée par la *start-up* française Kap Code**, spécialisée dans l'analyse de signaux sanitaires à partir des données des réseaux sociaux.

1. La Chine : une mobilisation numérique générale

Premier pays touché par le Covid-19, en décembre 2019, la Chine a d'abord tardé à prendre officiellement la mesure de la menace, et plus encore à y réagir. Après une « *période initiale de déni, marquée par l'absence de mesures appropriées pour contenir l'épidémie* », pour reprendre les termes de l'Institut Montaigne, les choses se sont toutefois radicalement inversées à partir du 20 janvier 2020, avec « ***un volte-face politique (…) à l'origine de mesures de confinement inédites [et] sans égales dans le monde, adossées à des moyens et outils de contrôle résidentiel et de traçage numérique*** ».

La réponse de la Chine a alors été massive dans tous les domaines : confinement strict assorti de sanctions très fortes, construction d'hôpitaux d'urgence, mobilisation générale de l'appareil industriel pour la production de masques, d'équipements médicaux puis de vaccins, recours à l'armée, contrôle des exportations, mais aussi contrôle de l'information, propagande à l'intérieur et diplomatie d'influence à l'extérieur, afin de légitimer le récit officiel du régime sur les origines de la pandémie et de promouvoir son modèle.

Tout cela excède le cadre du présent rapport, à l'exception de l'un des aspects majeurs de la stratégie chinoise : **le recours intensif aux outils numériques sous toutes leurs formes et avec tous les types de finalités, y compris les plus intrusives, avec une ampleur inégalée non seulement dans le monde, mais aussi dans l'histoire**.

La Chine a, sans ambigüité, privilégié la lutte contre la menace sanitaire par rapport à la protection des libertés individuelles, en particulier la liberté d'aller et venir et celle d'avoir une vie privée.

Si le modèle chinois n'est évidemment pas transposable aux pays occidentaux, on ne peut pas, pour autant, se satisfaire d'une simple posture d'indignation : **la stratégie chinoise est, globalement, une grande réussite**

---

[1] *François Godement, Mathieu Duchâtel et Viviana Zhu,* « Covid-19 : l'Asie orientale face à la pandémie », *Institut Montaigne, avril 2020 :* https://www.institutmontaigne.org/publications/covid-19-lasie-orientale-face-la-pandemie

[2] *Kap Code,* « Covid-19, analyse rétrospective : Comparaison de la gestion de la crise des 6 premiers mois d'épidémie à travers le monde », *livre blanc rédigé en partenariat avec l'Inalco, TechToMed, Pons & Carrère, datacraft et 23 Consulting :* https://www.epilogue-covid.org/livre-blanc-covid19/

sur le plan sanitaire, avec officiellement 4 846 morts pour 1,4 milliard d'habitants, soit 3 morts par million d'habitants, quand la France seule compte plus de 100 000 morts, soit 1 633 morts par million d'habitants.

Les chiffres officiels sont douteux, bien sûr, mais la maîtrise de la situation ne l'est pas – et, avec elle, la levée des restrictions et le retour à une vie économique et sociale normale.

a) Les données de masse au service de la gestion de crise

Les autorités nationales et locales se sont, tout d'abord, **appuyées de façon inédite – mais sans doute durable – sur l'exploitation des données (*big data*) pour piloter la gestion de crise**, surveiller les flux de population, anticiper les évolutions et *in fine* mieux allouer les ressources de prévention et de soin, dans une période de pénurie.

Les trois **opérateurs téléphoniques** (China Telecom, China Unicom et China Mobile) et les **services de cartographie** (équivalents de *Google Maps*) ont notamment fourni leurs données et leurs analyses pour prédire les flux de population. Il en va de même pour de nombreuses grandes entreprises publiques ou privées des secteurs de **l'énergie** ou encore des **transports**.

Le recours au *big data* a également permis **d'informer les individus sur l'épidémie**, en temps réel et avec des données utiles et complètes. Par exemple, afin de permettre d'éviter les zones à risques, la plateforme *Baidu* propose **une carte montrant la localisation des personnes contaminées** ainsi que l'historique de leurs déplacements, sans pour autant révéler leur identité ni aucune autre donnée personnelle. De **nombreux services** ont par ailleurs été créés très rapidement pour faciliter la vie des habitants en période de crise : réservation en ligne de créneaux pour le dépistage puis la vaccination, entraide pour la livraison de repas à domicile, etc.

b) Le ciblage individuel du contrôle des restrictions

Si l'exploitation des données au niveau agrégé permet aux autorités de mieux piloter la gestion de crise et aux habitants de s'informer, **ces mêmes données (mobilité, géolocalisation, transactions, etc.) peuvent, à une maille individuelle, servir à contrôler le bon respect des restrictions**.

À Hangzhou, par exemple, **les données de consommation d'électricité en temps réel** ont été utilisées pour surveiller les habitants astreints à une quarantaine, mais aussi pour porter le cas échéant assistance aux personnes vulnérables.

Au travers de multiples initiatives, souvent locales ou sectorielles, la Chine a fait un usage intensif – et bien documenté – de la **vidéosurveillance avec reconnaissance faciale** pour contrôler le respect des restrictions (déplacements, port du masque, etc.). Parmi les 20 villes du monde les plus équipées en caméras de surveillance dans l'espace public, 18 dont chinoises.

À Chongqin, on compte une caméra pour six habitants, contre une pour 130 à Nice, la ville la plus équipée de France.

Il en va de même pour l'usage **des caméras thermiques connectées** pour détecter les personnes à risque.

c) La voie chinoise du contact tracing

S'agissant du *contact tracing*, c'est-à-dire la remontée des chaînes de contamination et l'identification des personnes à risque, la Chine s'est dotée d'un **dispositif ambitieux et intrusif, croisant de multiples données personnelles, sans commune mesure avec ce qui s'est fait dans les pays occidentaux**, lesquels n'ont jamais souhaité aller au-delà des enquêtes par téléphone et des applications « aveugles » comme *TousAntiCovid*.

La plateforme chinoise de **« *détecteur de contact étroit* »**, développée par China Electronics Technology Group Corporations (CETC), est **intégrée aux incontournables applications *Alipay*, *WeChat*, qui comptent chacune près d'un milliard d'utilisateurs**. Elle exploite des bases de données fournies par la Commission nationale de Santé, le ministère des Transports, China Railway ou encore l'Administration de l'Aviation civile, sans compter les données fournies par de nombreuses entreprises privées.

Pour s'inscrire, chaque **utilisateur doit obligatoirement fournir son nom, son numéro national d'identité** et son numéro de téléphone. Il a ensuite accès à des informations générales sur l'épidémie (cartes, etc.), ainsi qu'à ses propres informations médicales. **En outre, chaque utilisateur peut demander des renseignements sur trois personnes maximum**, en pratique souvent sa famille ou ses voisins, ce qui permet une forme de **surveillance par les pairs**, c'est-à-dire de contrôle social. Les médias occidentaux ont d'ailleurs abondamment relayé ce phénomène de **contrôle par le voisinage** : thermomètres à infrarouge braqués sur toute personne entrant dans l'immeuble, malades enfermés chez eux par les membres des comités de quartier, dénonciation ou pression sur les contrevenants aux règles de quarantaine ou de confinement, etc.

Les **autorités** ont également accès aux données de la plateforme, de même que les **employeurs**, les **établissements scolaires** et les comités de quartier.

d) Le premier pass sanitaire

Premier pays touché mais aussi premier pays à lever les restrictions, la Chine a, **dès le mois de mars 2020, mis en place un dispositif analogue à ce qu'est aujourd'hui le « pass sanitaire »**, adopté par la France et la plupart des pays européens (cf. *infra*). À l'époque, pourtant, il était bon ton de s'inquiéter de la « *surveillance généralisée* » induite par un tel dispositif, de l'avènement d'une « *dictature sanitaire* » et du « *virus de l'autoritarisme* ».

Développé par Alibaba (sur *Alipay*) et Tencent (sur *WeChat*), le système **repose sur un « code couleur de santé » (*Health Code*), à présenter lors des déplacements**. Celui-ci, vert, orange ou rouge, donne le statut d'immunité. Contrairement à l'application française qui implique un téléchargement du certificat par l'utilisateur lui-même, l'application chinoise est directement connectée aux bases de données de l'administration.

Plus généralement, **l'application chinoise est bien moins protectrice de la vie privée que ses équivalents occidentaux** ; celle-ci envoie notamment aux autorités, en temps réel, la localisation de l'utilisateur, comme l'a relevé le *New York Times*[1], Alibaba et Tencent ayant par la suite assuré que cette remontée se faisait avec le consentement de l'utilisateur, et qu'aucune autre donnée n'était concernée.

La « carte d'itinéraire » repose sur le même principe que le *Health Code* : l'historique des déplacements des utilisateurs, reconstitué à partir des données des opérateurs télécom, sert de preuve qu'ils ne se sont pas rendus dans une zone à risque. À son lancement, l'application attribuait un code « rouge » à toute personne qui s'était rendue dans le Hubei au cours des 14 jours précédents, et un code « jaune » à toute personne de retour de l'un des 58 pays étrangers considérés comme à risque.

Si la carte d'itinéraire est un dispositif national, il convient de préciser que **la plupart des outils évoqués ici, à commencer par le code couleur, sont mis en œuvre à un niveau local**, notamment par les villes, en fonction de leurs propres circonstances sanitaires, par l'intermédiaire de nombreuses applications, concurrentes ou complémentaires.

e) Le premier passeport vaccinal

La Chine est également **le premier pays au monde à avoir présenté un passeport sanitaire complet, incluant un certificat vaccinal**. Le passeport sanitaire, qui sera abordé en détail dans la suite du présent rapport, est l'équivalent du pass sanitaire pour les voyages internationaux.

Présenté en mars 2021, le dispositif a, là encore, été développé par *Alipay* et *WeChat*. Il acceptait, au moment de son lancement, les certificats liés aux vaccins de Pfizer-BioNTech, Moderna, Johnson & Johnson, et bien entendu les vaccins de Sinovac et Sinopharm.

f) Le crédit social : un rôle marginal dans la lutte contre l'épidémie

Durant les premiers mois de la crise sanitaire, les différents dispositifs évoqués plus haut (code couleur de santé, carte d'itinéraire, *contact tracing* intrusif, etc.) ont **souvent été confondus, dans les pays occidentaux, avec le système du « crédit social »**, ce système complexe et

[1] https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

éclaté de « notation » des individus[1] qu'il est aisé de caricaturer en une version chinoise du *Big Brother* d'Orwell.

Pourtant, celui-ci n'a joué qu'un rôle secondaire dans la réponse numérique de la Chine au Covid-19. Comme l'a souligné Séverine Arsène, chercheuse associée à Sciences Po et enseignante à l'Université chinoise de Hong Kong, lors de son audition devant la délégation à la prospective[2], le système de crédit social « *constitue paradoxalement celui qui mobilise peut-être le moins les possibilités du numérique* », par comparaison avec d'autres dispositifs tels que le code couleur, que la ville intelligente ou la vidéosurveillance. En effet, **le crédit social demeure un système assez fruste, éclaté, local, très hétérogène** en fonction des lieux et des autorités qui choisissent – ou non – de le mettre en place (sous deux formes principales : une « liste noire » ou un « permis à points »), encore très largement focalisé sur la question des dettes et des impayés, et **somme toute assez inefficace.**

Certes, ponctuellement, le système du crédit social a pu être utilisé dans le cadre de la lutte contre la pandémie de Covid-19, comme une mesure parmi d'autres[3]. Séverine Arsène indique ainsi que « *l'administration chargée de la régulation des marchés a, par exemple, adapté son système afin de pouvoir* ***sanctionner ou mettre sur liste noire des entreprises qui auraient gonflé les prix de produits essentiels****. L'administration nationale chargée de la propriété intellectuelle a inséré dans ses critères la vente de produits médicaux contrefaits.* ***Les municipalités ont plutôt ajouté des critères tels que le fait de cacher ses symptômes, pour les personnes qui voulaient éviter une hospitalisation, ou le fait de ne pas porter de masque en public****, alors que c'était obligatoire. Ce type d'information est collecté au quotidien, presque manuellement, par des employés municipaux qui vont les saisir dans des bases de données spécifiques.*

« Est-ce efficace, au-delà du Covid, d'une manière générale ? Il est difficile de le dire. Rares ont été les personnes mises sur liste noire. ***Nous avons des estimations assez vagues, selon lesquelles environ 1 % de la population des villes concernées aurait figuré dans une liste à un moment donné****. Peu de gens sont, de fait, informés de la mise en place du système, malgré la propagande et les campagnes d'information qui ont été menées. De plus, il n'y a aucune donnée comparative permettant de savoir si la situation est meilleure avec ou sans ce dispositif de crédit social* ».

---

[1] *Au sujet du crédit social, voir notamment Emmanuel Dubois de Prisque,* « Le système de crédit social : comment la Chine évalue, récompense et puit sa population », *Institut Thomas More, note de juillet 2019.*

[2] *Audition de Séverine Arsène, chercheuse associée au Médialab de Sciences Po et enseignante à l'Université chinoise de Hong Kong, sur le crédit social en Chine, 11 février 2021. Le compte rendu intégral de cette audition figure en annexe du présent rapport.*

[3] *Sur ce sujet, voir également Pierre Sel,* « L'utilisation par la Chine du système de crédit social pour gérer l'épidémie de Covid-19 », *note de France Stratégie, 28 avril 2020.*

g) Drones et robots en Chine

Au-delà des outils numériques visant à contrôler les individus afin de limiter la propagation de l'épidémie, les nouvelles technologies ont aussi été mises à contribution pour **pallier la pénurie de moyens humains** dans la crise.

Par exemple, la Chine a eu recours à **des drones pour décontaminer massivement des villes entières, en dispersant un liquide virucide dans les airs**[1], et des robots ont été utilisés pour décontaminer les services de certains hôpitaux ou encore les transports en commun. Le 3 février 2020, par exemple, toute la ville de Huangshi, peuplée de 3 millions d'habitants et située non loin de Wuhan, a été aspergée de liquide virucide par des drones et des camions[2], ciblant en particulier les routes, magasins, toilettes publiques, poubelles, marchés, arrêts de bus, etc. Pendant l'opération, les habitants avaient reçu l'ordre de rester chez eux. Les drones ont aussi été utilisés, **plus directement, pour le contrôle du respect des restrictions** (détection des rassemblements, identification des contrevenants, etc.) ou, *a minima*, pour l'information et la prévention (diffusion de messages sonores).

Des **robots humanoïdes** ont aussi été utilisés pour renforcer les équipes médicales, assurer une présence auprès des patients, ou encore apporter des repas aux personnes confinées chez elles.

La Chine n'est toutefois pas le seul pays à avoir fait appel aux robots, même si cela y a été plus visible qu'ailleurs. Aux **États-Unis**, par exemple, des drones ont été utilisés par Walmart pour assurer des livraisons de nourriture, de médicaments ou autres kits de tests[3]. En France, même, **la RATP** a étudié la possibilité de recourir à des robots pour nettoyer les bus et rames de métro, avant de renoncer.

2. La Corée du Sud : le suivi jusqu'à la surveillance ?

La Corée du Sud est, avec Hong Kong, Singapour et Taïwan, l'un des pays d'Asie orientale – et du monde – dont **la réaction à l'épidémie a été la plus rapide, et par conséquent la plus efficace** : les premières mesures ont été prises dès le 3 janvier 2020, soit 17 jours avant les premiers cas détectés dans le pays et immédiatement après « l'alerte » de Wuhan.

Elles ont notamment consisté en **une campagne de dépistage massif**, **entièrement gratuite** et organisée *via* des *drive-through* (sans qu'il soit nécessaire de descendre de sa voiture). Au-delà du dépistage, **la prise en charge par l'État** s'étend aux **soins médicaux** (pour tous les patients, quelle que soit leur nationalité), ainsi qu'à **l'indemnisation des quarantaines** spontanées.

---

[1] *Un drone peut disperser du spray virucide sur une surface de 16 000 mètres carrés en une demi-journée.*
[2] *https://www.sciencesetavenir.fr/sante/coronavirus-quel-liquide-les-drones-deversent-ils-dans-les-rues-de-chine_141210*
[3] *https://www.usine-digitale.fr/article/covid-19-walmart-livre-des-kits-de-test-par-drone.N1008289*

L'aspect le plus notable de la stratégie sud-coréenne est que le pays a dès le début fait le choix du ***ciblage*** **plutôt que des mesures généralisées, et n'a notamment jamais mis en place de confinement ni fermé ses frontières**. En revanche, des **quarantaines individuelles obligatoires** (à domicile, pendant 14 jours), des fermetures ciblées (bars, discothèques, lieux de cultes, etc.), des interdictions d'entrée ciblées (pour les voyageurs en provenance des régions à risque) et des contrôles sanitaires systématiques aux frontières ont été mis en place.

Surtout, cette stratégie de ciblage s'est appuyée sur **un usage intensif du numérique, avec un *contact tracing* intrusif et obligatoire**, les autorités pouvant exploiter dans leurs enquêtes des données aussi sensibles que les **relevés bancaires, les factures téléphoniques détaillées, l'historique de géolocalisation, les images de vidéosurveillance publique ou encore les informations transmises par les administrations et employeurs**.

Afin de garantir leur efficacité, **les quarantaines individuelles ont fait l'objet d'une surveillance stricte**, *via* une application de **géolocalisation**, déjà utilisée en 2015, qui sonne et alerte directement les forces de l'ordre si les personnes concernées se déplacent, ou si le *smartphone* est éteint pendant plus de 15 minutes, formant ainsi une véritable « **clôture électronique** » (« *electronic fence* »). Afin de vérifier que la personne n'est pas sortie de chez elle sans son *smartphone*, les autorités l'appellent aléatoirement deux fois par jour, et n'hésitent pas à se déplacer. **Le voisinage peut être prévenu par SMS** de la présence d'une personne contagieuse. Enfin, les manquements font l'objet de **sanctions très dissuasives**, allant jusqu'à l'équivalent de **8 257 dollars et un an de prison.**

Ces mesures peuvent sembler très liberticides, mais il faut d'emblée rappeler que celles-ci, précisément parce qu'elles se sont avérées très efficaces et qu'elles ont permis au pays de **repasser sous la barre des 100 cas par jour en moins de deux semaines** (sur une population de 52 millions d'habitants) et de s'y maintenir durablement, **ont en pratique concerné très peu de monde, tandis que le reste de la population en était épargné**. Du reste, la stratégie mise en place par le gouvernement sud-coréen a, jusqu'à la récente remontée du nombre de cas (cf. *infra*), **bénéficié d'un très large soutien de la population**, celle-ci faisant preuve à la fois de solidarité, de discipline, parfois de zèle[1] et toujours d'**ouverture à l'égard du numérique**.

Cette stratégie a porté ses fruits : début mai 2021, la Corée du Sud ne comptait que **36 morts par million d'habitants** (soit environ 1 800 décès), quand la France déplorait au même moment 1 573 morts par million d'habitants (soit plus de 100 000 décès).

[1] *Fin janvier, une pétition signée par 540 000 Sud-Coréens réclamait une interdiction d'entrée pour tous les voyageurs chinois. Un mois plus tard, 500 000 personnes signaient une pétition réclamant l'interdiction de la secte Shincheonji.*

Il reste que, pour les personnes concernées, ces mesures intrusives posent avec acuité la question du respect de leur vie privée.

En particulier, les informations collectées à l'occasion des enquêtes de *contact tracing* étaient intégrées au sein d'un **registre public, librement accessible**, indiquant la nationalité des personnes, leur âge, leur sexe, le lieu de leur visite médicale, la date de leur contamination, et des informations encore plus précises telles que leurs horaires de travail, le respect du port du masque dans le métro, les stations empruntées, les bars et autres salons de massage fréquentés, etc. **Bien que non nominatives, ces informations permettaient parfois d'identifier facilement les personnes concernées** avec des applications dédiées, conduisant à des phénomènes de stigmatisation ou de dénonciation[1]. **Constatant les dérives du système, le gouvernement a toutefois réagi en mettant fin à cette possibilité un mois plus tard**.

Le premier *cluster* sud-coréen, apparu fin février 2020 dans la ville de Daegu suite à un rassemblement des **fidèles de la secte chrétienne Shincheonji**, montre combien les mesures peuvent être rigoureuses : face à la multiplication par six du nombre de cas détectés en seulement trois jours, les autorités ont exigé – et obtenu – **la communication immédiate de la liste des 210 000 membres de l'organisation** et soumis ces derniers à une enquête intrusive, en les géolocalisant grâce à leurs téléphones portables, tandis que le fondateur du mouvement, Lee Man-hee, était contraint à des excuses publiques à la télévision.

3. Taïwan : la chance de l'insularité, le choix du *big data*

Comme la Corée du Sud, Hong Kong et Singapour, et instruit par l'expérience de l'épidémie de SRAS qui avait fortement touché le pays en 2003, **Taïwan a réagi dès les premiers signes d'alerte en Chine**, instituant des contrôles renforcés près de trois semaines avant les premiers cas détectés sur l'île.

Les mesures, fortes et ciblées, ont permis au pays de n'être **presque pas touché par le Covid-19, tout en échappant à un confinement généralisé**. Début mai 2021, soit près d'un an et demi après le début de l'épidémie, Taïwan ne comptait que **12 décès et 1 100 cas positifs**, pour une population de 24 millions d'habitants, soit **3,5 morts par million d'habitants**, officiellement au troisième rang mondial[2]. Sur ces 1 100 cas positifs, 984 étaient des **cas « importés »**, détectés lors de la quarantaine obligatoire des voyageurs

De fait, tirant parti de son **insularité**, le pays a concentré sa stratégie sur le **strict contrôle des frontières**, instituant très tôt une **déclaration de santé obligatoire** à l'entrée sur le territoire, doublée de **vérifications intrusives**, notamment grâce à **l'interconnexion des bases de données de la**

[1] https://www.bbc.com/news/world-asia-51733145

[2] *Voire mieux, les chiffres du Vietnam et de la Tanzanie étant moins fiables en raison d'un plus faible dépistage.*

police aux frontières, des bases de données des **transporteurs aériens** et des bases de données **médicales**. Lors du passage de la frontière, les autorités peuvent ainsi vérifier les antécédents médicaux des voyageurs ; quant aux hôpitaux, ils ont accès à l'historique des voyages. Il s'agit là d'un **système sophistiqué, reposant sur une exploitation systématique du *big data***, et non d'un usage « artisanal » des données au cas par cas.

Une fois entrés sur le territoire, les voyageurs et personnes à risque sont soumis à une **quarantaine obligatoire de 14 jours**. Celle-ci est là encore **étroitement surveillée** grâce à la mobilisation du numérique : un **téléphone est fourni par les autorités** pour surveiller les déplacements grâce à la géolocalisation, et celles-ci peuvent accéder aux **données des téléphones personnels**. **En cas de violation** de la quarantaine, la sanction peut aller jusqu'à l'équivalent de **33 241 dollars, et l'identité des contrevenants est rendue publique**, ce dispositif de « ***name and shame*** » ayant pour l'occasion été doté d'une base législative.

Au-delà du ciblage des personnes à risque, le numérique a marqué deux autres aspects de la stratégie taïwanaise : **la lutte contre la désinformation sur Internet**, fortement sanctionnée, et la **mobilisation pour les masques** (au détriment des vaccins, cf. *infra*), dont la production a été quasi nationalisée et l'exportation interdite, et dont **la disponibilité était visible en temps réel *via* une application dédiée**.

4. Singapour : le pionnier du *contact tracing*

La réaction de Singapour présente de nombreux points communs avec celle de ses voisins asiatiques : une réaction rapide, un contrôle obligatoire et systématique des voyageurs, **une quarantaine obligatoire surveillée par géolocalisation par GPS**, ou encore **l'exploitation des images de vidéosurveillance** pour identifier les interactions des individus. La réponse sanitaire de la cité-État a été gérée conjointement par le ministère chargé de la Santé et le ministère chargé de la *Smart Nation* et de la gouvernance digitale, signe d'une priorité accordée aux outils numériques.

Si ces mesures **n'ont pas permis à Singapour d'échapper au confinement** (finalement décrété début avril 2020 face à la deuxième vague, dans le cadre d'une stratégie « zéro Covid »), contrairement à la Corée du Sud et à Taïwan, elles se sont néanmoins révélées **très efficaces**, au moins dans un premier temps, et en tout état de cause bien davantage que les mesures des pays européens.

Singapour est, surtout, **le premier pays au monde à avoir déployé, mi-mars 2020, une application de *contact tracing*, appelée *Trace Together***, fonctionnant grâce à la technologie *Bluetooth*. Les enjeux du *contact tracing* seront abordés plus en détails dans la suite du présent rapport. À ce stade, on peut toutefois signaler deux grandes spécificités.

D'une part, **l'usage de *TraceTogether* est obligatoire pour certaines catégories de population**, comme les travailleurs migrants, **et dans certains lieux**, notamment les écoles, bureaux, restaurants, cinémas ou centres commerciaux. Si le nombre de téléchargements a été dans un premier temps moindre qu'attendu (un million au bout d'un mois, pour une population de 6 millions d'habitants), elle est aujourd'hui **utilisée par près de 80 % de la population** – même si son efficacité, comme ailleurs dans le monde, est très incertaine.

D'autre part, **dans le cas particulier de Singapour, l'usage d'une telle application n'est pas sans risques pour la vie privée** et les droits et libertés des citoyens. *TraceTogether* est en effet construite sur une architecture dite « centralisée » (cf. *infra*), également retenue par *TousAntiCovid* en France, mais très minoritaire dans le monde. Dans ce modèle, **les données relatives aux interactions sociales des individus sont traitées par un serveur central**, géré par l'administration. En principe, celles-ci **ne doivent en aucun cas être utilisées pour d'autres finalités** que celles qui ont justifié leur collecte, c'est-à-dire la lutte contre l'épidémie de Covid-19. Le gouvernement de Singapour avait, naturellement, **pris des engagements formels** en ce sens, assurant que seules les autorités sanitaires auraient accès aux données.

Toutefois, en janvier 2021, **le gouvernement a reconnu devant le parlement que la police avait eu accès aux données de *contact tracing* du serveur central**, dans le cadre d'une enquête pour meurtre[1]. **Or *TraceTogether* n'est pas anonyme**, puisqu'il faut s'enregistrer pour pouvoir utiliser l'application, à la différence cette fois de *TousAntiCovid*. Finalement, le ministre de l'Intérieur a indiqué qu'il considérait que la police pouvait accéder à ces données, sur le fondement du code de procédure pénale, suscitant la colère de certains habitants estimant avoir été « trompés ».

Bien que le cas de Singapour ne soit pas transposable à la France ou aux autres pays occidentaux, **un tel épisode est très préjudiciable à la crédibilité du discours politique sur l'utilisation du numérique face à une crise sanitaire** – par des outils qui, en principe, ne devraient faire que cela.

Singapour est, enfin, l'un des premiers pays à avoir institué un **pass sanitaire**[2], avec l'application *SafeEntry*, qui permet de scanner le *QR code* apposé sur des « checkpoints » à l'entrée des gares, centres commerciaux, parcs, bâtiments publics, etc. Cette application se distingue de son équivalent français à deux égards :

- d'une part, si l'accès à certains lieux est, comme France, obligatoirement conditionné à l'usage de ce dispositif, **les lieux qui ne sont pas soumis à cette obligation sont vivement encouragés** à le mettre en place volontairement, alors qu'ils en ont l'interdiction en France ;

---

[1] *https://www.lepoint.fr/high-tech-internet/singapour-les-donnees-de-l-appli-anti-covid-accessibles-a-la-police-05-01-2021-2408207_47.php*

[2] *https://www.numerama.com/tech/622089-apres-lechec-du-stopcovid-local-singapour-passe-a-une-solution-beaucoup-plus-radicale.html*

- d'autre part, et contrairement au pass sanitaire français, *SafeEntry* donne lieu à la **collecte de données personnelles** à chaque « checkpoint », permettant aux autorités de savoir qui s'est rendu à quel endroit et à quelle heure.

5. Hong Kong : bracelet électronique ou *smartphone* ?

Face à la crise sanitaire, et comme les pays voisins**, Hong Kong a pris des mesures précoces, vigoureuses et largement fondées sur le recours au numérique** : *contact tracing* intrusif et minutieux pour les personnes contaminées ou à risque, fondé sur l'exploitation de multiples données (avions, trains, immeubles, etc.), contrôles systématiques aux frontières avec déclaration sanitaire, quarantaine obligatoire dans des centres dédiés, etc. Il a cependant fallu attendre le 25 mars pour que le gouvernement se résolve à fermer la frontière avec la Chine continentale, ce qui a sans doute affaibli la stratégie sanitaire de Hong Kong. En fait, et peut-être encore davantage qu'ailleurs, **l'autodiscipline et la solidarité communautaire semblent avoir joué un rôle important** pour freiner l'épidémie, de même que l'expérience des récentes épidémies, expliquant la priorité accordée très tôt aux masques.

Une spécificité de Hong Kong mérite d'être signalée : **le recours à des bracelets électroniques pour assurer le respect de la quarantaine**, en complément d'autres mesures telles que les visites inopinées, les appels vidéo surprise, et bien sûr les sanctions dissuasives (amende de 641 dollars et 6 mois d'emprisonnement). Délivré à l'aéroport, ce bracelet doit obligatoirement activé à l'arrivée sur le lieu de quarantaine (souvent un centre dédié) *via* l'application *StayHomeSafe*, et **tout changement de position est enregistré et notifié aux autorités**, c'est-à-dire le département de la Santé mais aussi la police.

Si l'image du bracelet électronique peut légitimement déranger, il convient toutefois de signaler que **la technologie est en réalité moins intrusive que le *tracking* par GPS** mis en place par d'autres pays asiatiques, car le bracelet utilise le *Bluetooth* ou le *Wifi*, moins précis. En outre, si **60 000 bracelets** avaient été commandés en mars 2020 dans la perspective de l'entrée en vigueur de cette obligation, il faut souligner que ce chiffre ne correspond à **rien d'autre qu'au confinement *potentiel* de 60 000 personnes sur une population de 7,5 millions d'habitants[1], là où les pays occidentaux, dont la France, faisaient le choix de confiner tout le monde sans se donner les moyens de contrôler personne, ou presque.**

Une seconde spécificité concerne **le contexte politique particulier de la région administrative spéciale**, marqué par la réaction des autorités aux manifestations « pro-démocratie » qui dénoncent, notamment, l'ingérence de

[1] *Ce qui ne signifie pas, bien sûr, que seules 60 000 personnes pourraient être touchées par les restrictions, compte tenu des mesures telles que les fermetures d'établissements etc.*

Pékin dans les affaires intérieures. Si la question excède le champ du présent rapport, on peut toutefois remarquer que ce contexte **complique la lecture de la stratégie sanitaire du gouvernement local, à la fois pour l'observateur extérieur, mais aussi pour les habitants**, qui ont pu voir dans les restrictions sanitaires, puis aujourd'hui dans la campagne de vaccination, un acte politique hostile de la part de la Chine. Cela rappelle que **l'acceptabilité des mesures sanitaires** est, partout dans le monde, intimement liée au contexte politique et historique de chaque pays.

Or, de fait, les autorités ont parfois eu **recours à des mesures bien plus « physiques » que « numériques »** pour faire respecter les règles, alimentant la défiance d'une partie de la population. Par exemple, face à la vague apparue début 2021, les forces de l'ordre ont adopté **une stratégie de confinement « embuscade »**, pour reprendre les mots de la cheffe de l'exécutif, Carrie Lam, consistant à boucler par surprise un quartier entier et à soumettre tous ses habitants à un test, y compris en forçant l'entrée des appartements. La première opération de ce type, menée le 23 janvier dans le quartier pauvre de Jordan, avait conduit 7 000 personnes à rester bloquées chez elles pendant 44 heures – pour 13 cas positifs détectés.

Il reste qu'Hong Kong ne comptait, début mai 2021, que **210 morts dus au Covid-19, soit 28 morts par million d'habitant**, un chiffre très bas et d'autant plus remarquable que la ville est l'une des plus ouvertes à la mondialisation, et donc du brassage des individus.

6. Le Japon : pas de numérique… pas de Jeux olympiques ?

Parmi les pays évoqués ici, le Japon est, de loin, celui qui a le moins recouru à des mesures fortes, et *a fortiori* à des outils numériques. L'Archipel n'a ainsi jamais décrété de confinement, n'a pas mené de campagne de dépistage massif, n'a pas utilisé d'application de *contact tracing*, n'a pas surveillé le respect des quarantaines, et n'a réussi à vacciner qu'une petite partie de sa population (6 % à ce jour pour deux doses).

Le Japon est aussi – faut-il y voir un hasard ? – celui de ces pays qui est le plus touché par l'épidémie, avec 13 000 morts à ce jour, soit 102 morts par million d'habitant, bien loin des 3 ou 4 morts par million d'habitants de ses voisins (mais certes en deçà des 1 633 morts par million d'habitants de la France). **En réalité, le pays a essentiellement compté sur l'autodiscipline de ses habitants et, de fait, cela s'est révélé suffisant dans un premier temps** : la circulation du virus s'est maintenue à un niveau très bas jusqu'en janvier 2021, avant d'augmenter ensuite, contraignant le gouvernement à décréter **un troisième état d'urgence sanitaire (toujours sans confinement) à trois mois des Jeux olympiques**.

B. UNE EFFICACITÉ DIRECTEMENT LIÉE À L'INTRUSIVITÉ

D'une manière générale, entre efficacité sanitaire et respect des libertés individuelles, l'arbitrage des pays asiatiques a clairement penché en faveur de la première : **leurs diverses stratégies reposent sur des mesures particulièrement intrusives**, sans équivalent dans les pays occidentaux.

De fait, cette stratégie semble avoir porté ses fruits : ces pays ont la plus faible mortalité du monde rapportée à leur population.

Nombre de morts et de cas confirmés par pays au 5 mai 2021

	Rang sur 155	Morts pour 1M d'hbs	Décès	Cas confirmés
Vietnam	2	0,4	35	2 985
Taïwan	3	3,5	12	1 145
Chine	6	3,5	4 846	102 549
Thaïlande	8	4,0	276	71 025
Singapour	10	5,5	31	61 235
Hong Kong	37	28	210	11 791
Corée du Sud	41	36	1 840	124 269
Japon	62	82	10 391	609 625
Danemark	94	430	2 491	254 368
Israël	104	717	6 367	838 621
Estonie	108	887	1 172	122 943
Allemagne	116	1 008	83 605	3 412 373
Lettonie	124	1 118	2 154	119 953
Lituanie	130	1 418	3 956	250 337
France	**136**	**1 573**	**105 387**	**5 656 007**
États-Unis	142	1 765	577 566	32 637 456
Royaume-Uni	144	1 922	127 797	4 423 796
Brésil	146	1 951	408 622	14 791 434
Italie	147	2 009	121 433	4 059 821
Hongrie	155	2 857	27 908	784 111

Source : Johns Hopkins Coronavirus Resource Center

Ainsi, au 5 mai 2021, et avec 12 décès seulement, Taïwan comptait 3,5 morts par million d'habitants, au 3e rang mondial, suivi de peu par la **Chine** (6e rang) puis **Singapour** (10e rang, avec 31 décès, soit 5,5 morts par million d'habitants). La France, quant à elle, se situe au 136e rang mondial sur 156 (compte tenu des *ex aequo*), avec 1 573 morts par million d'habitants, non loin des États-Unis (142e) et du Brésil (146e), deux pays qui ont notoirement refusé de s'appuyer sur des outils de contrôle intrusifs.

Si l'on peut douter des chiffres officiels de la Chine, on ne peut pas raisonnablement douter de ceux de Taïwan, de Singapour ou de la Corée du Sud. Corrélation, bien sûr, n'est pas causalité, et d'autres facteurs sont

susceptibles de contribuer à ce résultat : l'insularité (Taïwan, Japon) ou la quasi-insularité (Corée du Sud, *de facto*), le taux d'urbanisation et donc d'intensité des interactions sociales, la structure démographique et en particulier la pyramide des âges, des prédispositions génétiques ou une immunité acquise lors d'épidémies précédentes, etc. **Toutefois, même en tenant compte de tous les autres facteurs possibles, il est impossible d'expliquer de tels résultats sans reconnaître le rôle majeur joué par les outils numériques, et leur caractère particulièrement intrusif.**

Par ailleurs, si la stratégie de ces pays s'est appuyé sur un ensemble de mesures dont le numérique n'est qu'une partie, il convient de **ne pas opposer outils numériques et restrictions « physiques »**. Au contraire, ces mesures sont complémentaires : une stricte quarantaine, par exemple, n'a de sens que si elle peut être effectivement contrôlée. En contrepartie, ces mesures peuvent être plus ciblées et limitées dans le temps.

C. L'ASIE VICTIME DE SON SUCCÈS ?

La stratégie des pays asiatiques a toutefois, pour ainsi dire, les défauts de ses qualités. **Forts du succès de leur stratégie d'élimination du virus, ces pays ont accumulé un retard important dans la campagne de vaccination**, négligeant de commander suffisamment de doses, et au point même de dépendre aujourd'hui du mécanisme Covax de l'OMS (pour la Corée du Sud et Taïwan, notamment). Certains ont aussi fait de mauvais paris, à l'instar de la Thaïlande, qui avait misé sur le vaccin Astra Zeneca. Quant à la Chine, elle produit ses propres doses, mais en consacre la moitié à sa « diplomatie vaccinale ». D'une manière générale, **la défiance de la population de ces pays à l'égard des vaccins y est très forte**, comme symétrique de leur confiance envers les technologies numériques : seuls 14 % des Sud-Coréens et 22 % de Japonais se disaient prêts à se faire vacciner en janvier[1], et ils sont aujourd'hui respectivement 9,1 % et 6,4 % de la population à avoir reçu au moins une première dose.

Depuis peu, ces pays sont donc confrontés à un rebond de l'épidémie, qui avait pourtant presque disparu, si ce n'est totalement. Taïwan a ainsi connu 671 cas et 13 morts pour la seule journée du 27 mai. Le pays compte aujourd'hui près de 8 000 cas déclarés, soit sept fois plus que la totalité des cas (1 100) identifiés entre mars 2020 et avril 2021, et a dû se résoudre à de nouvelles restrictions, tout en évitant le confinement.

Car, et c'est le deuxième inconvénient de cette stratégie, ces pays sont très vulnérables aux cas « importés » depuis les pays qui, eux, n'ont pas été capables de contenir le virus – offrant ainsi un terrain propice à l'émergence de nouveaux variants, dont certains, à l'instar de celui

[1] *Selon une étude Ipsos citée par* Le Monde *du 29 mai :* https://www.lemonde.fr/planete/article/2021/05/29/l-asie-en-retard-sur-les-vaccinations_6082019_3244.html

récemment apparu en Inde, sont particulièrement inquiétants. Or les frontières ne peuvent rester indéfiniment fermées, et l'économie ne peut durablement être maintenue à l'arrêt.

Encore faut-il ne pas surestimer l'ampleur de ce retournement, pour l'instant modéré (malgré la hausse relative du nombre de cas, Taïwan compte seulement 5 morts par million d'habitants, Singapour 6 morts par million d'habitants), ni les ressources dont disposent ces pays pour réagir. Il ne faut pas non plus en conclure à l'inefficacité de leur stratégie initiale, mais plutôt que celle-ci aurait dû être mise en œuvre de manière coordonnée par un maximum de pays, et surtout, qu'elle **ne saurait en aucun cas dispenser d'une stratégie de vaccination ambitieuse, lorsqu'il existe un vaccin**.

Surtout, le récent retournement plaide plutôt pour *davantage* de numérique, plutôt que pour *moins* de numérique : face à une situation qui se dégrade brutalement, ces outils sont le meilleur moyen de réagir à court terme sans revenir à des restrictions généralisées, pour ***filtrer* les frontières** plutôt que de les refermer, pour ***cibler* les fermetures** plutôt que de les imposer à tous, etc.

III. DANS LE MONDE ENTIER, LE NUMÉRIQUE S'IMPOSE COMME UN ÉLÉMENT-CLÉ DE LA SORTIE DE CRISE

Au début de l'année 2020, les outils numériques mis en place dans les pays asiatiques suscitaient, dans la presse occidentale, des commentaires à tout le moins réservés, et souvent empreints de méfiance. Six mois plus tard, l'essentiel de ces outils (*contact tracing*, pass sanitaire, etc.) avaient été repris dans leur principe, et **le numérique constitue, avec la vaccination, l'un des piliers des stratégies de sortie de crise**.

Toutefois, d'une manière générale, **l'arbitrage fait par les pays occidentaux entre protection des libertés individuelles et préservation de la santé publique** diffère singulièrement de celui des pays asiatiques.

Pour autant, on constate là encore une grande diversité des cas individuels. Ainsi, les pays les plus avancés en matière d'**administration numérique,** comme l'Estonie, ont bénéficié d'un avantage précoce dans leur gestion de la crise (**A**). Ceux qui ont opté pour une **stratégie « zéro Covid »**, visant à éliminer le virus plutôt qu'à s'en accommoder, ont également fait un usage plus intensif des outils numériques (**B**). Toutefois, pour la grande majorité des pays occidentaux, dont la France, la « conversion » s'est faite plus tardivement, et plus partiellement, au travers de trois outils principaux : **le *contact tracing*, le passeport sanitaire et le pass sanitaire** (**C**).

A. L'AVANTAGE COMPARATIF DE L'ÉTAT-PLATEFORME

1. L'Estonie, une administration digitale face à la crise

Lorsque l'épidémie de Covid-19 a frappé l'Europe, **les pays les plus avancés en matière de numérisation des services publics** ont bénéficié d'un avantage notable, non seulement dans la continuité de l'activité en général, mais aussi – et surtout – dans la gestion de la crise sanitaire.

C'est notamment ce que montre **l'exemple de l'Estonie**, sur lequel s'est notamment penché l'Institut Montaigne, dans une note au titre signifiant : *« Les États face au coronavirus – L'Estonie, ou le numérique en action*[1] ». L'Estonie, en effet, se classe **au premier rang européen en matière de e-administration**, alors que la France n'est que douzième[2].

---

[1] *Morgan Guérin,* « Les États face au coronavirus – L'Estonie, ou le numérique en action », *Institut Montaigne, 6 mai 2020 : https://www.institutmontaigne.org/blog/les-etats-face-au-coronavirus-lestonie-ou-le-numerique-en-action*

[2] *Indice relatif à l'économie et à la société numériques (DESI) pour 2020. Cet indicateur synthétique publié depuis 2014 est composé de 37 indicateurs répartis en cinq grands domaines : connectivité, capital humain, utilisation d'internet, intégration des technologies numériques et services publics numérique. C'est dans ce dernier domaine que l'Estonie se classe systématiquement première. Voir notamment : https://ec.europa.eu/commission/presscorner/detail/fr/QANDA_20_1022*

L'État-plateforme en Estonie

Indépendante depuis 1992 et membre de l'Union européenne depuis 2004, **l'Estonie a lancé la transformation numérique de ses services publics dès la fin des années 1990, partant pour ainsi dire d'une page blanche** après le retrait de l'URSS, là où des pays comme la France doivent composer avec des siècles de construction administrative et, déjà, des décennies d'informatisation de l'administration. À cela s'ajoute l'avantage d'une **population réduite (1,3 million d'habitants), particulièrement confiante et ouverte à l'égard du numérique**, et d'un écosystème de *start-ups* très dynamiques.

Les services publics sont dès l'origine conçus comme des « **applications** », disponibles sur une **plateforme**, à l'instar d'un *App Store* ou d'un *Google Play*, où chaque usager dispose d'un **identifiant unique**. L'ensemble repose sur une **infrastructure unique**, mais décentralisée et cryptée, la ***X-Road***, lancée en 2000 et exportée dans plus de 20 pays depuis.

Ainsi, 96 % des démarches administratives se font en ligne : payer ses impôts, consulter son dossier médical, renouveler une ordonnance, créer une société, immatriculer sa voiture, demander un permis de construire, voter, porter plainte, déclarer la naissance d'un enfant, l'inscrire à la crèche, à la cantine ou à l'école, et même consulter ses bulletins scolaires – soit près de 3 000 services au total, proposés par quelque 900 acteurs publics comme privés (banques, assurances, transports, télécoms, etc.). Le taux de dématérialisation atteint 100 % pour les entreprises. **L'administration n'a pas le droit de demander deux fois la même information, et 90 % des formulaires sont pré-remplis**, contre seulement 40 % en France.

D'après le gouvernement estonien, qui a fait de la digitalisation de son administration un véritable élément de *soft power* (comme en témoigne le showroom *e-Estonia* de Tallinn), cette dématérialisation ferait gagner l'équivalent d'une semaine de travail par an à chaque citoyen estonien, pour une économie budgétaire de 2 % du PIB.

Les premiers cas de Covid-19 ont été détectés le 27 février 2020, à la suite d'une visite de l'équipe de volley-ball de Milan sur l'île de Saaremaa. **Le gouvernement a réagi très rapidement**, prenant en une vingtaine de jours une série de mesures restrictives : fermeture des frontières aux non-ressortissants, contrôles sanitaires systématiques, quarantaine obligatoire, campagne de dépistage massive, etc.

Il s'est, en outre, appuyé sur le numérique. Quelques heures après la déclaration de l'état d'urgence sanitaire, le gouvernement estonien a ainsi annoncé **l'organisation d'un *hackathon***, « *Hack the crisis* », qui s'est déroulé entièrement en ligne du 13 au 15 mars. En moins de 48 heures, près de mille participants avaient proposé une trentaine de projets. Certains ont par la suite bénéficié de financements de la part de fonds d'investissements. Plusieurs autres *hackathons* ont été organisés en Estonie pendant la crise, et une cinquantaine d'autres pays ont fait de même, dont la France.

Dans sa note de mars 2021, l'Institut Montaigne cite notamment quatre outils numériques qui ont, plus tôt qu'ailleurs, distingué l'Estonie :

- **un tableau de bord interactif**[1] pour suivre en temps réel et de façon détaillée l'évolution de l'épidémie, comprenant notamment **une carte** (***KoroonaKaart***) et également disponible sous forme d'application. L'initiative est proche du tableau de suivi de ***Covid Tracker*** en France (cf. *infra*), et aujourd'hui de celui de Santé Publique France, à cela près qu'il a été mis en place très tôt en Estonie, et directement intégré à la plateforme publique d'*open data*, là où plusieurs moins ont été nécessaires à la France ;

- **un *chatbot* (*Suve*) pour répondre aux questions des citoyens**[2] à n'importe quelle étape de leur recherche d'information sur la maladie, grâce à l'intelligence artificielle qui permet notamment d'enrichir continuellement les réponses. Cet outil représente non seulement un guichet unique appréciable pour les usagers, mais aussi une économie budgétaire notable par rapport aux multiples centres d'appels répartis entre les administrations, comme ce fut – et c'est encore – le cas dans de nombreux pays. Développé en *open source*, il permet aux développeurs extérieurs de contribuer à l'amélioration des réponses ;

- **un questionnaire en ligne pour l'auto-évaluation médicale des utilisateurs**[3]**, permettant à ceux qui le souhaitent de partager directement leurs informations** avec l'administration, afin de mieux suivre l'évolution de l'épidémie. Comme d'autres pays, la France a elle aussi mis en place des outils similaires, mais plus tardivement, et avec une portée bien moindre (il s'agit notamment d'applications tierces disponibles *via* l'espace numérique de santé, pour les Français encore peu nombreux qui y ont accès). Surtout, le système français a une fonction purement médicale (suivre l'état de santé d'un patient), et ne permet pas d'exploiter les données de façon plus large, notamment dans le cadre du suivi épidémiologique ;

- **la plateforme *Covidhelp*, permettant de mettre en relation des personnes âgées et vulnérables avec des soignants volontaires** : développée en à peine 48 heures par la *start-up* Zelos à partir d'une solution standard (l'outil de gestion de tableaux de bord *Trello*), cette application a permis de recruter 2 000 volontaires sur l'ensemble du territoire. C'est un exemple-type de ce que peut faire le numérique, et de ce que ne sait pas faire notre administration.

Ces différents outils n'ont pas **grand-chose en commun avec les dispositifs bien plus intrusifs déployés dans les pays asiatiques**. Pourtant, ils ont joué un rôle important dans la gestion de crise, et ceci dès le début.

---

[1] https://koroonakaart.ee/et

[2] https://eebot.ee/ et https://investinestonia.com/estonia-created-suve-an-automated-chatbot-to-provide-trustworthy-information-during-the-covid-19-situation/

[3] https://coronatest.ee/

2. Les leçons de l'exemple estonien

S'il est difficile de mesurer précisément l'avantage ainsi procuré, on peut à tout le moins noter que **l'Estonie est restée relativement préservée de l'épidémie par rapport à ses voisins**, et par rapport aux pays européens en général. Au 5 mai 2021, le pays ne comptait que 887 morts par million d'habitants, alors que ses proches voisins, la Lettonie et la Lituanie, comptaient respectivement 1 118 et 1 418 morts par million d'habitants. Si le taux d'incidence était en revanche plus élevé (95 cas pour 100 000 habitants, contre 63 cas pour la Lettonie et 89 cas pour la Lituanie), cet écart s'explique très vraisemblablement par la politique de dépistage bien plus ambitieuse de l'Estonie, dont la logistique s'est d'ailleurs appuyée dès le début sur des outils numériques matures.

De l'exemple estonien, l'Institut Montaigne tire **trois leçons**. **Premièrement, une telle stratégie ne s'improvise pas** : l'Estonie a entamé sa transition vers l'État-plateforme dès la fin des années 1990, et s'appuie aujourd'hui sur une infrastructure intégrée à partir de laquelle il est facile de construire de nouveaux services. **Deuxièmement, l'expérience utilisateur (ou *user experience* – UX) importe beaucoup**, qu'il s'agisse de la présentation des données publiques ou de l'accessibilité et de l'ergonomie des services. **Troisièmement, ce succès doit beaucoup à la fructueuse coopération entre secteurs public et privé, que facilite le modèle d'État-plateforme** : toutes les solutions évoquées ci-dessus ont été conçues par des *start-ups*, et directement intégrées à la plateforme publique par laquelle chaque citoyen peut accéder à l'ensemble des services publics.

L'OMS elle-même ne s'y est pas trompée : c'est avec la *start-up* estonienne Guardtime qu'elle a conclu en octobre 2020 un partenariat pour construire **une plateforme – *VaccineGuard* – qui allait devenir à la fois un système de gestion logistique de la campagne vaccinale et le support du passeport sanitaire** (cf. *infra*), bien avant que les Européens ne lancent leur propre projet[1]. La plateforme *VaccineGuard* a en effet pour objectif de relier entre eux différents agents, **depuis le point de fabrication du vaccin (sérialisation des flacons) jusqu'au garde-frontière contrôlant un voyageur individuel (certificat de vaccination), en passant par les centres de vaccination,** créant un système dans lequel des informations fiables sur le processus de vaccination peuvent être partagées entre une myriade de sources et de pays différents. **La technologie de Guardtime est basée sur la *blockchain***, qui rend infalsifiable les informations (cf. *infra*).

[1] *Avant le « certificat vert » européen, plusieurs pays ont lancé des initiatives en ce sens. L'Islande et la Hongrie avaient notamment rejoint l'Estonie et décidé d'adopter la technologie de Guardtime, elle-même développé en partenariat avec d'autres entreprises, dont la* biotech *française OpenHealth et la société de cybersécurité suisse SICPA. Voir à ce sujet : https://www.zdnet.fr/actualites/l-idee-d-un-passeport-vaccinal-connecte-fait-son-chemin-chez-les-geants-du-numerique-39916639.htm et https://www.sicpa.com/news/covid-19-health-passport-secured-blockchain-enable-deconfinement.*

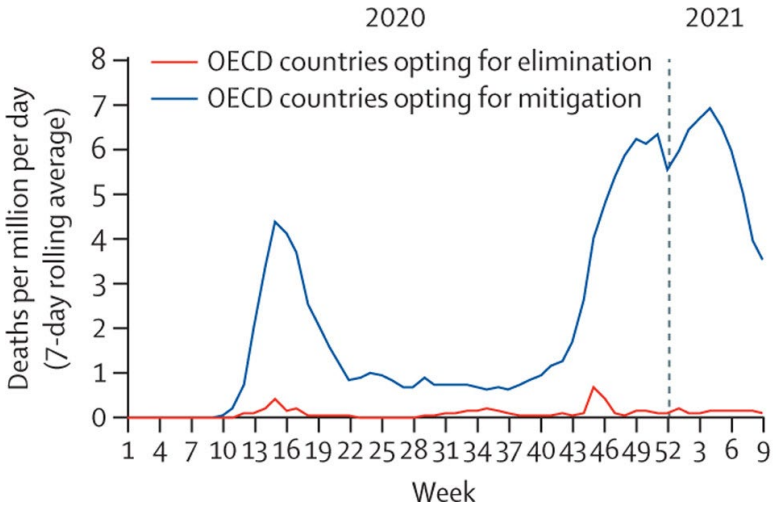
B. UN RÔLE-CLÉ DANS LE SUCCÈS DE LA STRATÉGIE « ZÉRO COVID »

1. L'élimination du virus, plus efficace que l'atténuation

Alors que la plupart des pays occidentaux – dont la France – ont opté pour une stratégie d'« atténuation » de l'épidémie, consistant à « vivre avec » le virus pour ne pas restreindre les libertés individuelles ou pénaliser l'économie, **quelques pays ont à l'inverse opté pour une stratégie d'« élimination » du virus, dite stratégie « zéro Covid »**, visant à en finir le plus vite possible avec l'épidémie, quitte à supporter dans un premier temps des restrictions plus fortes. C'est le cas non seulement des pays asiatiques évoqués précédemment, mais aussi de quelques pays occidentaux.

Or il apparaît de plus en plus clair que la stratégie « zéro Covid » est plus efficace que la stratégie d'atténuation. Dans une étude remarquée publiée le 28 avril 2021 dans *The Lancet*[1], des chercheurs issus de plusieurs disciplines ont comparé les effets des deux stratégies dans les 37 pays de l'OCDE sur une durée de 12 mois. Il apparaît clairement que **les cinq pays qui ont choisi la stratégie d'élimination – Australie, Nouvelle-Zélande, Islande, Japon et Corée du Sud – ont obtenu de meilleurs résultats**, non seulement en matière de santé, objectif premier des mesures, mais aussi en matière économique et en matière de protection des libertés.

Nombre de morts du Covid-19 par jour dans les pays de l'OCDE selon la stratégie retenue (élimination ou atténuation)



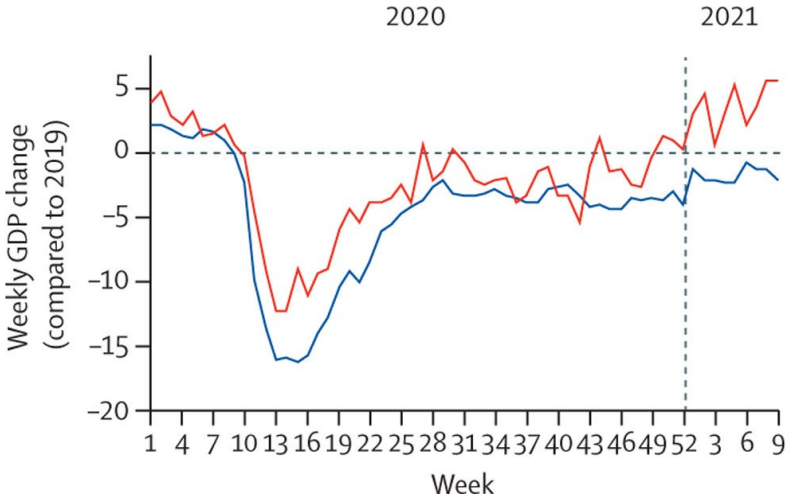
Source : The Lancet, *étude du 28 avril 2021 précitée.*

[1] *Miquel Oliu-Barton, Bary S. R. Pradelski, Philippe Aghion, Patrick Artus, Ilona Kickbusch, Jeffrey V. Lazarus et al.*, SARS-CoV-2 elimination, not mitigation, creates best outcomes for health, the economy, and civil liberties, *The Lancet, 28 avril 2021 :* https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(21)00978-8/fulltext

En matière sanitaire, tout d'abord, le nombre de morts par million d'habitants dans les pays « zéro Covid » a été 25 fois inférieur à celui constaté dans les pays choisissant de « vivre avec » le virus.

En matière économique, ensuite, on aurait pu s'attendre à un prix à payer plus fort pour les pays adoptant les mesures les plus vigoureuses (fermeture des entreprises et des transports, etc.). Or c'est tout le contraire qui s'est passé. Les cinq pays concernés ont d'ores et déjà tous retrouvé leur niveau de PIB d'avant-crise. Mais surtout, **l'évolution hebdomadaire de leur PIB a systématiquement été plus favorable que celle des autres pays, tout au long de la crise**, avec une moindre chute et une reprise plus forte.

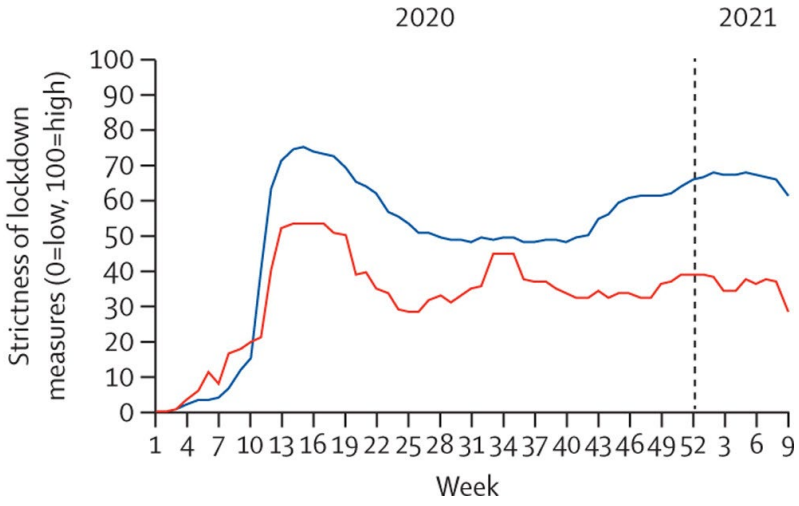
Variation hebdomadaire du PIB dans les pays de l'OCDE selon la stratégie retenue (élimination ou atténuation)



Source : The Lancet, *étude du 28 avril 2021 précitée.*

En matière de libertés publiques, enfin, l'étude livre sans doute son résultat le plus intéressant : alors que la stratégie d'élimination repose par définition sur des mesures plus sévères (confinements stricts, contrôles systématiques, etc.), **il apparaît que ces restrictions n'ont été plus fortes que pendant les trois premières semaines de la pandémie – alors que les pays plus « permissifs » se retrouvaient acculés à des mesures finalement bien plus attentatoires aux libertés, prises trop tard et maintenues sur la durée**, sans pour autant produire de meilleurs résultats en matière sanitaire ou économique. Les auteurs insistent d'ailleurs sur le fait que « ***la stratégie d'élimination a été conçue comme une approche civique et solidaire, visant à rétablir les libertés publiques le plus rapidement possible ; cet objectif d'intérêt général est fréquemment ignoré dans le débat politique*** ».

Restrictions des libertés dans les pays de l'OCDE selon la stratégie retenue (élimination ou atténuation)



Source : The Lancet*, étude du 28 avril 2021 précitée.*

*NB : le caractère plus ou moins strict des mesures est évalué sous la forme d'un indice (*strigency index*) développé par des chercheurs de l'université d'Oxford et publié dans la revue* Nature[1]*. Cet indice combine huit indicateurs relatifs aux mesures de confinement (écoles, entreprises, événements publics, rassemblements, transports publics, confinement à la maison, restrictions aux déplacements internes, restrictions aux voyages internationaux) et huit indicateurs relatifs à la politique de santé publique (campagnes d'information, tests,* contact tracing*, investissements d'urgence, investissement dans les vaccins, port du masque, vaccination, autres).*

Des restrictions plus fortes pendant une période limitée semblent donc plus efficaces sur le plan sanitaire, sur le plan économique, et sur le plan des libertés publiques. Naturellement, il importe de ne pas confondre corrélation et causalité. Par exemple, il est possible que la faible mortalité constatée dans ces cinq pays s'explique en partie par leur **insularité**[2]. Mais les résultats constatés dans les pays non insulaires qui ont également fait le choix d'une stratégie « zéro Covid », même tardive, suggèrent que cela ne saurait constituer la seule explication. En Europe, c'est par exemple **le cas de l'Écosse**, dont la stratégie d'élimination diffère de celle, plus permissive, de l'Angleterre.

[1] *Thomas Hale, Noam Angrist, Rafael Goldszmidt et al.,* A global panel database of pandemic policies (Oxford COVID-19 Government Response Tracker), *Nature Human Behaviour, 8 mars 2021 : https://www.nature.com/articles/s41562-021-01079-8*

[2] *Ou la quasi-insularité* de facto*, dans le cas de la Corée du Sud.*

La stratégie « zéro Covid » de l'Écosse

Extraits de l'interview de Devi Sridhar,
professeure de santé publique à l'université d'Edimbourg
***et conseillère du gouvernement écossais* (Le Monde *du 24 mars 2021*)**

Quelle est la situation en Écosse actuellement ?
Elle est bonne mais fragile. (…) Notre espoir est d'avoir immunisé tous les adultes d'ici à la mi-juillet. (…) En parallèle, il y a une grande pression pour alléger les restrictions, car tous les indicateurs vont dans le bon sens. Hier, pour la première fois depuis des mois, nous n'avons enregistré aucun mort. (…)

Quelle a été la particularité de l'approche écossaise ?
Elle s'est mise en place en avril 2020. Jusque-là, nous suivions la position anglaise. Mais, quand le gouvernement britannique a indiqué qu'il voulait juste aplatir la courbe, nous avons estimé que ***nous pouvions faire mieux que ça : l'écraser****. Et nous l'avons fait, grâce à des mesures de restriction plus longues. Le virus avait à peu près disparu d'Écosse l'été dernier. Pendant un mois, plus aucun mort, plus d'hospitalisations. Mais, en août, le tourisme a repris, sans quarantaine. Et la deuxième vague est arrivée. Lentement d'abord. (…) Mais, avec le variant B.1.1.7, à la fois plus contagieux et plus sévère, nous avons été contraints de mettre en place un confinement dur.*

Nous sommes parvenus à faire redescendre les chiffres. Et l'enjeu est de les maintenir à ce niveau tout en ouvrant peu à peu avec tous les outils disponibles. La vaccination, les tests, massifs et de toute nature, le traçage des cas contacts. Avec une nouveauté : des restrictions draconiennes sur les voyages. Nous avons retenu la leçon. Toute personne arrivant de l'étranger subit une quarantaine dans un hôtel, quel que soit le pays de provenance. Notre seul problème, c'est que l'Angleterre ne suit pas la même approche. Un visiteur peut arriver à Londres et prendre le train. C'est notre talon d'Achille. L'Europe continentale, avec ses frontières terrestres, connaît bien ce problème.

Quel a été le rôle de la science dans vos choix ?
Nous nous sommes constamment appuyés sur les preuves scientifiques. (…) Nous avons fait des études, mais aussi essayé de ***profiter de ce que les autres pays faisaient, notamment en Asie****. C'est une approche humble mais essentielle. Comme pour le vaccin : nous pouvons construire des modèles massifs sophistiqués, c'est très bien, ou alors profiter de l'exemple israélien, du Chili, des États-Unis. Ne pas avoir peur d'apprendre des autres : ne pas répéter leurs erreurs et se servir de leurs réussites.*

Avez-vous été surpris par l'apparition du variant britannique ?
Nous savions que les pathogènes évoluaient, bien sûr. (…) Alors nous avons décidé de confiner rapidement. Personne n'aime confiner. On en connaît les dégâts. ***Mais, s'il faut confiner, mieux vaut le faire vite, fermement, et en sortir vite****. Et grâce à ça nos services hospitaliers n'ont jamais été sous pression comme en Angleterre.*

Comment jugez-vous la réaction de l'Europe continentale, notamment de la France, face au variant ?
Étonnamment lente. Il suffisait de regarder l'Angleterre et de se dire qu'on ne voulait pas subir la même chose. ***Mais les gouvernements semblent incapables de faire ça****. (…)* ***En France, il y a cette idée de préserver l'économie en restant ouvert aussi longtemps que possible. C'est comme rouler en voiture vers un mur et affirmer qu'en freinant le plus tard possible on gagnera du temps. Vous perdez sur tous les tableaux : économique et sanitaire. Vous avez les morts et la crise****.*

Il n'y a que deux manières efficaces de combattre cette pandémie. ***Soit le modèle de l'élimination complète, celui choisi par les pays d'Asie, l'Australie, la Nouvelle-Zélande*** *: le virus n'est plus là, vous pouvez attendre tranquillement l'arrivée des vaccins, votre économie roule et vous surveillez le moindre retour de flamme.* ***Soit vous vaccinez massivement et aussi rapidement que possible votre population, comme Israël et les États-Unis le font****. Les autres options, celles du Brésil, de la Suède ou de la France, si différentes soient-elles, ne sont pas raisonnables. (…)*

Pourquoi les gouvernements occidentaux ont-ils si mal géré la crise, comparativement aux pays asiatiques ou africains ?
D'abord on s'est trompé de modèle, pensant que le virus allait agir comme la grippe, un pathogène que l'on n'arrête pas*. Quand on a vu que les pays asiatiques parvenaient à le stopper, on n'a pas trop su comment faire. C'est un virus très rusé.* ***Trop sévère pour vivre avec sans mettre en péril nos systèmes sanitaires, mais pas assez pour nous faire peur et entraîner une réponse massive et coordonnée****.*
De plus, il frappe les plus âgés, les plus pauvres, les obèses, les malades. Pour le combattre, les jeunes et ***les gens bien portants doivent faire des sacrifices qui profiteront aux plus vieux et aux plus fragiles. En Asie, c'est une évidence****. Ça ne l'est pas pour nous. Doit-on sacrifier les plus âgés ? Ici, nous nous sommes posé la question. Là-bas, c'était impensable. Ils savent que le tissage entre générations et entre conditions constitue la trame de notre tissu social.* ***Pour l'avoir oublié, nous avons payé très cher****.*

Source : https://www.lemonde.fr/planete/article/2021/03/24/covid-19-en-france-vous-perdez-sur-tous-les-tableaux-vous-avez-les-morts-et-la-crise_6074316_3244.html

Par ailleurs, de nombreuses études sont venues documenter **l'impact psychologique des restrictions**, moins visible immédiatement mais sans doute plus durable et plus insidieux, plaidant ainsi la cause des stratégies d'élimination rapides Dans une étude de modélisation épidémiologique, les chercheurs de l'Inserm ont élaboré **un indicateur synthétique de « détresse », construit à partir des données de mobilité**[1] des Français et reflétant les restrictions aux libertés individuelles liées aux différentes mesures de lutte contre l'épidémie (confinement plus ou moins strict, couvre-feu, etc.). Mesuré sur une échelle de 1 à 10, cet indicateur est « *imparfait, mais cela donne une idée de la fatigue "accumulée" par les Français dans le temps, et de l'impact psychosocial de différentes stratégies* », et reflète « *les*

[1] *Il s'agit des mêmes données de l'opérateur Orange, évoquées en première partie du présent rapport.*

conséquences psychosociales de ces restrictions comme l'anxiété, le sentiment de perte de sens, l'inquiétude face à l'avenir[1] ». En appliquant deux scénarios fictifs à l'Île-de-France, les chercheurs concluent que **le niveau de « détresse » lié à un confinement strict de deux semaines est comparable à celui d'un confinement modéré de deux mois** ; en revanche, dans le second cas, le nombre de décès et d'hospitalisations est beaucoup plus élevé.

2. Le numérique au service de l'élimination

Or, parmi les principales mesures susceptibles d'être mises en œuvre dans le cadre d'une stratégie d'élimination, les outils numériques jouent un rôle important.

Le cas du Japon et de la Corée du Sud a été évoqué plus haut. S'agissant de **l'Australie**, elle est l'un des premiers pays occidentaux à avoir mis en place une application de *contact tracing*, *COVIDSafe App*, qui n'est autre qu'une reprise de l'application *Trace Together* de Singapour. Elle est aussi l'un des premiers pays à avoir testé le passeport et le pass sanitaires. C'est également le cas de **l'Islande**. La stratégie de la **Nouvelle-Zélande**, l'un des premiers pays considérés comme « *Covid-free* », est en revanche davantage fondé sur une stricte fermeture des frontières, soutenue par une grande majorité de la population, même si les équipes de *contact tracing* ont été particulièrement mobilisées.

Tout cela ne signifie donc pas que les outils numériques puissent à eux seuls suffire à éliminer le virus. Les stratégies « zéro Covid » reposent en effet sur un **ensemble de mesures complémentaires** (fermeture des frontières, quarantaines obligatoires, etc.), dont le recours au numérique n'est qu'un volet parmi d'autres. De fait, et d'une manière générale, les outils numériques utilisés contre l'épidémie de Covid-19 restent **techniquement immatures** et **politiquement risqués**, ce qui limite leur efficacité, y compris dans le cadre d'une stratégie d'élimination.

En revanche, à l'avenir, les outils numériques pourraient bien constituer l'élément essentiel de toute stratégie d'élimination rapide d'une épidémie, notamment dans une situation où aucun traitement ni vaccin n'est disponible. En effet, ceux-ci **correspondent très précisément au principe de cette stratégie** : intervenir de la façon la plus précise, la plus rapide et la plus individualisée possible – avec, en échange, la promesse de restrictions bien plus limitées dans le temps, pour le plus grand bénéfice de la collectivité.

Comme Taïwan ou Singapour, les pays occidentaux qui ont opté pour la stratégie « zéro Covid » se trouvent aujourd'hui confrontés à une résurgence de l'épidémie.

---

[1] *Vittoria Colizza, citée par* Le Monde *du 20 mai 2021 : https://www.lemonde.fr/planete/article/2021/05/19/covid-19-la-difficile-evaluation-de-la-fatigue-pandemique-due-aux-restrictions_6080720_3244.html*

3. Des atteintes parfois fortes aux libertés individuelles

Si les atteintes généralisées aux libertés fondamentales sont le plus souvent restées de l'ordre du fantasme (cf. *infra*), le recours aux outils numériques par les pays occidentaux les plus volontaristes s'est dans certains cas accompagné de **pratiques sensiblement plus intrusives que dans la plupart des autres pays**, pour un surcroît d'efficacité incertain.

Par exemple, la **Pologne** a mis en place une application réservée aux personnes placées en quarantaine. Celles-ci pouvaient recevoir un SMS inopiné, qui leur donnait **20 minutes pour envoyer un *selfie* aux forces de l'ordre**, lesquelles vérifiaient alors qu'il s'agissait de la bonne personne et qu'elle se trouvait au bon endroit. Faute de réponse, la police pouvait le cas échéant se déplacer, constater l'infraction et sanctionner les contrevenants.

À l'instar de la Chine, la **Russie** a fait un usage intensif de la **vidéosurveillance**, y compris avec reconnaissance faciale.

En **Israël**, c'est le service de renseignement intérieur, le *Shin Bet*, qui a été chargé en mars 2020 par le gouvernement d'identifier les cas contacts, en **croisant des données de localisation et des réseaux sociaux**, avant que la Cour suprême ne l'interdise.

Il est reste toutefois délicat, à ce jour, de porter un jugement définitif quant à l'opportunité ou à la proportionnalité de telles mesures : elles sont certes plus intrusives que celles de la plupart des pays occidentaux, et n'auraient du reste pas été légales en France (cf. *infra*), mais les outils les moins intrusifs ont, comme on le verra, été largement inefficaces. Elles sont, par contre, moins intrusives que celles des pays asiatiques, et leur finalité – contenir l'épidémie – n'est pas contestable soi.

C. TROIS OUTILS EN VOIE DE GÉNÉRALISATION POUR ACCOMPAGNER LA SORTIE DE CRISE

Pour la grande majorité des pays occidentaux, dont la France, la « conversion » aux outils numériques s'est faite plus tardivement, plus partiellement, et plus douloureusement.

Trois outils, tous mis en œuvre en Asie dans un premier temps, se sont progressivement imposés : le ***contact tracing* numérique**, dont la finalité est plutôt de freiner la progression de l'épidémie, le **passeport sanitaire** et le **pass sanitaire**, ceux-ci visant surtout à accompagner la sortie de crise – même si ces différentes finalités dépendent surtout, en réalité, du moment où les outils sont adoptés.

1. Le *contact tracing*

À la fin du premier semestre 2020, **de nombreux pays occidentaux, dont la majorité des pays européens, ont décidé de développer des applications nationales de *contact tracing***, en s'inspirant des applications mises en place notamment par Singapour et la Corée du Sud, ou encore par l'OMS dans la lutte contre le virus Ebola. Compte tenu de la sensibilité du sujet pour l'opinion publique, ce développement s'est dans un premier temps déroulé dans une relative confidentialité, **avant d'être, à partir de l'été 2020, pleinement assumé par les différents gouvernements**. Les conditions de leur déploiement varient toutefois selon les pays, en fonction notamment du degré d'*intrusivité* de la solution retenue, et des circonstances où son utilisation est obligatoire ou encouragée.

Dans sa version numérique, **le *contact tracing* exploite les données des *smartphones* des individus**, afin d'identifier les personnes susceptibles d'être contaminées et de les inviter, le cas échéant, à se faire dépister et/ou à s'isoler, pour briser les chaînes de transmission du virus.

Le *contact tracing* (ou traçage de proximité, *promixity tracing*), doit être distingué du *tracking* (ou suivi) : il vise seulement à déterminer qu'une personne a été au contact d'au moins une autre personne positive au Covid-19 au cours des derniers jours, grâce à la **technologie *Bluetooth*** qui permet à deux *smartphones* de reconnaître qu'ils sont à proximité l'un de l'autre, **sans pour autant révéler l'identité de l'autre personne** (les identifiants sont chiffrés), ni la localisation géographique des terminaux. **À l'inverse, les systèmes de *tracking* reposent sur la géolocalisation précise des terminaux, soit par GPS, au mètre près, soit par bornage sur les antennes GSM**.

Les enjeux techniques et politiques du *contact tracing* seront abordés **en détails dans la deuxième partie du présent rapport**, notamment à travers l'exemple de la France, dont l'application *StopCovid* (devenue *TousAntiCovid*) présente d'importantes singularités.

Toutefois, d'une manière générale, on peut d'ores et déjà préciser qu'**à lui seul, le *contact tracing* ne constitue nullement une solution miracle**, mais qu'il doit plutôt se concevoir comme un outil parmi d'autres, dans une logique de complémentarité. Ainsi, alors même que l'application a été massivement téléchargée et utilisée par leur population, des pays comme **Singapour ou le Royaume-Uni n'ont pas échappé à des mesures de confinement particulièrement strictes**.

De fait, le *contact tracing* est soumis, tout d'abord, à des **limitations technologiques** : la portée du *Bluetooth* est limitée à quelques mètres, peu précise et dépendante de paramètres tels que le modèle du *smartphone*, le niveau de sa batterie ou encore sa position (dans la main, dans un sac, etc.).

Ensuite, cette technique fournit des **informations incomplètes**, susceptibles de générer de nombreux faux positifs : elle ne dit rien, par exemple, de l'environnement (intérieur ou extérieur), de la position des personnes, de leur physiologie, de leur charge virale, du respect des gestes barrières (en particulier le port du masque), etc. Ces biais ne peuvent être atténués que par des hypothèses statistiques nécessairement fragiles.

Enfin, l'efficacité du *contact tracing* **dépend de la fiabilité du modèle épidémiologique sous-jacent**, encore très changeant et incertain : combien de temps faut-il rester à proximité pour qu'il y ait un risque de contamination significatif ? La transmission se fait-elle plutôt par aérosols, qui restent longtemps dans l'air, ou par gouttelettes, plus lourdes ? Etc.

Surtout, son efficacité dépend étroitement de son adoption par la population, qui est demeurée relativement faible (avec un taux moyen d'environ 20 %) et toujours facultative, alors que de la plupart des pays asiatiques étudiés ci-dessus l'avaient tout simplement rendue obligatoire.

2. Le passeport sanitaire

Il convient de distinguer deux types de dispositifs, qui peuvent être fondés sur la même technologie mais dont le périmètre d'application est différent : le « **passeport sanitaire** » pour voyager d'une part, et le « **pass sanitaire** » pour accéder à certains lieux d'autre part (cf. partie dédiée).

Moins « *high tech* » que les algorithmes de *contact tracing* mais sans doute plus importants pour la sortie de crise, ces dispositifs numériques reprennent le principe ancien du carnet de vaccination papier, en y ajoutant d'autres critères (tests et preuve d'infection) et en garantissant un haut niveau de sécurité et de fiabilité.

a) Dans le monde

Le passeport sanitaire constitue un instrument-clé de la réouverture des frontières. Il ne s'agit pas *stricto sensu* d'un passeport, titre d'identité officiel délivré par un État permettant à ses ressortissants de voyager à l'étranger, mais d'une **preuve numérique de leur immunité**. Celle-ci, sous la forme par exemple d'un *QR code*, permet d'attester d'un test négatif, d'une vaccination, ou encore d'une guérison.

La Chine, dont les frontières sont fermées depuis mars 2020, a très tôt annoncé le sien, qui a été **lancé officiellement le 9 mars 2021**, dans une version pour l'instant facultative, réservée à ses ressortissants et intégrée à l'application *WeChat*. On peut également citer le cas de **l'Inde**, ou encore du **Royaume-Uni**, dont le passeport numérique, disponible *via* l'application du NHS, est exigé depuis mi-mai. Juridiquement, celui-ci n'est pas obligatoire, mais il l'est *de facto* : ceux qui n'ont pas ou ne souhaitent pas utiliser de *smartphone* doivent adresser une demande pour obtenir un courrier officiel.

Toutefois, parmi les pays qui ont développé un passeport sanitaire national, certains devraient *in fine* se rallier au « certificat vert européen », reconnu de façon plus large. C'est notamment le cas de **l'Islande**, membre de l'Espace Schengen, qui avait pourtant présenté son dispositif dès le mois de janvier 2021.

Le secteur privé a ici joué un rôle majeur, en particulier le secteur aérien qui a subi une perte de quelque 510 milliards de dollars en 2020 et une chute de 75 % de son trafic. Déjà familière de la gestion, *via* sa base de données **TIMATIC**, des innombrables règles nationales applicables aux voyages internationaux[1], **l'Association internationale du transport aérien (IATA) a développé un « *Travel Pass* »**, inauguré en mars 2020 par Singapore Airlines. D'autres initiatives, concurrentes ou complémentaires, sont également développées par Air France-KLM (*via* l'application *AOK Pass*, testée sur les vols Paris-Outre-mer), Lufthansa, Air New Zealand, etc. À terme, l'objectif est bien de faire converger ce *Travel Pass* avec le passeport sanitaire là où il existe, et le cas échéant de l'intégrer aux applications de voyage de chaque compagnie.

De **nombreuses entreprises privées** – *start-ups*, *biotechs*, géants du numérique, etc. – se sont également positionnées comme prestataires pour le développement du passeport (international) ou du pass (domestique) sanitaire – la technologie sous-jacente étant la même. Par exemple, l'alliance formée par plusieurs entreprises (Microsoft, Oracle, Salesforce, Cerner, Epic, etc.) dans le cadre de la *Vaccine Credentiel Initiative* (VCI) développe une technologie permettant de conserver une preuve de vaccination sur son téléphone, dans un « *Health Wallet* ».

b) Le certificat vert numérique européen

Le « certificat vert », dans sa version papier ou numérique, est **la version européenne du passeport sanitaire**.

En Europe, les pays dépendants de l'activité touristique – Grèce, Italie, Espagne, Portugal, etc. – ont très tôt appelé à la mise en place d'une telle solution au niveau européen, et l'ont parfois déjà adoptée au niveau national (la Grèce a par exemple signé un accord bilatéral avec Israël en ce sens). **Initialement, la France, l'Allemagne ou encore les Pays-Bas y étaient opposés**, pointant notamment les risques en matière de droits et libertés, et surtout la prise en compte, dans les premiers projets, du seul critère de la vaccination, alors même que celle-ci n'avait pas débuté.

---

[1] *Créée en 1963 et gérée par l'IATA, la base de données TIMATIC (*Travel Information Manual Automatic*) contient la liste de toutes les règles et recommandations applicables aux voyageurs internationaux par voie aérienne : passeport, visa, règles sanitaires, taxes d'aéroport, règles douanières, etc. Les règles applicables, en perpétuelle évolution, sont collectées auprès de quelque 1 800 sources officielles différentes. Afin de mettre en place le* Travel Pass*, la base TIMATIC a été enrichie de nouveaux champs : résultats des tests, certificats de vaccination et règles nationales applicables.*

Les choses ont toutefois évolué rapidement, avec la sensibilité de l'opinion, et alors que des dispositifs « internes » (pass sanitaires) étaient par ailleurs mis en place dans plusieurs pays.

Le 17 mars 2021, la Commission européenne a présenté son projet de « certificat vert numérique », dont l'objectif est de faciliter la libre circulation en toute sécurité dans l'Union européenne durant la pandémie de Covid-19. Ce certificat présentera les caractéristiques suivantes[1] :

- il sera **gratuit** et **facultatif** ;

- il sera disponible **sous forme électronique**, à présenter sur un *smartphone*, ou **sous forme papier** ;

- il comportera un ***QR code*** contenant les informations nécessaires et garantissant sa sécurité et son authenticité ;

- il couvrira **trois types de certificats** : certificats de **vaccination**, résultats des **tests de dépistage** (PCR ou antigéniques), et certificats de **guérison** du Covid-19.

Ce certificat n'implique pas la mise en place d'une politique européenne en matière de circulation : **les États-membres demeureraient libres de décider des restrictions applicables aux voyageurs** (quarantaines obligatoires, tests et vaccins reconnus, délais applicables, etc.). En revanche, ils devront appliquer les assouplissements **de la même manière à tous les voyageurs titulaires d'un certificat vert, sans discrimination**.

Le projet présenté par la Commission européenne a été adopté par le Parlement européen le 29 avril. Deux jours plus tôt, la France, qui y était initialement opposée, devenait le premier État-membre à présenter par anticipation un dispositif correspondant (partiellement). Si les négociations ne sont pas tout à fait terminées à ce jour, **le certificat vert devrait en principe permettre les voyages au sein de l'UE à partir du 1er juillet 2021**.

Celui-ci a vocation à être intégré dans les différentes applications nationales : d'un point de vue technique, il n'y a donc pas de développement d'une application européenne. En revanche, le projet prévoit la mise en place d'un portail européen pour assurer la compatibilité des pass nationaux entre eux, afin que les autorités d'un État-membre puissent vérifier l'authenticité du document présenté par le ressortissant d'un autre. Le développement de cette infrastructure a été confié aux **entreprises allemandes SAP et T-Systems**, qui ont déjà développé le portail permettant l'interopérabilité des applications de *contact tracing* (à l'exception de *TousAntiCovid*, cf. *infra*), ainsi que l'application allemande *CoronaWarnApp*.

La Commission européenne indique que le certificat vert constitue une **mesure temporaire, qui sera suspendue dès que l'OMS aura déclaré la fin de l'urgence sanitaire internationale** liée à la pandémie de Covid-19.

---

[1] *Source : https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_1181*

Il semble toutefois **peu probable – et pas souhaitable –** que ce système, une fois mis en place sur le plan technique, **ne soit pas *a minima* conservé ensuite dans un état de « veille »**, prêt à être réactivé facilement en cas de nouvelle menace épidémique.

En réalité, il est même assez probable qu'il devienne un dispositif permanent, dans la mesure où :

- **nul ne sait quand se terminera la pandémie**, ni si sa fin au niveau mondial correspondra à sa fin en Europe, ni surtout **où et quand les prochaines épidémies apparaîtront** ;

- la flexibilité et la fiabilité du dispositif en font **un candidat naturel pour remplacer les multiples dispositifs existants tels que le carnet de vaccination ou encore du « certificat jaune » mise en place sous l'égide de l'OMS pour la fièvre jaune**[1]. Il serait ainsi possible d'attester très facilement du respect des milliers de critères sanitaires fixés par tous les pays du monde, et d'intégrer l'ensemble aux systèmes d'informations des compagnies aériennes et gestionnaires d'infrastructures, fluidifiant ainsi le « parcours » des voyageurs ;

- la politique européenne en la matière **dépend également de la réciprocité appliquée par certains pays**. Or il est probable que d'autres pays fassent le choix de se doter d'un dispositif pérenne, à commencer par la Chine qui l'a annoncé très tôt, ou les pays dont la situation sanitaire le requiert.

Bien entendu, si le passeport sanitaire devait à terme devenir aussi nécessaire pour voyager qu'un titre d'identité, il faudrait alors répondre à de nombreuses questions relatives, notamment, à la **protection des droits et libertés des voyageurs**.

Du reste, il n'est en est pour l'instant pas question officiellement, et le 20 avril dernier, le comité d'urgence de l'OMS s'est déclaré, dans un communiqué, opposé à la mise en place d'un passeport vaccinal obligatoire, « *étant donné les preuves limitées (bien que croissantes) concernant la performance des vaccins sur la réduction de la transmission et étant donné l'inégalité persistante en matière de distribution mondiale des vaccins* ».

3. Le pass sanitaire

Le « pass sanitaire » n'est autre que la version « domestique » du passeport sanitaire, c'est-à-dire **un certificat permettant d'accéder à certains lieux ou à certaines activités**. Là encore, les pays asiatiques ont été les premiers à le mettre en place, à commencer par la Chine avec le système de *QR code* disponible *via WeChat* (cf. *supra*).

---

[1] *Modèle de certificat international de vaccination ou de certificat attestant l'administration d'une prophylaxie, en vigueur depuis le 15 juin 2007. La fièvre jaune est la seule maladie qui doit obligatoirement figurer dans ce certificat, pour les voyageurs se rendant dans les pays concernés.*

Parmi les premiers pays occidentaux à l'avoir mis en place, on compte notamment Israël, l'Australie, l'Islande, l'Estonie, le Danemark, la Grèce, Chypre, la Hongrie ou encore la Pologne. L'un des exemples les plus connus est celui d'**Israël, dont le « *green pass* » est, avec une campagne de vaccination massive et précoce, l'un des deux piliers** d'un déconfinement effectif depuis mi-février. Au sein de l'Union européenne, c'est **le Danemark** qui a donné l'exemple, suivi depuis par la Belgique, les Pays-Bas, l'Autriche et même l'Allemagne, où celui-ci dispense notamment du respect des règles de couvre-feu.

Le pass sanitaire (*Coronapas*) au Danemark

En avance sur ses voisins européens, **le Danemark a fait du pass sanitaire (*Coronapas*) le pilier de sa stratégie de déconfinement et de réouverture**. Testé dès le mois de mars 2021 avec les zoos, utilisé depuis le 6 avril 2021 pour aller chez le coiffeur, à l'institut de beauté ou encore à l'auto-école, il permet depuis le 21 avril d'accéder aux bars, cafés, restaurants, musées, bibliothèques, tribunes et stades de sport et, depuis le 6 mai, aux cinémas et aux salles de spectacle.

Le *Coronapas* danois présente plusieurs spécificités qui méritent d'être signalées, en comparaison notamment de la stratégie française :

- il est **obligatoire** pour les plus de 15 ans ;

- il est **directement intégré au compte santé sécurisé** des citoyens : comme en Estonie (cf. *supra*), les Danois peuvent accéder à la plateforme *via* une application pour *smartphone* dédiée (*Min Sundhed*). Celle-ci contient l'ensemble de leur dossier médical, y compris donc les résultats des tests et les preuves de vaccination ou d'infection. Une application spécifique au *Coronapas* et au passeport sanitaire vient d'être lancée, avec un *QR code*, mais celle-ci permet toujours d'importer les résultats depuis le dossier médical ;

- les infractions sont **fortement sanctionnées** : les petits commerces encourent ainsi une amende de 295 euros, doublée en cas de récidive.

- la stratégie s'appuie sur **un fort soutien de la population**, ouverte au numérique et au sein de laquelle **l'idée d'un certificat d'immunité en échange de libertés retrouvées plus vite ne fait pas polémique.**

Après Gibraltar, le Danemark est d'ailleurs **le deuxième pays au monde où le plus de tests ont été effectués en proportion de la population** : 575 000 tests (10 % de la population) pour la seule journée du 21 avril, dans 584 centres de dépistage. Ce chiffre est aujourd'hui proche de 700 000 tests journaliers, dont un tiers de PCR, mais est appelé à baisser au fur et à mesure de la campagne de vaccination – laquelle, du reste, affiche un certain retard.

Les opposants aux restrictions sont très minoritaires, en dépit des manifestations parfois violentes des « *Men in Black* », proches du parti d'extrême droite Nye Borgelige.

Avec 2 517 morts au 31 mai, le Danemark compte **434 décès par million d'habitants, soit l'un des taux les plus bas d'Europe**.

Le pass sanitaire a parfois été mis en place **au niveau local**. Aux États-Unis, **l'État de New York** est le seul à l'avoir lancé : l'*Excelsior Pass*, développé par IBM affiche un code couleur (rouge ou vert) et permet d'accéder aux restaurants, mariages ou encore enceintes sportives. À vrai dire, l'initiative locale de New York s'explique d'abord par **le blocage rencontré au niveau fédéral** : face à l'opposition républicaine, et alors que plusieurs États (Texas, Floride, Missouri, Arkansas, etc.) ont tout simplement interdit aux commerçants d'exiger de leur clients une preuve de vaccination, l'Administration fédérale a renoncé. Sans pour autant avoir mis en place un pass sanitaire, la Californie encourage en revanche les organisateurs d'événements à se doter de leurs propres dispositifs de contrôle.

En France, le pass sanitaire, dont la mise en place a été confirmée le 29 avril, constitue l'un des piliers du déconfinement progressif. Comme pour d'autres dispositifs, le Gouvernement y était pourtant opposé quelques semaines auparavant. Il devrait être disponible à partir de juin.

IV. FACE AUX PROCHAINES PANDÉMIES, DES PERSPECTIVES IMMENSES ET DES QUESTIONS VERTIGINEUSES

Si le recours aux outils numériques s'est fait de façon très inégale en fonction des pays, toutes les stratégies ont un point commun : par choix politiques ou par impossibilité matérielle, **elles n'exploitent en réalité qu'une très faible part des possibilités théoriques des technologies actuelles, sans même parler des possibilités des technologies à venir**. À cet égard, la pandémie de Covid-19 présente une double particularité : c'est à la fois la première fois que le numérique est autant mobilisé, et sans doute la dernière fois où il le sera aussi peu.

On peut en prendre la mesure à travers **l'exemple des géants du numérique, et notamment des GAFA**, qui joué un rôle important dans cette crise, mais largement en deçà de leurs capacités technologiques réelles (**A**).

À plus long terme, les technologies numériques ouvrent des **perspectives immenses** pour mieux gérer les pandémies (**B**), mais celles-ci soulèvent en même temps des risques considérables pour les libertés individuelles (**C**), dont il faut dès à présent se préoccuper.

A. LES GAFA FACE AU COVID-19

Par la quantité et la diversité des données qu'ils collectent sur chacun d'entre nous, par leur maîtrise des technologies les plus avancées, et plus généralement par leur importance désormais systémique dans la vie économique et sociale, **les géants du numérique se sont trouvés en position de jouer un rôle majeur dans la gestion de l'épidémie, parfois à l'égal des États**, si ce n'est en position de force par rapport à eux.

Leur rôle dans le développement des technologies de *contact tracing* sera spécifiquement abordé dans la deuxième partie du présent rapport, à l'occasion des développements sur l'application française *TousAntiCovid*.

Ce sont aussi leurs services qui ont, d'abord, permis **d'assurer la continuité de la vie économique et sociale**, qu'il s'agisse de communiquer, de travailler, d'enseigner ou encore de faire ses courses à distance. Leur chiffre d'affaire a d'ailleurs augmenté de 19,5 % en 2020, et leur bénéfice opérationnel de 24,7 %, tandis que le reste de l'économie mondiale connaissait une crise sans précédent[1].

Plus généralement, leur rôle s'est étendu, dans des proportions variables, dans **tous les aspects de la réponse à la crise** – de la recherche scientifique pure au soutien direct aux campagnes de tests et de vaccination,

[1] *Le cas d'Amazon est éloquent : en un an, ses revenus ont augmenté de 37 % (96 milliards de dollars) et ses bénéfices ont triplé (6 milliards de dollars), portés par le e-commerce, le* streaming *(*Amazon Prime Video*) et le* cloud *(*AWS*). L'entreprise a même embauché 375 000 personnes supplémentaires, pour un effectif total de 1,1 million de personnes.*

en passant par l'information et la lutte contre la désinformation sur les réseaux sociaux. À titre d'exemple, les développements qui suivent retiennent quelques initiatives de **Google** et **Facebook**.

Mais ces remarques s'étendent au-delà du seul cas des GAFA (Google, Apple, Facebook, Amazon), même si leur importance systémique leur confère de fait un rôle particulier. Il en va de même, et peut-être plus encore, pour les BATX (Baidu, Alibaba, Tencent, Xiami et autres) en Chine (cf. *supra*). On pourrait encore mentionner, par exemple, **le contrat passé entre le *National Health Service* (NHS) britannique et la société Palantir pour exploiter grâce à l'intelligence artificielle les données relatives à la crise du Covid-19**, avec toutes les questions que cela soulève en matière de souveraineté et de protection données personnelles.

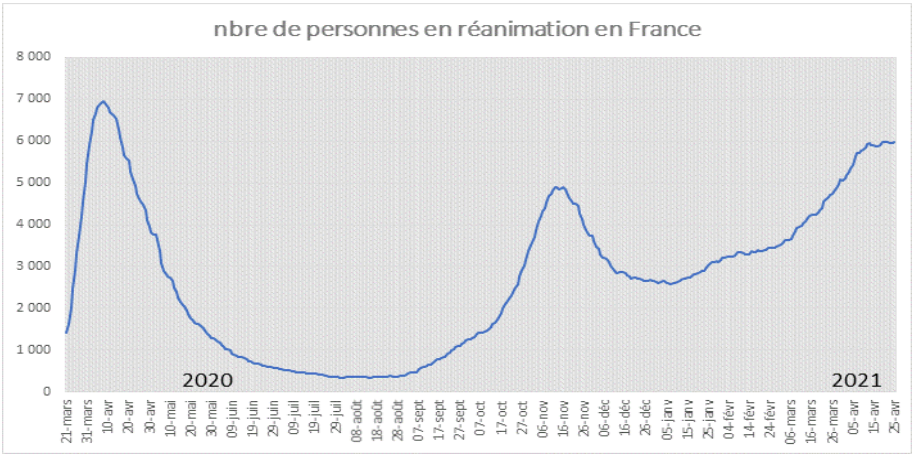
1. L'exemple de Google

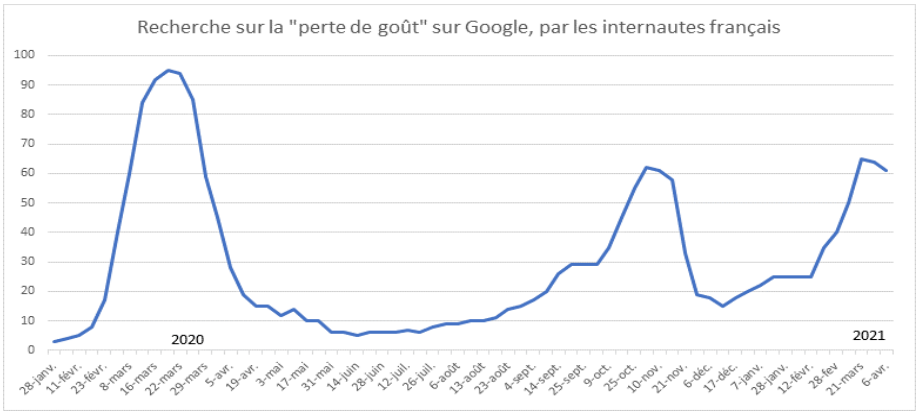
Les termes tapés dans le moteur de recherche de Google, associés à leur localisation géographique *via* l'adresse IP, constituent un indicateur assez précis de l'évolution de l'épidémie, et sont susceptibles de **pallier les insuffisances des systèmes publics de surveillance épidémiologique**, du reste bien plus problématiques aux États-Unis qu'en France.

Sous certaines conditions, **ces résultats peuvent même avoir une valeur prédictive et servir à la modélisation épidémiologique**. Lancé dès 2008 et accessible à tous, l'outil *Google Flu Trends*, visait ainsi à anticiper les pics grippaux grâce aux recherches des internautes sur les symptômes (fièvre, toux, etc.). Sa précision insuffisante, notamment lors de l'épidémie de H1N1 l'année suivante, avait finalement conduit Google à limiter son utilisation aux seuls chercheurs, tout en poursuivant son amélioration.

Il suffit, plus généralement, d'utiliser l'outil ***Google Trends*** pour obtenir des résultats intéressants sur la pandémie de Covid-19. En France, on trouve par exemple **une corrélation forte entre les recherches portant sur la perte de goût et le nombre de personnes en réanimation, avec un décalage constant de 20 jours**, faisant de recherches *Google* un indicateur avancé de la charge des hôpitaux.

Corrélation entre recherches Google sur la perte de goût et nombre de personnes en réanimation en France

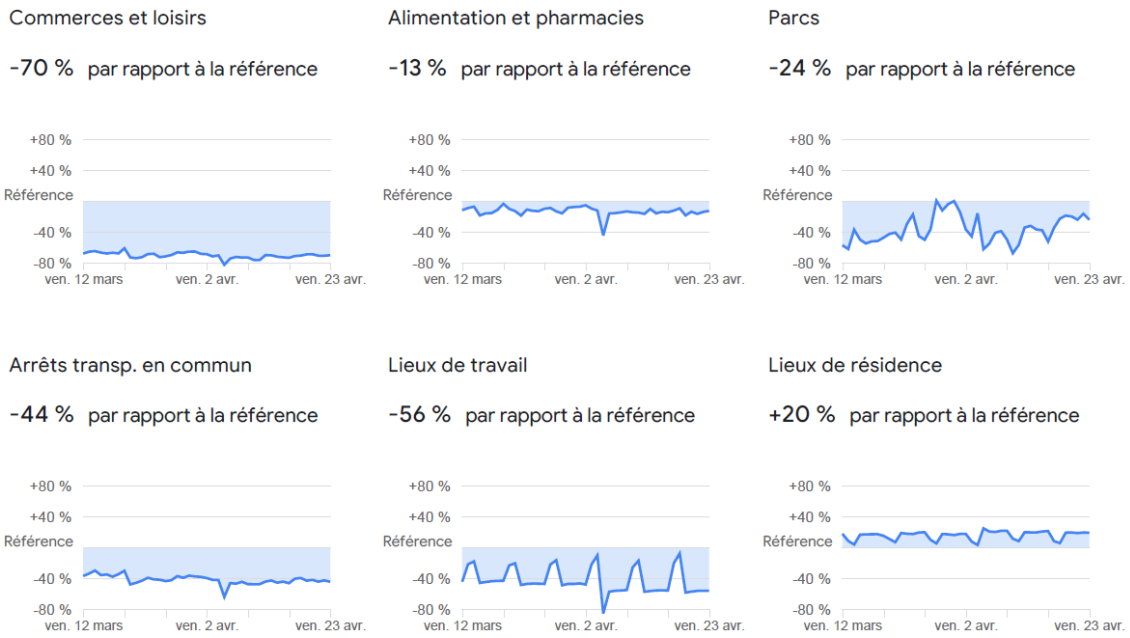




Source : projet « Algorithmes contre le Coronavirus », http://meteosensible.free.fr/coronavirus.html

Google publie également les données relatives à la fréquentation de certains lieux (commerces, parcs et jardins, transports en commun, etc.), à partir des données agrégées issues de produits tels que *Google Maps* ou de la géolocalisation des *smartphones* sous *Android*. Pour la France, ces données sont disponibles **au niveau départemental sur les dix derniers jours**. Ils font sans surprise apparaître une baisse de la fréquentation des commerces hors alimentation, mais aussi un passage au télétravail insuffisant au regard des recommandations gouvernementales.

Impact du Covid-19 sur les tendances de mobilité à Paris du 12 au 23 mars 2021



Source : Google Trends, *https://www.google.com/covid19/mobility/*

2. L'exemple de Facebook

À l'instar de Google, Facebook a joué un rôle dans une multitude de domaines au cours de la crise sanitaire, dont on ne citera ici que quelques exemples.

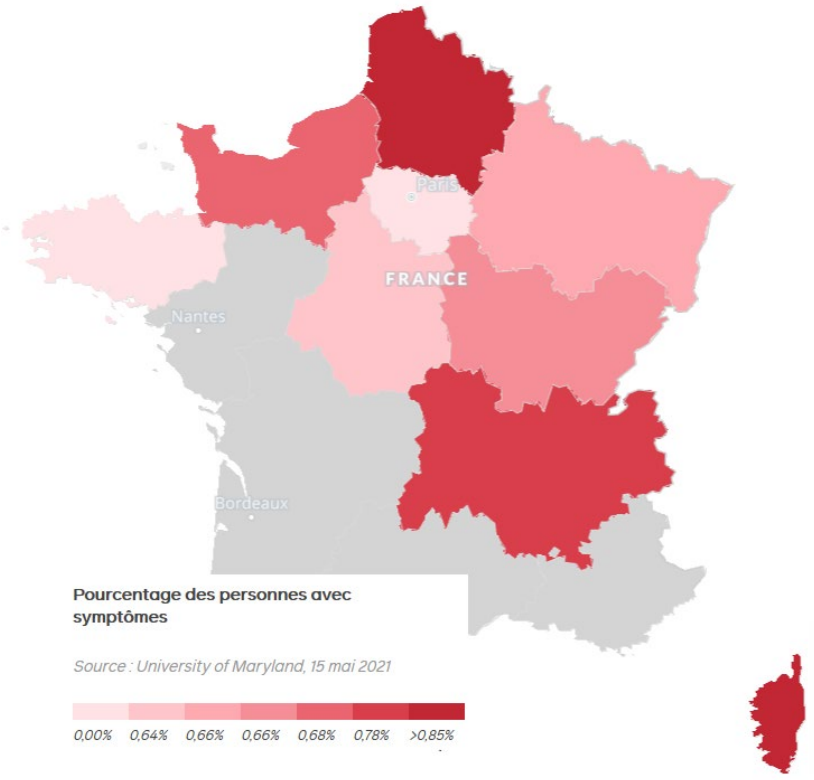
Certains sont aujourd'hui **des « attendus » d'un réseau social** : à travers son **Centre d'information sur le coronavirus**[1], Facebook met à la disposition de ses utilisateurs une série d'informations, statistiques, liens officiels et autres contacts utiles sur la pandémie. De façon plus proactive, le réseau social a créé dans certains pays **des « badges » et « filtres » affichés sur le profil des utilisateurs qui se sont fait vacciner**, afin d'encourager leurs « amis » à le faire, grâce à une visibilité accrue dans leur « fil d'actualité ». **Diverses campagnes de lutte contre la désinformation**, dont le réseau social est désormais familier, ont également été menées au sujet de l'épidémie, et plus particulièrement de la vaccination.

Une fonctionnalité, en particulier, est particulièrement intéressante pour le sujet du présent rapport : **le *Safety Check*, qui permet depuis 2014 aux utilisateurs de se signaler comme « en sécurité »** lorsqu'ils se trouvent sur le lieu d'une catastrophe naturelle ou d'origine humaine, d'un attentat terroriste ou d'une menace sanitaire.

[1] *https://www.facebook.com/coronavirus_info et plus généralement https://about.fb.com/?s=covid*

S'agissant ensuite de la connaissance du virus et de son mode de propagation, Facebook dispose d'un atout de taille : ses **deux milliards d'utilisateurs**. Dans le cadre du programme ***Data For Good***, lancé en 2017, le réseau social met ces données à disposition des universités et ONG. Dans le cadre de la crise sanitaire actuelle, les utilisateurs de *Facebook* peuvent ainsi être invités, *via* leur fil d'actualité, à participer à **un sondage optionnel**, conçu par les chercheurs du Delphi Research Center de la Carnegie Mellon University, **dans lequel ils décrivent notamment leurs symptômes et leurs facteurs de risque**. Les résultats s'avèrent globalement corrélés avec des données de dépistage officielles – et peuvent dans certains cas avoir une valeur prédictive. La carte ci-dessous, élaborée à partir des seules données de *Facebook*, montre les symptômes du Covid-19 en France, à l'échelle régionale.

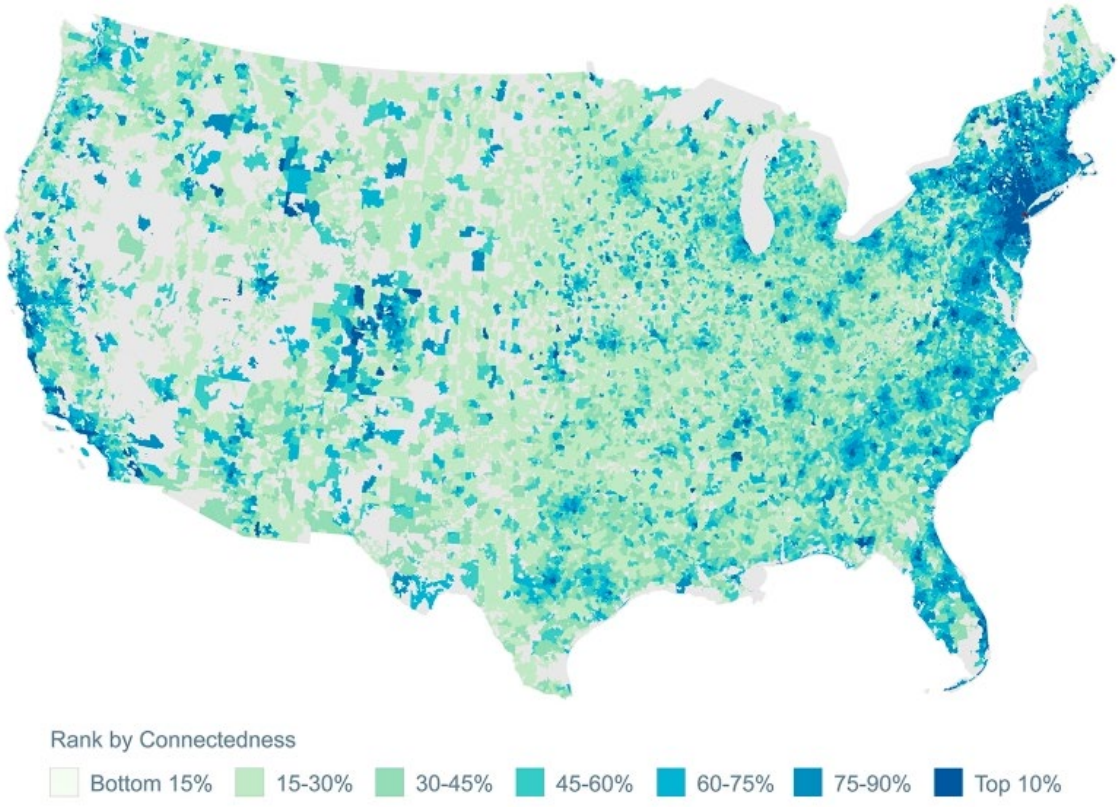
Symptômes du Covid-19 en France
(par région, pour la semaine du 20 mai 2021)



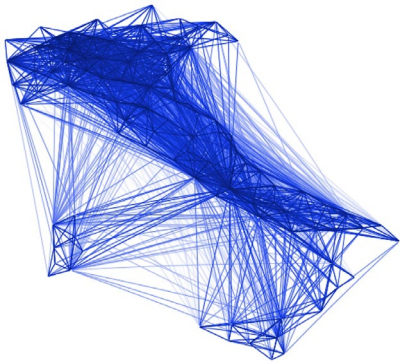
Source : Facebook, projet Data For Good *: https://dataforgood.facebook.com/covid-survey*

Naturellement, les données de Facebook dépassent largement les seules données médicales fournies volontairement à l'occasion d'un sondage. Par exemple, la carte ci-dessous fait apparaître **les « liens d'amitié » qui connectent les habitants d'East Village, à New York, avec les autres régions des États-Unis**, à l'échelle du *ZIP code* (code postal). Un tel outil peut être utilisé par les épidémiologistes pour prédire les risques d'apparition ou d'aggravation de l'épidémie en fonction des lieux.

Degré de « connexion sociale » (*social connectedness*)
***via Facebook* avec East Village (New York) en mars 2020**



Source : Facebook, projet Data For Good *: https://about.fb.com/news/2020/04/data-for-good/*



Source : Facebook, projet Data For Good

Les contacts entre des personnes situées dans différents lieux peuvent également contribuer à affiner les modèles.

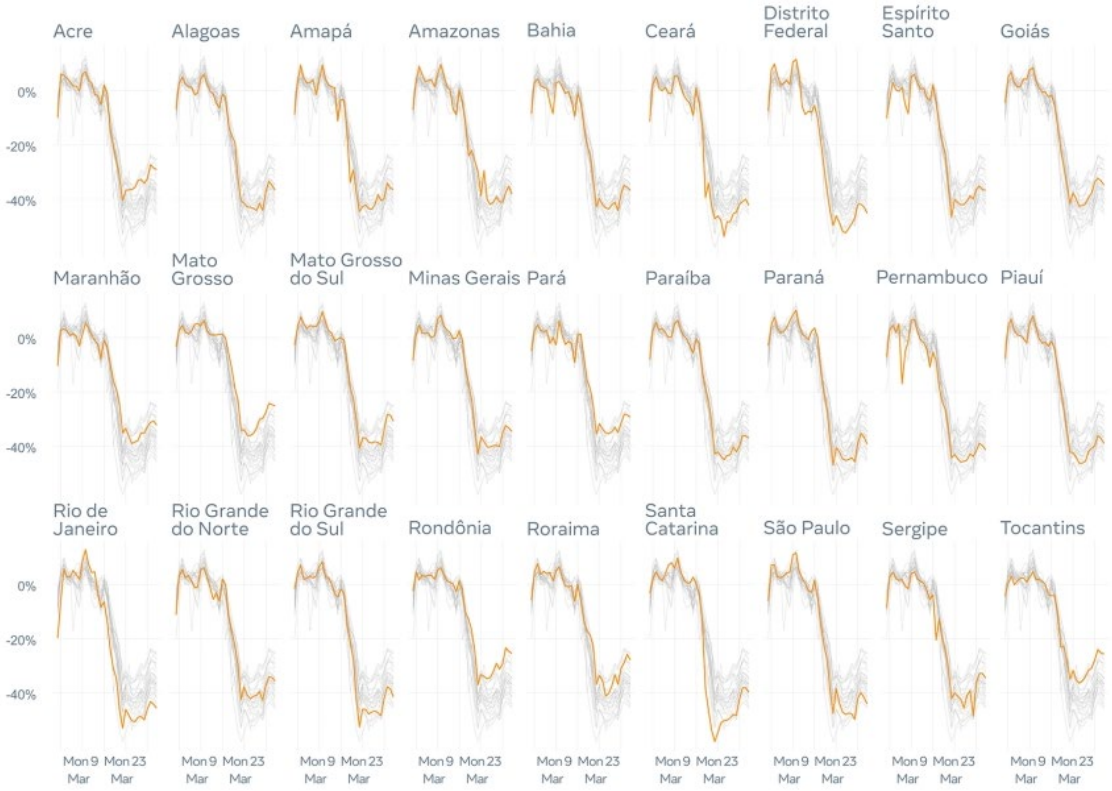
La carte ci-contre (*co-location map*) est un exemple de visualisation de ces liens à l'échelle d'un pays entier, en l'occurrence l'Italie. En pratique, les études s'appuient naturellement sur des données plus fines que celles qui permettent de réaliser une carte à l'échelle nationale.

Des **données de mobilité** sont également disponibles *via Facebook*. Les graphiques ci-dessous font ainsi apparaître, pour chaque État brésilien, l'évolution des déplacements de la population, mesurée par **le nombre d'endroits différents visités chaque jour**[1]. Ces données peuvent constituer

[1] *Concrètement, la carte est divisée en parcelles carrées de dimension égale* (tiles)*. Le nombre d'endroits visités correspond au nombre de* tiles *dans lesquelles l'utilisateur se rend.*

un bon indicateur du respect des mesures de confinement ou de couvre-feu (les habitants restent-ils chez eux ou se rendent-ils au contraire dans de nombreux endroits différents chaque jour ?).

Tendances de mobilité (*movement range trends*)
au Brésil, à l'échelle régionale



Source : Facebook, projet Data For Good *: https://about.fb.com/news/2020/04/data-for-good/*

3. Un rôle très en deçà des possibilités réelles et à venir

Il faut bien comprendre que les données publiées à ce jour, même si elles dépassent déjà très largement la capacité de production de n'importe quelle autorité étatique, sont **très en deçà des données dont disposent réellement les GAFA, en termes de volume comme de niveau de précision**.

Reprenons l'exemple de la carte des « liens d'amitié » sur *Facebook* entre les habitants d'East Village et le reste des États-Unis. D'une part, même dans le strict cadre de la modélisation épidémiologique, **de telles données sont aujourd'hui sous-exploitées** : aucun modèle actuel n'est suffisamment abouti pour en faire une exploitation systématique et en temps réel et pour les croiser avec d'autres données pertinentes (par exemple les données de mobilité), afin qu'elles puissent éclairer et appuyer la décision publique (confinements locaux, etc.). Pourtant, la possibilité existe, les algorithmes se perfectionnent, et les capacités de calcul augmentent : à terme, cette perspective n'a rien d'irréaliste techniquement.

D'autre part, et surtout, les données sont ici mises à disposition des chercheurs uniquement sous forme agrégée, ce qui est suffisant pour la modélisation, mais Facebook dispose en réalité de l'ensemble de ces données – et bien davantage encore – à une échelle individuelle, en temps réel, dans le monde entier et avec une précision de l'ordre du mètre[1] plutôt que du code postal. Il en va de même pour les données de fréquentation des lieux et des transports collectées par Google, etc.

En recoupant ces données avec d'autres, que détiennent les mêmes entreprises, il serait donc possible de déterminer si un individu se rend au travail ou plutôt chez des amis ou de la famille, s'il exerce une profession « essentielle » lui permettant de sortir de chez lui ou non, s'il a récemment eu des conversations privées au sujet de l'organisation d'une soirée rassemblant plus de dix personnes, ou s'il a effectué des achats en vue d'une telle soirée.

B. DEMAIN, UNE GESTION DES CRISES PAR LE NUMÉRIQUE ?

1. Crises sanitaires, catastrophes naturelles, accidents industriels

On le voit : les perspectives ouvertes par le recours aux technologies numériques sont immenses, et **la crise du Covid-19 n'a donné qu'un avant-goût des multiples cas d'usage possibles**, à court, moyen ou long terme.

Alors que la pandémie de Covid-19 n'est pas terminée, et qu'il est probable que celle-ci ne soit ni la dernière, ni la plus forte, **il serait irresponsable de ne pas se saisir de telles possibilités**. Les restrictions généralisées imposées aux libertés « physiques » ces derniers mois sont de moins en moins supportables. Elles ne sont ni durables, ni même très efficaces, en comparaison de ce que permettrait un usage plus systématique du numérique.

Le recours au numérique permettrait de contrôler précisément le respect des mesures sanitaires, à un niveau individuel et en temps réel : en contrepartie, les restrictions pourraient être ciblées sur un faible nombre de personnes, et être plus limitées dans le temps, tout en ayant une efficacité maximale. **Peut-être pourrons-nous demain, grâce au numérique, retrouver nos libertés « physiques » plus vite, ou même ne jamais les abandonner, et avoir des pandémies sans confinement** - et ceci même si aucun vaccin ou traitement n'est disponible.

---

[1] *Dans le détail, tout dépend du mode de connexion (fixe, GPS, W*ifi, Bluetooth*) et de l'autorisation donnée par l'utilisateur (géolocalisation activée ou non), étant précisé que cette dernière est souvent favorisée, puisqu'indispensable au modèle économique du réseau social.*

Les outils envisageables sont multiples mais, à court et moyen terme du moins, les cas d'usage les plus évidents concernent **le contrôle du respect des règles visant à limiter la transmission du virus** (pass sanitaire, couvre-feu, confinements, quarantaines, etc.), **qui implique de croiser trois types de données : données d'*identification*, données *médicales*, et données de *localisation*** (des plus intrusives, avec le *tracking* GPS, aux plus légères et occasionnelles, avec l'accès conditionnel à certains lieux, en passant par les données de localisation relative avec le *contact tracing*).

L'utilité des outils numériques dans la gestion de crise **dépasse le seul domaine sanitaire**, et s'étend également à d'autres types de crises, liées en particulier aux **risques dits « NRBC », pour nucléaires, radiologiques, biologiques et chimiques**, qui ont en commun de présenter un danger élevé et imminent pour la population, appelant à une réaction rapide et efficace. Ceux-ci peuvent résulter d'une **attaque volontaire** (conventionnelle ou terroriste, en particulier bioterroriste), mais aussi d'un **accident industriel** ou d'une **catastrophe naturelle** (y compris sans dimension NRBC : tsunami, tremblement de terre, inondation, etc.). **Le *Safety Check* de Facebook**, par exemple, est utilisé dans l'ensemble de ces cas. Toutes ces situations peuvent nécessiter d'identifier rapidement des personnes, d'évaluer leur état de santé ou les risques qu'ils encourent, et de les localiser précisément pour leur porter assistance.

Les développements ci-dessous exposent donc quelques cas d'usage potentiels, au travers d'une **typologie fondée sur les finalités des mesures, qui peuvent être très différentes pour une même technologie sous-jacente.** Cette liste est nécessairement incomplète, incertaine, et discutable : il s'agit d'un exercice de prospective.

2. Essai de typologie prospective

a) L'information et l'incitation

Dans le cadre d'une gestion de crise, **l'information** – sur les risques encourus, sur les règles applicables, etc. – est aussi une **incitation**.

La plupart des mesures mises en œuvre en France, et dans les pays occidentaux en général, lors de la crise du Covid-19 relèvent en réalité de cette catégorie, puisqu'elles sont **non contraignantes** et qu'elles ne donnaient généralement lieu à **aucune transmission de donnée nominative** à un tiers. C'est le cas de l'application ***TousAntiCovid***, dans sa fonctionnalité initiale de *contact tracing* (envoi d'une notification en cas de contact avec une personne infectée), mais aussi dans ses fonctionnalités annexes : statistiques sur l'évolution de l'épidémie, information sur les gestes barrières et les démarches à suivre, etc. Les outils permettant de faciliter la prise de rendez-vous pour les tests de dépistage ou la vaccination (***Doctolib***, *ViteMaDose*, etc.) s'y rattachent également.

Au-delà du domaine sanitaire, outre le ***Safety Check*** de Facebook déjà cité, on peut citer le dispositif ***Amber Alert***, l'équivalent américain de l'*Alerte Enlèvement*, qui existe depuis 2002 et permet un ciblage précis des personnes situées dans une certaine zone (cf. *infra*).

On pourrait imaginer, pour l'avenir, bien d'autres cas d'usage. Par exemple, en France, des campagnes régulières de **distribution de pastilles d'iode** ont lieu depuis 1997 auprès des personnes qui résident à proximité d'une centrale nucléaire (dans un rayon de 10 km), afin de protéger leur thyroïde **en cas d'accident nucléaire**. Ces pastilles sont mises à disposition dans un réseau de pharmacies partenaires, mais la démarche est purement volontaire et, en 2016, **seuls 42 % des foyers avaient retiré leurs pastilles**, et seulement 27 % des établissements recevant du public. Grâce au numérique, il serait possible d'organiser des **campagnes de rappel sur les *smartphones***, et surtout, en cas de d'accident nucléaire, il serait possible de localiser **sans délai toutes les personnes se trouvant dans la zone, et de leur porter assistance**.

b) L'assistance

Les données permettant d'informer les individus pourraient, si les circonstances l'exigent, informer en même temps les professionnels de santé ou les autorités chargées de la gestion de crise, afin de **porter assistance aux personnes vulnérables dans les meilleurs délais**.

Par exemple, dans le cas d'une épidémie qui se répand rapidement ou dont la mortalité est très élevée, des équipes médiales pourraient ainsi **se rendre immédiatement au domicile des personnes vulnérables (où dans tout lieu où elles se trouvent)**, pour les vacciner, les soigner ou encore les mettre en sécurité. Il ne s'agit pas ici d'intervenir auprès de « *tous les plus de 65 ans* » ou « *tous les habitants de telle commune* » : les croisements de données et le recours à l'intelligence artificielle **rendent en effet possible un ciblage extrêmement fin**. Par exemple :

- en exploitant des **données génétiques**, il pourrait être possible d'identifier immédiatement les personnes réceptives à un variant très rare d'un virus, ou à un vaccin ou traitement particulier, et de mobiliser ainsi les ressources médicales de façon beaucoup plus efficiente. Sans aller jusque-là, la simple **exploitation automatisée du dossier médical** de chaque individu d'une population cible pourrait déjà permettre de faire beaucoup ;

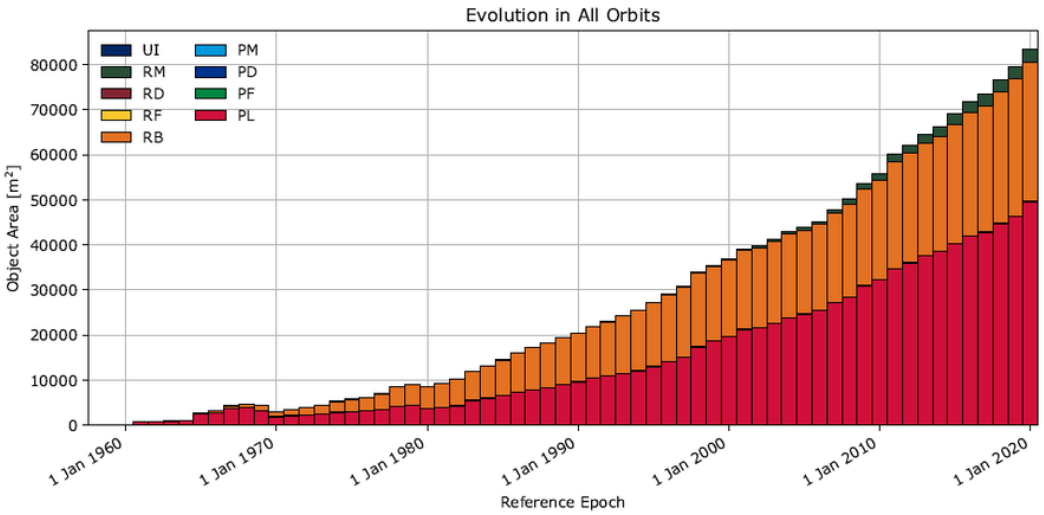
- en exploitant les **données des objets connectés**, qui pourraient elles aussi être accessibles depuis l'espace numérique de santé, il pourrait être possible d'intervenir en amont de l'apparition ou de la dégradation des symptômes : données d'ECG, de balances connectées, de thermomètres connectés, de caméras thermiques détectant les symptômes fiévreux, etc. ;

- en exploitant des **données de mobilité**, il pourrait être possible de positionner les équipes (d'information, de test, de vaccination, etc.) **aux bons endroits et aux bons moments** pour intervenir auprès d'un maximum de personnes (un *hub* de transport, un rassemblement public, etc.), celles-ci ayant le cas échéant été prévenues en avance.

Là encore, ces cas d'usage ne se limitent pas aux crises sanitaires : en cas de **catastrophe industrielle**, par exemple, les personnes particulièrement vulnérables à **certains produits chimiques** pourraient bénéficier d'une évacuation prioritaire ou de soins particuliers, quel que soit l'endroit où ils se trouvent.

Un autre exemple est **la chute de débris spatiaux** : le phénomène, aujourd'hui rare, pourrait devenir bien plus important à l'avenir, avec la hausse le vieillissement du parc de satellites, et surtout le développement de « constellations » de petits satellites. Par exemple, **le projet *Starlink***, porté par la société SpaceX, prévoit **la mise en orbite basse de 12 000 satellites** à horizon 2025, un chiffre à comparer avec les 2 000 satellites en activité aujourd'hui. Quelque **30 000 objets de plus de 10 cm** sont actuellement en orbite, pour l'essentiel des déchets spatiaux, souvent petits mais hors de contrôle et susceptibles de s'écraser sur Terre ou d'entrer en collision avec d'autres satellites, générant davantage de déchets encore.

Le risque de collision des objets spatiaux



(c) Evolution of area.

Les objets que nous envoyons en orbite occupent de la place, tout comme les débris qu'ils créent. Plus la surface occupée par les objets dans l'espace augmente, et plus la probabilité de collision augmente. Rouge (PL) = satellites ; Orange (RB) = lanceurs ; Vert foncé (RM) = objet lié à un lanceur.

Source : Agence spatiale européenne (ESA)

Certains mesurent près d'une tonne, à l'instar des satellites GOCE (5 mètres de long), qui s'est écrasé sur Terre en 2013 ou des **lanceurs de la station spatiale chinoise *Tiangong* (*Longue Marche*) :** l'un s'est écrasé en 2018 après que les autorités chinoises en eussent perdu le contrôle, un autre en 2020 près d'un village de Côte d'Ivoire, heureusement sans faire de dégâts, et encore un autre, un segment de 18 tonnes, a fini sa course le 9 mai dernier dans l'océan Indien[1].

Or, si les moyens actuels permettent d'estimer assez précisément le point de chute des débris, comme l'indique l'Agence spatiale européenne (ESA), qui publie un rapport annuel à ce sujet[2], **celui-ci n'est connu qu'au dernier moment**, une fois que l'objet initial s'est désintégré dans l'atmosphère. Dans ces circonstances, la capacité à prévenir immédiatement la population est cruciale, et **seul le numérique permet de le faire**.

c) La contrainte et le contrôle

Même s'ils sont rarement présentés comme tels, des dispositifs tels que le **pass sanitaire** ou le **passeport sanitaire** relèvent bien de la catégorie des **outils contraignants**, car ils conditionnent, *de facto* ou *de jure* selon les cas, l'accès à certains lieux et à certaines activités. En soi, cela n'a rien d'exceptionnel : le « vrai » passeport, le carnet international de vaccination ou le permis de conduire font la même chose, c'est-à-dire autoriser ou interdire, soit l'une des fonctions principales de la puissance publique.

Mais la contrainte change de nature dès lors qu'elle s'exerce par un **contrôle**, le cas échéant assorti de **sanctions**. Et c'est précisément là que le numérique pourrait être le plus « efficace ».

Précisons qu'il existe des formes de contrôle ou de contrainte **plus implicites, mais non moins efficaces** : un **portique d'entrée** dans le métro qui se mettrait à sonner très fort au passage d'une personne contagieuse ou censée être confinée serait dans la plupart des cas suffisamment dissuasif pour qu'il ne soit même pas nécessaire de transmettre cette information aux autorités chargées de contrôler le respect des règles. Début 2021, la presse a rapporté le cas d'un **boîtier connecté, porté autour du cou**, qui sonnerait (avec un son de 85 décibels) en cas de non-respect des règles de distanciation par les salariés d'une entreprise[3]. L'initiative a été dénoncée comme anxiogène et inacceptable. Techniquement, toutefois, nul besoin d'un boitier autour du cou : un *smartphone* peut faire la même chose avec son *Bluetooth*, et un son de 100 décibels. **En Asie, le contrôle social a pris des formes beaucoup moins anecdotiques** : en Corée du Sud, les habitants positifs d'un quartier pouvaient être géolocalisés sur une carte accessible à tous, et en

[1] https://www.courrierinternational.com/article/debris-le-premier-etage-de-la-fusee-chinoise-longue-marche-finit-sa-course-dans-locean

[2] https://www.esa.int/Space_in_Member_States/France/Point_de_situation_sur_les_debris_spatiaux

[3] *Voir par exemple :* https://www.capital.fr/entreprises-marches/covid-19-des-salaries-munis-dun-boitier-qui-sonne-en-cas-de-rapprochement-trop-marque-1390710

Chine, on a vu d'honnêtes citoyens prendre eux-mêmes en charge la « police sanitaire » de leur immeuble. Plus généralement, le **système du crédit social** (cf. *supra*), s'il n'implique que rarement des sanctions effectives, se rattache à cette logique de contrôle social.

Enfin, dans les situations de crise les plus extrêmes, les outils numériques pourraient permettre d'exercer un contrôle effectif, exhaustif et en temps réel du respect des restrictions par la population, assorti le cas échéant de sanctions dissuasives, et fondé sur une exploitation des données personnelles encore plus dérogatoire.

Ces outils sont les plus efficaces, mais aussi les plus attentatoires aux libertés – mais une fois de plus, il serait irresponsable de ne pas au moins les envisager, ne serait-ce que pour se convaincre de tout faire en amont pour ne pas en arriver là. De nombreux cas d'usages sont possibles, et notamment :

- le contrôle des déplacements : bracelet électronique pour contrôler le respect de la quarantaine, désactivation du pass pour les transports en commun, détection automatique de la plaque d'immatriculation par les radars, portiques de contrôle dans les magasins, caméras thermiques dans les restaurants, etc. ;

- le contrôle de l'état de santé, *via* des objets connectés dont l'utilisation serait cette fois-ci obligatoire, et dont les données seraient exploitées à des fins de contrôle ;

- le contrôle des fréquentations, par exemple aller voir un membre vulnérable de sa famille alors que l'on est contagieux ;

- le contrôle des transactions, permettant par exemple d'imposer une **amende automatique**, de détecter **un achat à caractère médical** (pouvant suggérer soit une contamination, soit un acte de contrebande en période de pénurie), ou encore **la poursuite illégale d'une activité professionnelle** (commerce, etc.) en dépit des restrictions.

d) L'assurance

Situé entre la simple information et la contrainte directe, mais presque absent du débat public**, le modèle assurantiel** soulève pourtant des questions intéressantes.

Au niveau individuel, les restrictions sont souvent difficiles à vivre et **nécessairement binaires** (sortir ou ne pas sortir de chez soi), alors qu'elles correspondent à un risque individuel faible d'attraper ou de transmettre la maladie (du moins dans le cas du Covid-19). **Au niveau de la société**, en revanche, **ce risque se mesure de manière beaucoup plus fine** (le taux de mortalité, le taux d'occupation des lits de réanimation, etc.) et correspond à un **coût financier collectif** (par exemple l'investissement dans les structures de soin, la rémunération des heures supplémentaires ou encore l'achat des vaccins).

Plutôt que de restreindre drastiquement les libertés individuelles de toute la population ou d'une partie de celle-ci qui pourrait considérer cela comme inacceptable[1], **le numérique pourrait permettre d'internaliser une fraction du coût collectif correspondant au comportement de chaque individu ou de chaque groupe de personnes**.

Appliqué au confinement, le raisonnement serait le suivant : chaque sortie de mon domicile comporte un risque, non seulement pour moi-même mais aussi pour le système de santé dans son ensemble. Si je préfère malgré tout disposer de ma liberté d'aller et venir, et que je sors effectivement de chez moi, **il est légitime que j'assume en contrepartie une fraction du surcoût payé par la société du fait de l'épidémie**, par exemple sous la forme d'une **petite hausse de mes cotisations sociales** si le nombre ou la durée de mes sorties excède un certain seuil.

Ce surcoût serait en tout état de cause **très minime** : il s'agit bien ici d'une **logique assurantielle** (le surcoût est réparti entre toutes les personnes qui choisissent de se déplacer, cela n'étant nullement interdit), **et non d'une logique de sanction**, dont le principe est totalement différent (sortir de chez soi est interdit, la sanction est calculée pour être dissuasive, et est d'autant plus élevée que la chance de « se faire prendre » est faible).

Un tel modèle, bien sûr, **ne fonctionne qu'en cas d'épidémie de basse intensité**, où la surcharge imposée au système de soins est absorbable par l'engagement de moyens financiers supplémentaires. Elle n'est donc pas adaptée à des situations de crise aiguë, où des mesures plus fortes sont nécessaires, et correspond davantage aux situations où il est pertinent de « vivre avec » une maladie en circulation, moyennant quelques adaptations.

Dans le détail, le calibrage précis d'une telle solution dépend ensuite des **préférences de la société** et des **arbitrages politiques**. On pourrait ainsi imaginer, en reprenant l'exemple de l'alternative au confinement :

- un système « universel », ou « beveridgien », où chaque sortie compte de façon identique pour le calcul de la surprime, quels que soient les facteurs de risques individuels ou les motifs de la sortie ;

- un système « assurantiel » *stricto sensu*, ou « bismarckien », où ceux qui courent un risque plus important (les personnes âgées par exemple), et ont par conséquent une plus grande probabilité de peser sur le système de santé, paient un prix plus élevé pour chacune de leurs sorties ;

---

[1] *Par exemple, lors de la levée du premier confinement en France, le Président de la République avait initialement envisagé de maintenir les restrictions pour* ***les seules personnes âgées****, soit environ 15 millions de personnes de plus de 65 ans. Devant le tollé provoqué, la mesure avait été abandonnée, bien qu'elle fût défendue par de nombreux médecins et experts, et par le Conseil scientifique lui-même. On peut également penser aux restrictions qui touchent* de facto ***surtout les plus jeunes****, telles que l'interdiction des grands rassemblements (concerts, festivals, etc.), la fermeture prolongée des boîtes de nuit, ou encore, quoique dans une moindre mesure, la fermeture des bars et restaurants.*

- un système de « responsabilisation », où le surcoût dépend non pas du risque que l'on prend pour soi, mais du risque que l'on *fait prendre* aux autres, en fonction par exemple de son état de santé (vacciné/immunisé ou non), des motifs du déplacement (de l'activité professionnelle vitale à la sortie en boîte de nuit) ou encore de ses circonstances (en ville, à l'heure de pointe, etc.). Ce dernier modèle est plus « juste » mais aussi plus intrusif, car il nécessite d'exploiter davantage de données. Selon les critères retenus, il peut en outre impliquer d'apprécier la « légitimité » des motifs de sortie (comme les attestations papier, du reste), ainsi que leur caractère contraint ou choisi.

Au-delà de leurs différences, tous ces modèles ont en commun un principe de **solidarité** et de **mutualisation du risque**.

C. DES MENACES POUR LA LIBERTÉ INDIVIDUELLE

Les immenses perspectives qu'ouvrent les technologies numériques à moyen et long terme dans le cadre de la gestion des crises sanitaires soulèvent en même temps **de vertigineuses questions sur les moyens de garantir les libertés individuelles, à commencer par la vie privée**.

Les risques de dérives sont évidents, notamment parce que les technologies susceptibles d'être utilisées dans le cadre de la gestion d'une crise sanitaire pourraient être utilisées à d'autres fins – et beaucoup le sont déjà dans de multiples situations (reconnaissance faciale, drones, portiques, badges d'accès numériques, bracelets électroniques, géolocalisation, etc.).

1. Le pire n'est jamais impossible

Précisons-le d'emblée : raisonner en termes absolus n'a strictement aucun sens, et des atteintes considérées comme inacceptables face à une menace modérée ne le seront pas forcément face à une crise plus grave. À cet égard, **il est de notre responsabilité d'imaginer le pire, même si celui-ci n'est pas certain, et la délégation sénatoriale à la prospective est ici dans son rôle**.

Or rien ne garantit que la prochaine pandémie ne sera pas bien plus grave que celle du Covid-19, qui, rappelons-le, a un taux de létalité relativement faible, autour de 1 %. Et pourtant, elle a déjà causé près de huit millions de morts, forcé à confiner la moitié de l'humanité et causé une récession historique. Qu'en sera-t-il si, demain, nous étions frappés par une maladie plus virulente encore, ou qui touche en priorité nos forces vives et notre jeunesse, comme ce fut le cas avec **la grippe espagnole, avec ses 100 millions de morts (5 % de l'humanité) et son taux de létalité de 3 % ?** Si les progrès de l'hygiène et de la médecine rendent fort heureusement très

improbable une calamité comparable à la grande peste de 1347-1352[1], **nos sociétés modernes ont aussi leurs propres vulnérabilités –** à commencer par **la mondialisation**, qui favorise la transmission partout dans le monde à une vitesse inédite dans l'histoire, et **le risque de bioterrorisme**, c'est-à-dire la possibilité d'un agent pathogène *volontairement* conçu pour faire le plus de mal possible, le plus rapidement possible[2]. **Que se passerait-il si, face à une maladie émergente à diffusion très rapide, nous ne disposions d'aucun traitement ni vaccin ?**

2. Réfléchir avant pour ne pas subir ensuite

Plus la menace sera grande, plus les sociétés seront prêtes à accepter des technologies intrusives, et des restrictions plus fortes à leurs libertés individuelles – et c'est logique.

Dès lors, comment garantir que données collectées à l'occasion d'une crise sanitaire ne seront ni conservées au-delà du strict nécessaire, ni exploitées ensuite à d'autres fins, notamment politiques ? Comment assurer que les traitements mis en œuvre n'aboutissent à **aucune discrimination**, notamment en raison de l'âge, du sexe ou de l'origine ethnique ?

Ces questions sont déjà pressantes aujourd'hui, et pourraient l'être davantage encore demain, posant de véritables dilemmes moraux. Ainsi, que faire si une discrimination liée à l'origine ethnique s'avérait *objectivement* pertinente, par exemple pour une maladie contagieuse grave ne touchant ou n'épargnant que les seuls porteurs d'un gène spécifique, comme c'est le cas de plusieurs maladies infectieuses ? Que faire si le « droit à l'oubli » très protégé en Europe allait *objectivement* à l'encontre de la santé publique, par exemple dans le cas d'une période d'incubation de plusieurs années, ou d'un virus dont les porteurs sains demeurent très contagieux, ou encore d'une maladie ancienne qui, même guérie, constitue un facteur de risque – ou de protection – particulier pour une nouvelle ? Que faire si, dans une situation où les autorités seraient déjà débordées, le contrôle social par le voisinage ou l'employeur était la seule alternative ?

---

[1] *La peste noire, ou « grande peste », est une pandémie qui frappé le monde au milieu du XIV^e^ siècle.* ***En Europe, elle a tué entre 30 % et 50 % de la population en seulement six ans*** *(1347-1352), soit près de 25 millions de personnes, avant de reculer puis de revenir par vagues sporadiques, par exemple à Marseille en 1720.Ses conséquences ont été terribles pour l'ensemble des sociétés touchées. Elle a durablement affaibli les pays européens, mais aussi provoqué indirectement la chute de la dynastie Yuan en Chine (1271-1368, dynastie mongole) et contribué à affaiblir encore davantage l'Empire byzantin (qui tombe finalement face aux Ottomans en 1453).La peste noire, causée par la bactérie* Yersinia Pestis*, était principalement une peste bubonique (60 % de létalité). La peste pulmonaire avait quant à elle un taux de létalité de 100 %.*

[2] *Alors qu'un virus qui, par mutation naturelle, se retrouverait particulièrement virulent serait plus vraisemblablement éliminé par la sélection naturelle : tuer tous ses hôtes potentiels n'est pas une bonne stratégie évolutive.*

Et encore ne s'agit-il ici que de technologies limitées à la détection d'un état de santé *avéré* ou au contrôle d'un comportement *effectif*. **Mais à plus long terme, il est probable qu'émergent des technologies *prédictives*, soulevant des questions bien plus difficiles encore**. Un employeur pourra-t-il refuser de recruter quelqu'un au motif que celui-ci pourrait, *un jour*, faire courir un risque sanitaire aux autres employés, non seulement en raison de ses prédispositions (une comorbidité, un gène spécifique, etc.) mais aussi du fait de sa personnalité ou de ses comportements (parce qu'il a un cercle social élargi, qu'il fréquente certains lieux, etc.) ? Une voiture autonome pourra-t-elle refuser de démarrer s'il existe une probabilité que le conducteur – le passager, donc – prenne ou fasse courir un risque sanitaire particulier ? Sa prime d'assurance augmentera-t-elle ? Devra-t-il souffler dans un spectromètre de masse comme on « souffle dans le ballon » ?

Des millions de personnes ont volontairement fourni leurs données génétiques à des sociétés comme *23&Me* ou *MyHeritage*, pour se découvrir une éventuelle ascendance ou de supposées prédispositions à telle ou telle maladie. En cas de crise grave, les autorités américaines pourraient-elles demander la communication de ces données – juridiquement, elles le peuvent déjà – et les opposer à un voyageur lors de son passage de la frontière ? Ou à leurs propres résidents ?

Il existe déjà des algorithmes permettant d'identifier un individu à la manière qu'il a de taper sur un clavier (vitesse de frappe, etc.) ; il s'agit notamment d'un indicateur de sa fébrilité, et donc – c'est l'une des fonctions de ces algorithmes – de sa propension à effectuer un achat compulsif sur Internet. Demain, la manière de remplir une attestation de sortie à une heure tardive comptera-t-elle autant que les réponses données ?

La prospective est un exercice délicat, surtout lorsqu'elle amène à des considérations dystopiques. Nul besoin d'aller jusque-là, ceci dit, pour se poser les bonnes questions : **la crise actuelle nous donne déjà toutes les raisons de veiller à la protection de nos droits et libertés**.

Mais elle nous donne aussi toutes les bonnes raisons de recourir davantage aux outils numériques, en conscience et en responsabilité – parce qu'ils sont potentiellement bien plus efficaces que les autres méthodes, parce qu'ils pourraient permettre de retrouver bien plus rapidement nos libertés « physiques », et **parce que si nous ne le faisons pas, d'autres le feront pour nous**. Et, face à une crise majeure, nous n'aurons pas d'autre choix que de leur demander leur aide, **et il sera alors trop tard pour défendre nos principes démocratiques**.

DEUXIÈME PARTIE :
LA FRANCE, ENTRE IMPRÉPARATION ET CONTRADICTIONS

Par contraste avec la stratégie des pays asiatiques et le volontarisme de certains de ses partenaires européens ou occidentaux, et plus encore au regard des possibilités que laissent entrevoir les technologies actuelles, **la France apparaît très en retrait dans son usage, par les pouvoirs publics, des outils numériques dans la gestion de la pandémie de Covid-19**.

Un tel décalage est extrêmement préoccupant, non seulement dans le cadre de la pandémie actuelle, qui a déjà fait plus de 100 000 morts[1] et causé la plus forte récession jamais connue en temps de paix[2], et qui dure encore, **mais aussi et surtout dans la perspective des épidémies à venir**. Si nul ne peut aujourd'hui prédire quand ni sous quelle forme celles-ci surviendront, **leur haute probabilité ne fait désormais plus guère de doute au sein de la communauté scientifique**.

Pourtant, dans leur rapport présenté devant la délégation à la prospective en 2015 et consacré à la prévention et à la gestion des crises liées aux maladies infectieuses émergentes[3], **Fabienne Keller et Roger Karoutchi appelaient déjà à s'appuyer davantage sur le numérique** – même si leurs propositions concernaient alors surtout la modélisation épidémiologique et, dans une moindre mesure, le traçage de la population[4], sans envisager les usages plus poussés qui existent aujourd'hui.

---

[1] *Au 30 mai 2021, d'après les chiffres de Santé Publique France (SPF), l'épidémie avait causé 109 402 décès (dont 83 145 à l'hôpital) pour près de 5,7 millions de cas confirmés.*

[2] *Soit un recul de -8,2 % du PIB en 2020, d'après les chiffres du programme de stabilité (PSTAB) présenté le 21 avril 2021. Le déficit public a atteint 9,2 % cette année-là, et la dette publique 115,7 % du PIB. L'explosion du chômage et des faillites n'a pu être évitée qu'au prix d'un « quoi qu'il en coûte » qui ne saurait être durable : entre 2020 et 2022, la crise sanitaire devrait coûter au minimum 424 milliards d'euros aux finances publiques, sous forme d'aides d'urgence (environ 8 milliards d'euros par mois), de mesures de relance et de moindres recettes fiscales.*

[3] *Rapport d'information n° 472 (2014-2015) de Roger Karoutchi et Fabienne Keller, fait au nom de la Délégation sénatoriale à la prospective, déposé le 28 mai 2015.*

[4] *Dans sa présentation devant la délégation, Fabienne Keller insistait ainsi «* sur le fait que l'utilisation des outils numériques doit absolument être développée et valorisée. Il n'est qu'à voir, pour s'en convaincre, l'apport de la télé-épidémiologie, qui permet, en s'appuyant sur les données d'observation de la Terre par satellite, de mettre en lumière les liens entre les facteurs environnementaux ou climatiques et l'émergence et la propagation des maladies infectieuses. Ou encore les progrès réalisés en matière de cartographie, notamment grâce aux réseaux sociaux et aux outils collaboratifs. Non seulement le numérique facilite le traçage des épidémies et la gestion des crises, mais il permet également de lutter contre les rumeurs et les fausses informations qui circulent dans ce genre de situation alors qu'on a besoin, au contraire, d'informations fiables et complètes. C'est également le bon moyen, le seul à mon sens, de toucher les jeunes, souvent réfractaires aux messages sanitaires de prévention ».

Avant de formuler des propositions, dans la troisième et dernière partie du présent rapport, il faut donc s'attacher à **comprendre les raisons** de ce retard, en distinguant dans cette seconde partie :

- d'une part, ***les raisons techniques et matérielles*** **(I), tenant à l'impréparation de nos systèmes d'information**, qu'une mobilisation dans l'urgence, quoique forte dans le domaine de la santé publique, ne pouvait qu'imparfaitement compenser ;

- d'autre part, ***les raisons politiques et idéologiques*** **(II), tenant à la profonde méfiance de la population à l'égard du numérique et au conservatisme juridique du régulateur** – au nom de « principes » qui apparaissent aujourd'hui coûteux et, en réalité, mal placés.

Enfin, des développements spécifiques seront consacrés à **l'échec de *TousAntiCovid* (III), cas d'école des contradictions de la France** qui, à vouloir à la fois défendre ses « valeurs » et préserver la santé de ses citoyens, n'a pu faire ni l'un ni l'autre avec cette application.

I. LA GRANDE IMPRÉPARATION NUMÉRIQUE

Si la France n'a pas *voulu* tirer parti des outils les plus puissants, mais aussi les plus intrusifs, elle n'a bien souvent pas *pu* tirer pleinement parti des autres non plus, **faute de disposer des moyens, des compétences et des systèmes d'information adaptés lorsque la crise est arrivée**.

On peut, parmi de nombreux exemples, reprendre les mots de David Gurson, fondateur du *think tank* Ethik-IA[1], « *il faut être très clair :* ***l'IA n'a joué jusqu'ici qu'un rôle très subsidiaire en France. La réponse à la crise a été et reste principalement humaine, dans des conditions parfois rudimentaires*** ». D'une manière générale, la crise a agi comme un révélateur du retard pris en la matière, qu'il convient à présent de rattraper.

A. DES OUTILS IMPROVISÉS ET LIMITÉS POUR GÉRER LA CRISE

1. Des fichiers *ad hoc* pour gérer l'état d'urgence sanitaire

a) SI-VIC, SI-DEP, Contact-COVID et VAC-SI

Surprise, comme la plupart des autres pays, par la brutalité de la crise sanitaire, **la France a dû s'adapter en urgence**, en réutilisant certains fichiers et en en créant d'autres à des fins spécifiques.

---

[1] *Institut Montaigne,* « L'intelligence artificielle contre le Covid-19 : améliorer la recherche et accélérer le diagnostic », *13 novembre 2020 :* *https://www.institutmontaigne.org/blog/lintelligence-artificielle-contre-le-covid-19-ameliorer-la-recherche-et-accelerer-le-diagnostic*

Créé en 2016 après les attentats terroristes de l'année précédente, et initialement conçu pour traiter au maximum 8 000 dossiers par événement, **le fichier SI-VIC (*système d'information pour le suivi des victimes d'attentats et de situations sanitaires exceptionnelles*) a dû être rapidement adapté** à la gestion par les hôpitaux du flux de patients atteints d'une forme grave du Covid-19. Son déploiement, qui s'est accompagné d'inévitables difficultés dans les premières semaines, est aujourd'hui quasi généralisé.

Surtout, deux fichiers *ad hoc* ont dû être mis en place pour lutter contre les chaînes de contamination[1], dans le cadre de la stratégie « Tester, alerter, protéger » :

- **le fichier SI-DEP (*système d'information national de suivi et de dépistage*)**, développé par l'AP-HP et géré par le ministère des Solidarités et de la Santé, est disponible depuis juin 2020. Il contient les résultats des tests PCR et antigéniques, transmis par près de 600 laboratoires publics et privés. Il contient les données suivantes : identification[2], coordonnées personnelles (adresse, téléphone, *e-mail*), date et résultat de l'examen, contexte (hébergement collectif, etc.) et autres informations médicales (date des premiers symptômes, etc.) ;

- **le fichier Contact-COVID**, développé et géré par la CNAM, et disponible depuis le 13 mai 2020. Il permet d'assurer le **suivi des cas positifs** (vérifier que chacun a été appelé, informé, testé, accompagné) et la **conduite des enquêtes sanitaires** (remontée des chaînes de contamination). Il contient principalement les données suivantes : identification[3], données de santé strictement limitées au Covid-19 (statut sérologique, symptômes, etc.), contexte (hospitalisation, isolement, besoin d'accompagnement social, etc.), données nécessaires à l'identification des chaînes de transmission (profession, lieu d'exercice, lieux fréquentés, participation à des événements, existence d'une quarantaine et ses raisons, etc.).

Enfin, **le fichier Vaccin Covid[4], ou VAC-SI,** a été mis en place dans le cadre de la **campagne de vaccination**. Mis en œuvre par la CNAM, il est disponible depuis le 4 janvier 2021 et son utilisation est obligatoire. Il contient les données relatives à l'identité du patient et à la vaccination (éligibilité, nom du vaccin, numéro de lot, date et lieu de chaque injection, etc.), et permet d'**éditer un certificat** pour le patient, désormais informé ***via*** SMS ou courrier électronique. Une fonctionnalité permet également de déclarer les éventuels effets indésirables, par un lien vers le portail de l'ANSM.

---

[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. Les traitements de données réalisés dans le cadre de l'application* TousAntiCovid *font l'objet de développements spécifiques au III.*

[2] *Y compris l'identifiant national de santé (INS).*

[3] *Y compris le numéro de Sécurité sociale (NIR).*

[4] *Décret n° 2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la Covid-19.*

Avant d'en évoquer les limites, il convient de préciser qu'**en elle-même, la mise en place en urgence de ces différents outils *ad hoc* est une réussite qu'il faut saluer**, compte tenu de la difficulté du contexte. En particulier, le fichier **SI-DEP a été développé en moins d'un mois, un temps record, et 90 % des laboratoires y étaient raccordés** au moment du premier déconfinement, alors même qu'un projet similaire porté par Santé Publique France se heurtait depuis huit ans à une succession d'obstacles administratifs.

Il faut en tirer les bonnes leçons, qui valent pour l'ensemble des chantiers informatiques du secteur public : pour réussir, il est indispensable de bénéficier d'une **réelle implication politique**, en l'espèce celle du ministre des solidarités et de la santé et du secrétaire d'État chargé du numérique, d'une **gouvernance forte, ici portée par la délégation ministérielle du numérique en santé (DNS)**, qui a su faire travailler ensemble tous les acteurs concernés (ministère, SPF, laboratoires, éditeurs) et s'appuyer sur l'expertise technique de l'AP-HP, et d'un **financement à la hauteur**. En l'occurrence, le choix a été fait d'une prise en charge par la puissance publique du coût des adaptations logicielles par les éditeurs, tandis que le remboursement des tests aux laboratoires a été conditionné à la bonne saisie des résultats dans SI-DEP.

b) Une remontée d'informations initialement chaotique

La mise en place des fichiers ne suffit pas : encore faut-il être en mesure de les alimenter.

L'impréparation des acteurs concernés est ici apparue de manière criante, en particulier dans le secteur médico-social, où aucun outil ne permettait la remontée des données épidémiologiques au niveau national, ni même au niveau régional. C'est ce qui explique, par exemple, **le retard dans la publication des statistiques des décès en EHPAD par rapport aux décès survenus à l'hôpital, et les nombreuses erreurs dans les chiffres transmis**.

De fait, la remontée des données se faisait *via* de simples tableurs *Excel*, remplis manuellement par les personnels des établissements dont ce n'était ni la compétence, ni la priorité à ce moment-là. **Les données étaient en outre lacunaires**, limitées à des statistiques agrégées, sans qu'il soit possible de connaître la répartition par âge ou par sexe des personnes décédées, pourtant cruciale pour la prise de décision publique. Enfin, cette méthode donnait lieu à des **remontées concurrentes et parfois contradictoires**, par les préfets, les ARS ou encore les départements. Si la mise en place par Santé Publique France, à partir de fin mars 2020, d'un outil de signalement centralisé pour les établissements de santé médico-sociaux, a progressivement permis d'améliorer les choses, les remontées demeurent encore aujourd'hui imparfaites.

Jusqu'à récemment, le fichier SI-DEP **ne permettait pas d'identifier un patient se faisant tester plusieurs fois**, ce qui conduisait à majorer artificiellement le nombre de cas positifs (sans pour autant fausser la compréhension de l'évolution de l'épidémie). Ce problème a été corrigé.

Des problèmes similaires se sont présentés, quoique dans une moindre proportion, pour **la remontée des données de vaccination**. Celle-ci a en effet débuté avant l'ouverture du téléservice Vaccin Covid, les données étant alors transmises par les ARS qui les recueillaient auprès des EHPAD et des centres de vaccination.

La France, bien sûr, n'a pas été la seule à devoir improviser face à une crise sanitaire d'une ampleur inédite. À des degrés divers, tous les pays du monde ont dû s'adapter en un temps très réduit et sous de fortes contraintes, avec leur lot de bourdes. Par exemple, au **Royaume-Uni**, les résultats de plusieurs milliers de tests de dépistage ont été accidentellement « perdus » fin septembre 2020 en raison de la limitation à 65 536 lignes du fichier *Excel* utilisé pour le système *Test and Trace*[1]. **Reste que tous les pays ne se sont pas retrouvés dans la même situation** : ceux qui disposaient d'une avance en matière d'administration numérique, à l'instar de l'Estonie (cf. *supra*), ont connu bien moins de problèmes.

2. Une portée très limitée en l'absence d'interconnexion

a) Le problème de l'interopérabilité

En fait, le problème est surtout que ces outils *ad hoc* ne font que compenser – et très imparfaitement – les insuffisances criantes de notre système de santé en matière numérique. La crise du Covid-19 constitue à cet égard un révélateur et agira, espérons-le, comme une prise de conscience salutaire en amont des prochaines épidémies.

Le principal enjeu est celui de **l'interconnexion des fichiers**.

Tout d'abord, ces différents fichiers ne sont pas connectés entre eux. Ainsi, les données saisies dans **SI-DEP** (résultats des tests) ne sont pas liées aux données saisies dans **Contact-COVID** (suivi des cas contacts) ni dans **Vaccin Covid** (vaccination), ce qui oblige les professionnels concernés à effectuer une **ressaisie manuelle**, et **interdit surtout les recoupements automatiques qui permettraient de sauver de nombreuses vies** (cf. *infra*).

Ensuite, et par nécessité, les outils développés pour la crise l'ont été ***à côté* des grands systèmes existants**, et non pas comme une fonctionnalité de ceux-ci, ce qui **limite grandement le champ des possibilités, y compris pour la gestion immédiate de la crise sanitaire**. Leur intégration, qui

[1] *L'arrêt automatique du téléchargement au-delà de cette limite résulte en outre d'un problème bien connu de la version de* 2003 *de* Microsoft Excel*, les nouvelles versions pouvant aller jusqu'à un million de lignes. Voir à cet égard :* https://news.sky.com/story/coronavirus-data-can-save-lives-data-can-cost-lives-and-this-latest-testing-blunder-will-likely-prove-it-12090904

supposerait que chaque individu soit identifié par un **numéro unique**, se heurte encore à d'importants obstacles à la fois techniques et juridiques (cf. *infra*).

Certes, les choses s'améliorent peu à peu. Depuis le 20 avril, les personnes testées reçoivent un SMS ou un courriel lorsque les résultats sont entrés dans le fichier SI-DEP, et le dispositif devrait bientôt être étendu au fichier VAC-SI. Ces améliorations sont de toute façon **indispensables à la mise en place de la fonctionnalité « Carnet » de *TousAntiCovid***, version française du « certificat vert numérique » européen. **Mais il ne s'agit toujours pas d'une interconnexion** : la saisie se fait manuellement et incombe à l'utilisateur, et ne permet aucun recoupement automatique.

b) Les brigades du monde d'avant

Ce manque d'interopérabilité, qui caractérise en fait l'architecture de l'ensemble notre système de santé, est lourd de conséquences.

Le débat public s'est souvent limité à déplorer les retards dans la production de statistiques à partir de ces fichiers, au niveau national ou départemental, ou encore par classe d'âge ou sexe, utiles à la décision publique et demandées par les citoyens. Mais **les statistiques agrégées de contamination ou de vaccination n'ont pas besoin d'interconnexion**. En revanche, la mission principale de ces fichiers, c'est-à-dire **l'intervention au niveau des individus vulnérables eux-mêmes, ne peut s'en passer**.

Ainsi, l'absence d'interopérabilité a **considérablement entravé la remontée des chaînes de contamination, faisant perdre un temps précieux qui, *in fine*, se paie en vies humaines et en restrictions qui s'éternisent.**

Afin de casser les chaînes de contamination, les autorités sanitaires ont en effet mis en place – dans des délais qu'il faut saluer – **des « brigades de traçage » chargées d'interroger les personnes au téléphone, voire de se déplacer physiquement**, suivant en cela les recommandations du Conseil scientifique dans son avis du 20 avril, qui proposait à cette fin **le recrutement de 30 000 personnes**. Si les chiffres exacts ne sont pas connus, en pratique, ce sont principalement **les agents des ARS et des CPAM** – 4 000 agents pour ces dernières – qui ont été mobilisés. En Île-de-France, **l'AP-HP** a mobilisé 800 agents répartis en 34 équipes pour effectuer des visites à domicile[1], dans le cadre du programme « Covisan ».

Le problème est que les agents chargés de ce travail, une fois connues les circonstances dans lesquelles le « patient zéro » a pu contaminer ses contacts, **n'ont pas la possibilité de savoir lesquels de ces contacts ont ensuite été infectés. Il suffirait pourtant, tout simplement, de croiser les bases Contact-COVID et SI-DEP – mais aucun croisement n'est fait**.

[1] https://www.aphp.fr/actualite/lancement-de-covisan-un-dispositif-de-suivi-renforce-des-personnes-covid

Comme l'indique le directeur général de la CNAM, Thomas Fatome[1], *« c'est un peu compliqué côté système d'information. On aimerait obtenir ce type de données de façon plus systématique mais, pour l'instant, on ne peut pas le faire.* (…) *On est très attentifs à ces fichiers qui sont des données sensibles ».* **En pratique, la « chaîne » de contamination se réduit donc bien souvent à un seul maillon**.

Or le dispositif des « brigades de traçage », coûteux en ressources humaines et financières, présente par ailleurs d'importantes limitations : au moins aurait-on pu lui épargner cette entrave supplémentaire, d'autant qu'elle était en l'occurrence parfaitement évitable.

Les autres limitations, que le secrétaire d'État chargé de la transition numérique, Cédric O, rappelle lui-même dans un message du 3 mai 2020, à l'appui de la cause de l'application *StopCovid*[2], sont déjà très fortes :

*« **Leur temps de réactivité** : dans un contexte où une part importante de contaminations (la moitié selon l'équipe d'épidémiologistes anglais ayant évoqué la première l'utilité de l'application) se fait avant même que les personnes vecteur ne développent les premiers symptômes (sans compter les asymptomatiques), il est impératif de couper les « départs de feu » quasiment en temps réel — ce que ne peuvent faire les brigades sanitaires confrontées à des limites physiques évidentes ; quelques heures de gagnées peuvent sauver des vies ;*

*« **La mémoire des personnes interrogées** : il n'est pas aisé, qui plus est dans les conditions de stress que l'on imagine aisément, de se souvenir de l'ensemble de ses interactions sociales, même sur les seuls derniers jours ; en période normale, les « cas contacts » d'une personne donnée sont entre 30 et 50 ;*

*« Ces enquêtes sanitaires se heurtent surtout, dans les centres urbains, à **l'impossibilité de reconstituer les chaines de transmission dans les transports en commun, les lieux publics ou les commerces** ; il est impossible (…) de retrouver une personne assise à côté de vous pendant 10 minutes dans le métro ».*

Dans le cas d'une épidémie qui a déjà touché une part importante de la population française, la tâche des « brigades de traçage » **revient bien souvent à chercher une aiguille dans une botte de foin**.

Il ne s'agit pas pour autant de conclure à l'inutilité pure et simple du dispositif : le *contact tracing* est encore une technologie immature (cf. *infra*), et un outil en réalité aussi *peu* intrusif que *TousAntiCovid* ne saurait suffire à lui seul à identifier les chaînes de contamination. **Les deux approches sont plutôt complémentaires – et elles ont en commun leur inefficacité, conséquence directe du refus de croiser les fichiers, dans un cas comme dans l'autre.**

---

[1] Le Monde *du 8 mai 2020 : https://www.lemonde.fr/pixels/article/2020/05/08/suivi-des-cas-contacts-ce-que-contiendront-les-deux-nouveaux-fichiers-medicaux-prevus-par-l-etat_6039059_4408996.html*

[2] *https://cedric-o.medium.com/stopcovid-ou-encore-b5794d99bb12*

La différence est qu'un outil « purement » numérique, pour peu que soient levées certaines réticences, offre **des perspectives d'efficacité que n'a pas et n'aura jamais le travail « manuel » des centres d'appel**.

À cet égard, on ne peut que déplorer la disproportion des critiques adressées à chacun des dispositifs, jusqu'au paradoxe : *TousAntiCovid* est totalement anonyme et automatique, alors que **les enquêtes téléphoniques impliquent que les citoyens livrent, à des inconnus, des informations personnelles nominatives, y compris médicales et souvent intimes**, sur leurs allées et venues, leurs activités, leurs fréquentations.

3. Le rôle de la société civile et la question de la dépendance aux acteurs privés

Alors que les pouvoirs publics se révélaient en partie incapables d'exploiter pleinement les possibilités ouvertes par le numérique, **des acteurs privés, au sein de la société civile notamment, ont parfois pris le relais au pied levé**.

Tout d'abord, cette crise a révélé **une forte demande citoyenne pour des éléments précis et chiffrés sur l'épidémie**, qui constituent un levier précieux pour susciter l'adhésion à des mesures difficiles – au point que les allocutions les plus solennelles du Président de la République s'accompagnent désormais de cartes et autres graphiques, à la manière des *slides* d'un consultant. **Dans ce domaine, la société civile a tout de suite fait bien mieux que l'administration**. On peut évidemment se féliciter de ces multiples initiatives qui témoignent d'un véritable dynamisme au sein de la société. Mais on peut aussi se demander pourquoi l'État n'est pas capable de produire des chiffres fiables et « parlants », quand un jeune informaticien de 24 ans – Guillaume Rozier, le créateur des sites ***Covid Tracker*** et ***Vaccin Tracker***, pour ne citer que lui – peut le faire, et de surcroît avec des outils de visualisation (*datavizualisation*) de grande qualité ?

D'importants progrès ont toutefois été réalisés en peu de temps, et Santé Publique France publie désormais près de 80 indicateurs, dont certains sous forme de cartes, sur sa plateforme et sur la plateforme d'*open data* du Gouvernement, *Etalab*. On peut notamment souligner le rôle joué par la plateforme ***OpenCovid***, une initiative lancée dès mars 2020 pour agréger les données des ministères, des ARS, des préfectures, etc., à l'époque où aucune base de données publique exhaustive n'existait, et où les chiffres officiels se limitaient au bilan hebdomadaire de Santé Publique France. Comme le relève le rapport de la mission Bothorel sur l'*open data*[1], *OpenCovid* a constitué « ***un levier essentiel pour l'ouverture des données*** » : « *la découverte de* veille-coronavirus.fr *au sein de l'administration a accéléré les*

[1] « Pour une politique publique de la donnée », *rapport de la mission confiée par le Premier ministre à Éric Bothorel, député des Côtes d'Armor, Stéphanie Combes, directrice du* Health Data Hub*, et Renaud Vedel, coordinateur national pour l'IA, décembre 2020.*

discussions et a rendu indispensable la communication des chiffres officiels exhaustifs sur la situation sanitaire ». Or, si *OpenCovid* est bien une initiative citoyenne, ses membres entretiennent par ailleurs des liens étroits avec Etalab, qui opère la plateforme publique *data.gouv.fr*, de sorte que les indicateurs et tableaux de bord d'*OpenCovid* ont ensuite pu être été intégrés facilement aux plateformes officielles.

Par contraste, les pays les plus avancés en matière d'administration numérique ont été très rapidement en mesure de fournir à leurs citoyens des informations précises sur l'évolution de l'épidémie. C'est notamment **le cas de l'Estonie** (cf. *supra*).

Au niveau mondial, la plateforme du *Coronavirus Resource Center* de **l'université Johns Hopkins** s'est très vite imposée comme la référence en matière d'agrégation des données, bien davantage, par exemple, que celle de l'OMS.

Le rôle de la société civile ne s'est pas limité à l'information des citoyens : il a aussi joué **un rôle actif dans la réponse à la crise, notamment dans le cadre des campagnes de dépistage et de vaccination.** Le site *ViteMaDose*, associé à *Covid Tracker*, a par exemple permis d'offrir une solution simple, rapide et fiable pour trouver des créneaux de vaccination. Fin mai, 300 000 créneaux de vaccination y étaient disponibles, et plus de 2 500 centres de vaccination étaient couverts. Le site ***CovidListe***, quant à lui, permettait aux publics non prioritaires de bénéficier d'éventuelles doses non utilisées en fin de journée.

Au-delà des bénévoles de la société civile, ce sont surtout des entreprises privées qui ont permis de combler rapidement les insuffisances de l'administration dans le domaine de la logistique et de la gestion de la crise. Ce fut notamment le cas pour **la prise de rendez-vous en ligne et la téléconsultation**. **Le site *Doctolib* est ainsi devenu incontournable pour la réservation des créneaux de vaccination** : 90 % des réservations se font par son intermédiaire, dans le cadre d'un partenariat avec l'Assurance maladie[1]. C'est même Doctolib qui, le 31 mai, a annoncé que l'objectif de 30 millions de personnes vaccinés pourrait être atteint « avec cinq jours d'avance » sur l'objectif fixé par le Gouvernement.

En soi, le rôle joué par ces acteurs privés n'est pas un problème - ni à court terme, compte tenu de l'insuffisance de la réponse publique à ce moment-là, **ni à long terme**, car la *e-santé* de demain ne pourra pas se bâtir sans associer l'ensemble des acteurs innovants, qu'ils soient publics, privés ou issus de la société civile. **Nous devrions donc commencer par nous réjouir d'avoir pu, grâce à l'une des rares « licornes » françaises, disposer d'un outil numérique performant** pour gérer la campagne de vaccination.

---

[1] *Voir notamment https://www.lemonde.fr/economie/article/2021/05/20/les-ambitions-devorantes-de-doctolib_6080802_3234.html*

Toutefois, le rôle joué par certains acteurs privés peut aussi conduire à **instituer une dépendance plus problématique**. À cet égard, **le rôle joué par les géants du numérique** dans la crise actuelle, en matière notamment de *contact tracing*, doit nous interpeler : il n'est qu'un avant-goût de ce qui pourrait arriver demain, avec des solutions dont la puissance et l'efficacité se paieront d'une dépendance peut-être irréversible.

B. LE GRAND CHANTIER DU NUMÉRIQUE EN SANTÉ

Si la France s'est appuyée sur des dispositifs numériques *ad hoc* pour faire face à la pandémie, avec toutes les limites que cela implique, c'est tout simplement parce qu'**elle n'était pas prête : son système de santé repose sur des systèmes informatiques qui ne sont pas faits pour la gestion de crise**, qu'il s'agisse du suivi individuel des patients (1) ou de l'exploitation des données de santé agrégées (2).

Pourtant, les choses commençaient à changer, notamment grâce à la « feuille de route du numérique en santé » présentée en avril 2019, et aux mesures du volet numérique de la loi Santé du 24 juillet 2019[1] – mais la crise est arrivée trop vite.

1. Une plateforme de santé unique, condition indispensable à la gestion de l'épidémie au niveau individuel

a) La feuille de route de 2019 : une réponse au retard accumulé ?

Comme évoqué dans la première partie du présent rapport, **les pays disposant d'un système de santé organisé sur le modèle d'une plateforme numérique**, où les bases de données sont interopérables, où les services sont automatiquement liés entre eux et où chaque usager dispose d'un identifiant unique, **ont disposé d'un atout précieux dans leur gestion de la crise sanitaire**. C'est notamment le cas de **l'Estonie**.

La France, quant à elle, est très loin du compte. Si elle n'est pas, loin de là, le seul pays au monde dans ce cas, elle fait pourtant partie des premiers à avoir théorisé puis lancé ce grand chantier. Mais celui-ci s'est **heurté à l'immense complexité de son système de santé**, au morcellement des services et des acteurs, à la rigidité des règles et des structures, à l'incompatibilité des systèmes d'informations – en bref, au poids de sa longue histoire, mais aussi au manque de courage politique et au conservatisme des acteurs concernés.

---

[1] *Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.*

La France a ainsi accumulé un important retard[1], lourd de conséquences pour la santé en général (cf. encadré), et **pour la gestion des crises sanitaires en particulier – celle du Covid-19 et les suivantes**.

Le **dossier médical partagé (DMP)** est sans doute l'exemple le plus significatif. Lancé en 2004, ce chantier a connu des débuts laborieux, sinon chaotiques. En 2012, seuls 158 000 dossiers avaient été ouverts, dont 89 500 vides de toute information. Suspendu en 2012, il est relancé en 2016, avec cette fois des résultats plus encourageants. En novembre 2018, la ministre de la Santé, Agnès Buzyn, annonce sa volonté de généraliser le DMP d'ici 2023.

Les enjeux de la e-santé

Les enjeux du développement du numérique en matière de médecine et de santé **vont bien au-delà de la prévention et de la gestion des épidémies**.

Sans développement du numérique, **la médecine des « 4P » – prédictive, préventive, personnalisée et participative –** ne demeurera en France qu'un horizon très lointain.

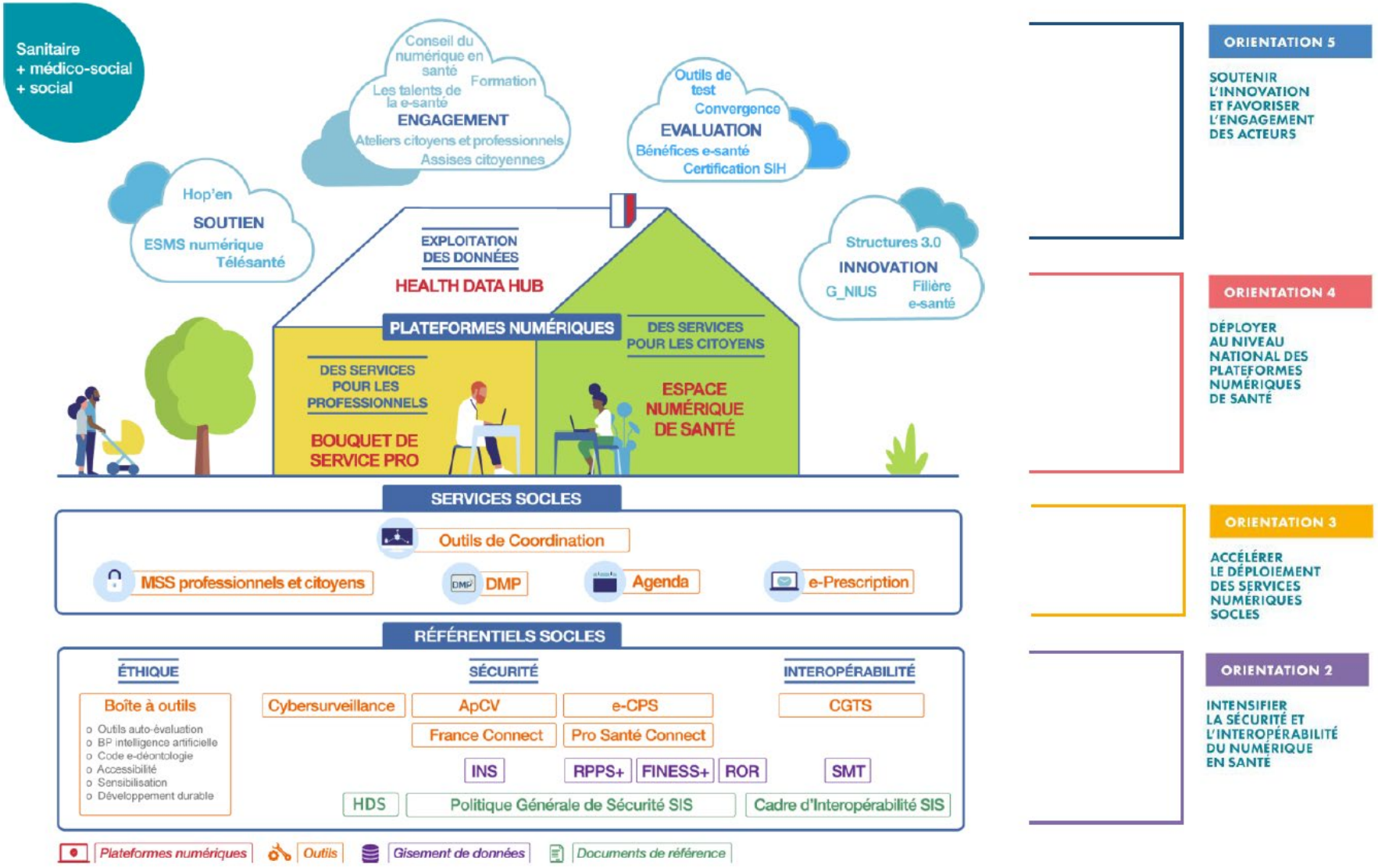
Or, pour reprendre les termes de l'Institut Montaigne dans le rapport qu'il a récemment consacré au sujet, « *le* ***déploiement de la e-santé associé à un recueil systématique des données de santé*** *fait partie des bases indispensables sur lesquelles doit reposer notre système de soins. Cette digitalisation est essentielle pour répondre aux nombreux défis auxquels le système fait face : l'explosion des maladies chroniques, le vieillissement de la population, l'évolution du nombre de soignants sur le territoire, la soutenabilité économique du système de santé et les nouveaux défis sanitaires et sociaux. (…)* ***Pourtant, de nombreux outils numériques permettent déjà d'avoir une vision de ce que pourrait être la santé de demain*** *: des patients acteurs de leur santé grâce aux objets connectés et au suivi à distance, des professionnels de santé accompagnés par des logiciels d'aide au diagnostic et aux traitements, un système de santé plus collaboratif et agile* ».

Source : Institut Montaigne, « e-santé : augmentons la dose ! »*, juin 2020*

Présentée par la ministre de la Santé le 15 avril 2019, **la « feuille de route du numérique en santé » visait précisément à combler ce retard**, en commençant par un **renforcement inédit de la gouvernance**, qui s'est traduit par la création, fin 2019, de la **délégation ministérielle au numérique en santé (DNS)**, chargée du pilotage de l'ensemble des projets menés, pour les faire avancer dans la même direction.

[1] *De nombreux rapports alertent de longue date sur ce retard. Citons par exemple le rapport n° 465 (2014-2015) du 26 mai 2015, intitulé* « Le numérique au service de la santé »*, fait par Catherine Procaccia, sénateur, et Gérard Bapt, député, au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST), à la suite d'une audition publique organisée le 15 mai 2014 sur le sujet.*

Le numérique en santé : l'image de la maison



Source : Ministère des Solidarités et de la Santé, feuille de route du numérique en santé – Bilan 2020

Sans entrer dans le détail d'un sujet qui excède le cadre du présent rapport, on pourra rappeler que le grand chantier du numérique en santé repose sur les éléments suivants (cf. schéma ci-dessus) :

- **des référentiels socles**, soit une série de répertoires, de règles de sécurité, de standards d'interopérabilité et de principes de conception « éthiques », qui constituent ensemble la **condition préalable** à la réussite et à la pérennité de tous les autres projets. **L'identifiant national de santé (INS)** est l'un de ces référentiels socles ;

- **des services socles** à destination des usagers, soit principalement la messagerie sécurisée de santé (MSS), un agenda, un service de e-prescription et le **dossier médical partagé (DMP)** ;

- **trois plateformes numériques**, permettant d'accéder simplement à un ensemble d'applications et de services connectés entre eux : **l'espace numérique de santé (ENS)** grâce auquel chaque usager bénéficiera d'un compte personnel unique lui donnant accès à ses données personnelles et à un ensemble de services, le **Bouquet de services** pour les professionnels, et le ***Health Data Hub*** (cf. *infra*) pour les chercheurs.

b) Ce que l'espace numérique de santé (ENS) aurait changé

Début 2020, lorsque la pandémie a frappé la France, ce chantier n'en était qu'à ses débuts – au stade de la remise à plat des référentiels socles, pour l'essentiel. Or, **s'il s'était trouvé à un stade plus avancé, il aurait pu changer la donne. La généralisation de l'échange et du partage sécurisé de données** de santé entre professionnels de santé d'une part, et avec l'usager d'autre part, aurait en effet permis d'**assurer beaucoup plus efficacement le suivi individuel des patients et des cas contacts dans le cadre de la stratégie « Tester, alerter, protéger ».**

Deux outils cruciaux ont en particulier fait défaut : l'espace numérique de santé (ENS), outil majeur de la couche « supérieure » du système qui contient notamment le DMP, **et l'identifiant national de santé (INS).**

Pour reprendre les mots de Laura Létourneau, déléguée ministérielle au numérique en santé, lors de son audition par la commission des affaires sociales de l'Assemblée nationale le 17 février 2021[1], « *si nous avions eu **l'espace numérique de santé**, nous aurions pu **référencer dans le catalogue toutes les applications de téléconsultation** qui respectaient les référentiels d'interopérabilité et de sécurité ; **disposer d'une messagerie sécurisée citoyenne***

[1] *Table ronde du 17 février 2021 sur le numérique en santé à l'heure de la crise sanitaire : audition de Laura Létourneau, déléguée ministérielle au numérique de la santé (DNS), Emmanuel Gomez, directeur délégué à la gestion et à l'organisation des soins de la Caisse nationale de l'assurance maladie (CNAM), Annika Dinis, directrice opérationnelle du numérique et de l'innovation de la CNAM, Sara-Lou Gerber, directrice de cabinet du directeur général de la CNAM, Dominique Martin, médecin-conseil national de la CNAM et François Lescure, président du LET - Les Entreprises de la Télémédecine.*

et envoyer des prescriptions de tests Covid *ou échanger de nombreuses informations avec le patient ;* ***croiser simplement les données issues de SI-DEP, de Contact Covid et de Vaccin Covid*** *afin de déterminer si une personne vaccinée pouvait être recontaminée* ».

Toutes les informations pertinentes concernant un patient ou un cas contact auraient été **rassemblées en un même endroit, et auraient pu être exploitées systématiquement de façon sécurisée**. Les perspectives vont bien au-delà d'un simple rapprochement des données liées au Covid-19 et issues des fichiers SI-DEP (tests), Contact-COVID (contacts) et VAC-SI (vaccins) :

- **le DMP** aurait donné accès (sous réserve d'autorisation expresse) à l'historique médical du patient, donc à ses **éventuelles comorbidités** et à des **facteurs de risques** peut-être inconnus – du patient, du professionnel ou même de la recherche médicale – au moment des enquêtes ;

- **les autres fonctionnalités de base (messagerie, prise de rendez-vous et e-prescription)** auraient facilité le suivi des mesures (isolement, etc.) et l'organisation logistique des campagnes de dépistage et de vaccination ;

- **le catalogue d'applications tierces** disponibles *via* l'ENS aurait permis de déployer rapidement et massivement des services utiles dans le contexte de la crise, exploitant par exemple **les données médicales (ECG, poids, etc.) issues d'objets connectés**, à l'instar de l'application *HealthMate* de *Withings*, qui centralise les données issues de ses montres connectées, balances connectées, capteurs de sommeil, etc. **Une trentaine de solutions** de ce type font actuellement l'objet d'une étude à cette fin par la DNS, en association avec l'ANSSI (sécurité) et la CNIL (données personnelles), pour un déploiement en 2022.

Plusieurs applications spécifiques au Covid-19 sont d'ores et déjà disponibles sur le catalogue de l'ENS[1] : aux services directement proposés par le ministère des Solidarités et de la Santé (*Dépistage Covid* et *Mes Conseils Covid*) s'ajoutent par exemple **des applications de téléconsultation ou de télésuivi** (questionnaires en ligne, *chatbots*, *bots* téléphoniques, etc.) comme *MonMedecin.org, AlloCovid, Therap-e, MaQuestionMedicale*, ou *Stimulab*, ou encore **des guides interactifs** sur les conduites à tenir, à l'instar d'*Obal* qui permet de suivre l'usage des différents types de masques. Mais il s'agit pour l'instant d'**apports tout à fait modestes** (une application qui rappelle les gestes barrière, comme s'il était possible de les oublier…), et très-deçà de ce que l'on pourrait attendre pour une gestion de crise efficace.

Ainsi, peut-être s'en est-il fallu de peu – quelques années tout de même – pour que la France dispose, avec l'ENS, d'outils autrement plus efficaces pour réagir à une crise comme celle du Covid-19.

---

[1] *La liste – encore très modeste – est disponible ici : https://www.sante.fr/covid-numerique*

De façon plus optimiste, on peut supposer que les choses auraient été plus graves si la crise était arrivée un peu plus tôt : le rôle de pilotage confié à la DNS a indéniablement facilité la mise en place rapide des outils *ad hoc* faute de mieux, et ceux-ci en dépit de leurs limites sur le plan du suivi individuel, ont permis de doter la France de l'un des dispositifs de suivi épidémiologique les plus performants du monde.

La nécessité d'investir massivement dans le numérique en santé est désormais un acquis, et **2 milliards d'euros supplémentaires lui ont été accordés au titre du « Ségur de la Santé »** pour développer les services prioritaires (DMP, ENS, INS, etc.)[1].

Malgré la crise – si ce n'est grâce à elle –, les travaux préparatoires (passation du marché, développement, etc.) se sont poursuivis à un rythme soutenu en 2020, et **« Mon espace santé » (son nouveau nom), devrait être accessible à l'ensemble des Français en janvier 2022**, après une phase d'expérimentation débutant en juillet 2021 pour 1,3 million de personnes.

Gardons-nous toutefois d'un optimisme démesuré : si le plan « Ma Santé 2022 » et la crise sanitaire ont permis une mobilisation salutaire et inédite en faveur du numérique en santé, **la seule certitude à ce stade est que la France n'était pas prête**. D'autres grands « plans » ont échoué dans la période récente, et il conviendra de ne pas relâcher l'effort une fois cette crise terminée.

c) Ce que l'identifiant national de santé (INS) aurait changé

Après l'espace numérique de santé, **l'identifiant national de santé (INS) est l'autre outil majeur dont la France a cruellement manqué**, entre autres, pour gérer efficacement la crise, s'agissant du suivi sanitaire au niveau individuel et de l'organisation du parcours de soins. Il s'agit de l'un des référentiels socles de la feuille de route du numérique en santé.

En effet, il n'existe pas aujourd'hui d'identité unique et pérenne pour identifier une même personne au sein du système de santé, mais un grand nombre d'**identifiants « locaux »** attribués séparément par l'hôpital, le médecin de ville, le laboratoire, le dentiste, etc., selon des règles fixées par chaque acteur, sources de fréquentes erreurs d'identification (homonymes, nom de jeune fille, nom composé, etc.) et de démarches administratives inutiles, pesant à la fois sur les patients et les professionnels. Cette situation **entrave considérablement l'échange et le partage de données** entre l'ensemble des acteurs intervenant dans la prise en charge et le suivi médico-social de la personne, et **nuit à la qualité et à la sécurité des soins**. Elle cause des retards de prise en charge, des erreurs de diagnostic ou de thérapie, ou encore des phénomènes de patients « perdus de vue ».

[1] *Sur ces 2 milliards d'euros, 1,4 milliard d'euros seront consacrés sur 3 ans aux services prioritaires, et 600 millions d'euros sur 5 ans seront spécifiquement alloués au secteur médico-social pour le rattrapage de son retard en matière de numérique, d'après les annonces du 21 juillet 2020.*

En situation de crise sanitaire, lorsque le système de soins est sous pression et que la rapidité et l'efficacité de la prise en charge revêtent une importance cruciale, l'absence d'un identifiant unique de santé est lourde de conséquences.

Pourtant, tout citoyen français se voit attribuer à la naissance un numéro de Sécurité sociale, le NIR, ou numéro INSEE, qui permet son inscription au répertoire national d'identification des personnes physiques (RNIPP) et constitue un identifiant unique et fiable. Toutefois, soucieuse d'éviter les interconnexions de fichiers et afin de prévenir toute utilisation des données personnelles à d'autres fins que celles qui ont justifié leur collecte, **la CNIL a toujours refusé l'utilisation du NIR au-delà de la sphère sociale, s'opposant en particulier à son utilisation dans le domaine de la santé**[1]. En vertu de cette doctrine de « cantonnement », le NIR saurait être utilisé qu'à des fins administratives, par la Sécurité sociale et ses partenaires (professionnels et établissements de santé, organismes d'assurance maladie obligatoires et complémentaires, assurance chômage, employeurs, etc.), afin de procéder aux remboursements des soins, d'assurer le paiement des cotisations sociales et de verser les droits sociaux aux assurés. **Par conséquent, la CNIL s'était opposée en 2007 à l'utilisation du NIR en tant qu'identifiant du DMP**[2], une décision qui n'est pas étrangère à l'impasse dans laquelle celui-ci s'est longtemps trouvé.

La loi Santé du 24 juillet 2019[3] **a permis de renverser cette doctrine, en prévoyant l'utilisation du NIR comme identifiant national de santé**. Plus précisément, l'INS est constitué du **NIR et de cinq « traits d'identité »** permettant une identification certaine (nom de naissance, prénom, date de naissance, lieu de naissance, sexe), auxquels s'ajoute l'identifiant de l'organisme qui a attribué l'INS. **L'ensemble est sécurisé par le téléservice INSi**, qui permet aux seuls acteurs de la santé d'obtenir l'INS d'un patient ou usager, conformément aux standards d'identitovigilance.

Initialement fixée au 1er janvier 2020, **l'obligation d'utiliser l'INS pour référencer les données de santé a été reportée au 1er janvier 2021**. En pratique, toutefois, sa généralisation est encore loin d'être effective. Elle dépend en particulier de la mise à jour des multiples logiciels[4] utilisés par les professionnels et les établissements de santé – et de la bonne volonté de ces derniers à l'utiliser.

---

[1] *Il faut préciser que le NIR, composé de 15 chiffres indiquant notamment le sexe, le mois et l'année de naissance, est particulièrement signifiant en lui-même. Rétrospectivement, ce choix initial, plutôt que d'un numéro « neutre », peut apparaître malheureux.*

[2] *Conclusions de la CNIL sur l'utilisation du NIR comme identifiant de santé, 20 février 2007.*

[3] *Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé et décret n° 2019-1036 du 8 octobre 2019 modifiant le décret n° 2017-412 du 27 mars 2017.*

[4] *Lors de la publication du bilan 2020 de la feuille de route du numérique en santé, 49 solutions logicielles étaient ainsi capables d'utiliser l'INS.*

Une partie des 2 milliards d'euros alloués au numérique par le « **Ségur de la Santé** » devrait d'ailleurs permettre de prendre en charge les coûts de développements liés à l'intégration de l'INS.

Au-delà de l'INS, la crise a également permis d'accélérer la mise en œuvre d'un **autre élément fondamental du « socle » du système : les cartes professionnelles « e-CPS »,** dont le nombre a connu une très forte augmentation, tirée par le déploiement de SI-DEP et SI-VAC**.**

2. Le *Health Data Hub* et l'exploitation des données agrégées : un effort à poursuivre pour des perspectives immenses

a) Une plateforme de partage des données à l'avenir très prometteur

Le numérique n'est pas seulement indispensable à une meilleure gestion de la crise sanitaire au niveau individuel : **l'enjeu est aussi celui de l'exploitation des données au niveau agrégé, à des fins de recherche médicale et de modélisation épidémiologique**. C'est l'autre aspect majeur de la e-santé. Dans une crise comme celle du Covid-19, ces données constituent par exemple une ressource précieuse pour **développer des vaccins ou des traitements, identifier d'éventuels effets indésirables ou prédispositions, et guider les autorités dans la prise de mesures difficiles** (confinements, restrictions, etc.).

Tel est précisément l'objectif du *Health Data Hub* (HDH), la plateforme des données de santé (PDS) créée par la loi Santé de 2019[1], à la suite notamment du rapport de Cédric Villani sur l'intelligence artificielle[2], qui pourrait **faire de la France le leader mondial de l'IA en santé**.

Comme le souligne le rapport Bothorel sur l'*open data*, cosigné par la directrice du *Health Data Hub*, Stéphanie Combes, « *dans le domaine de la santé, c'est par le traitement et le croisement d'un grand volume de données de qualité, que les recherches à plus grand impact peuvent être menées, par exemple pour améliorer le dépistage et le diagnostic d'une maladie, analyser les effets secondaires des traitements, faire évoluer les essais cliniques. **Les données publiques et d'intérêt général peuvent donc être mises au service de la data science et de l'IA**, qu'il s'agisse de projets publics, privés ou mixtes. Une grande partie de l'IA se développe sur des ressources ouvertes, des jeux de données d'entraînement, des modèles pré-entraînés et des logiciels libres* ».

---

[1] *Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé et arrêté du 29 novembre 2019.*

[2] *Cédric Villani, Marc Schoenauer, Yann Bonnet, Charly Berthet, Anne-Charlotte Cornut, François Levin et Bertrand Rondepierre,* « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne », *rapport remis au Premier ministre le 28 mars 2018.*

Des « *hubs* » pour valoriser les données

Les « *hubs* » désignent des infrastructures de stockage de données provenant de multiples sources, ainsi que les outils de traitement et d'analyse associés et les services d'organisation et d'animation de la communauté.

Beaucoup de projets dans le domaine de l'intelligence artificielle nécessitent d'accéder à des données détenues par des tiers, et qui n'ont pas vocation à être publiques (en raison par exemple du secret fiscal, médical, ou professionnel).

On recense aujourd'hui **huit hubs sectoriels ou intersectoriels**, dont certains ne sont qu'à l'état de projet :

	Domaine	Initiative	Ouverture	Infrastructure	Modèle économique
Health Data Hub	Santé	Loi Santé 2019	Accès distant	Cloud centralisé (entrepôt de données)	Gratuit/ Payant pour acteurs privés
Green Data Hub	Environnement	Publique	Ouvert/ Partage	Non arrêté	Non arrêté
Energy for Climate (E4C)	Énergie/ Climat	Polytechnique/Ponts	Ouvert/ Partage/ Accès distant	Mutualisation	Non arrêté
AgDataHub	Agriculture	Filière	Ouvert/ Partage/ Accès distant	Cloud centralisé (entrepôt de données)	Abonnement
Alliance Culture Data	Industries culturelles	Filière	Ouvert/ Partage/ Accès distant	Non arrêté	Non arrêté
Apidae Tourisme	Tourisme	Filière région ARA	Partage	En propre	Abonnement
Numalim	Agroalimentaire	Filière	Partage/ Ouvert	Mixte (centralisée et décentralisée)	Abonnement, commission, formation

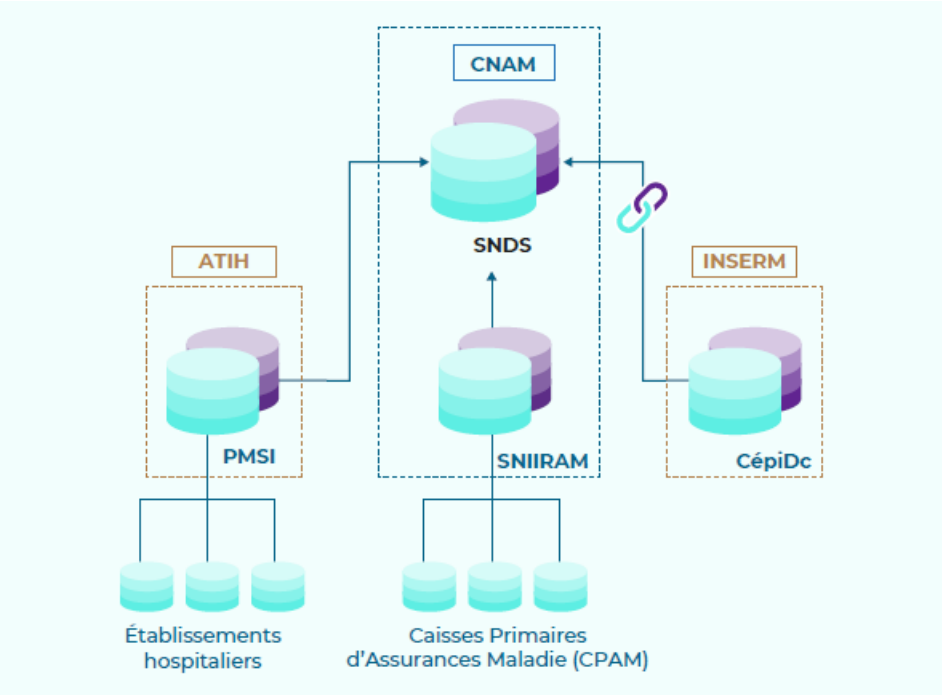
Source : délégation à la prospective, d'après le rapport de la mission Bothorel

D'un point de vue juridique, le HDH est un groupement d'intérêt public (GIP), qui associe **56 membres fondateurs**, principalement issus du secteur public (CNAM, CNRS, Haute autorité de santé, etc.), mais représentant également les usagers (France Assos Santé) et, bien sûr, les acteurs privés de la santé. Son financement est majoritairement public.

Concrètement, le HDH est **un guichet unique permettant un accès aisé et unifié, transparent et sécurisé aux données de santé**, sous la forme d'un **catalogue** comprenant, d'une part, les bases de **données médicales et administratives issues du Système national des données de santé (SNDS)**[1], et d'autre part, de **nouvelles bases de données**.

[1] *Créé en 2016, le SNDS est un entrepôt de données médico-administratives pseudonymisées couvrant l'ensemble de la population française et contenant l'ensemble des soins présentés au*

Le Système national des données de santé (SNDS)



Source : rapport annuel 2020 du Health Data Hub

L'accès se fait dans le respect du droit des patients, dont les données sont **pseudonymisées**.

b) Une portée encore limitée pendant la crise

Le *Health Data Hub* est opérationnel depuis 2020, quoique son catalogue soit encore réduit. **Face à la crise sanitaire, le Gouvernement a pris la décision d'accélérer son déploiement**, en l'autorisant par arrêté à centraliser les données du SNDS pour les besoins de la recherche sur le Covid-19, ainsi que les **données issues des fichiers SI-VIC, SI-DEP et Contact Covid**.

Plusieurs projets de recherche ont ainsi pu être lancés, en dépit des lenteurs et difficultés liées à la procédure d'autorisation préalable par la CNIL (cf. II *infra*).

remboursement. Il permet de croiser les données de l'assurance maladie (base SNIIRAM), les données des hôpitaux (base PMSI), les causes médicales de décès (base du CépiDC de l'Inserm), les données relatives au handicap (données de la CNSA), et d'autres données à venir.

Exemple de projets menés *via* le *Health Data Hub* en lien avec la pandémie de Covid-19

Le projet CoviSAS : *en partenariat avec la chaire d'intelligence artificielle MIAI de l'université Grenobles-Alpes et l'entreprise Semeia, il vise à connaître la prévalence des formes sévères de la COVID-19 chez les patients atteints du syndrome d'apnée obstructive au sommeil. En effet, ces derniers sont plus à risque de développer des pathologies associées à des formes plus graves de la Covid-19 (diabète, hypertension). Les résultats contribueront ainsi à l'amélioration des connaissances sur l'épidémie, et à la définition de stratégies de prévention et de prise en charge précoce pour les patients touchés par ces comorbidités. Pour reconstituer le parcours de soins des patients atteints du syndrome, l'étude repose sur les données du SNDS, notamment celles des hospitalisations et celles sur la consommation de médicaments.*

Le projet FrogCovid : *en partenariat avec l'unité de recherche MASCOT de l'INSERM et Clynitix, sur les données du SNDS, l'étude s'intéresse aux facteurs prédictifs du risque de développer une forme sévère de la Covid-19, afin de mieux comprendre qui sont les facteurs à risque, et développer des accompagnements post-hospitalisations plus pertinents. Les conséquences d'un passage en réanimation pour chaque profil de patient caractérisé seront également mieux connues.*

Le projet CoData : *en partenariat avec l'Institut de cancérologie Strasbourg Europe (ICANS) et Quantmetry, cette étude se penche sur l'impact de la première vague de la Covid19 sur la prise en charge de patientes atteintes du cancer du sein. Les données analysées permettent de fournir un panorama complet des parcours de soin de ces patientes. L'objectif est de comprendre l'impact des perturbations issues de la pandémie de la Covid-19 sur leur la prise en charge et ainsi développer des outils de pilotage aux hôpitaux pour les aider vers un retour à la normale.*

Source : audition du Health Data Hub *par les rapporteurs*

Si le *Health Data Hub* n'est pas, en lui-même, un outil de gestion de crise, les recherches qu'il facilite peuvent néanmoins contribuer de manière décisive à la réponse à une menace sanitaire. **Toutefois, la plateforme n'en est pour l'instant qu'à ses premiers pas**, et si la crise a permis d'accélérer certains chantiers, elle en a aussi ralenti d'autres. Le Covid-19 est, pour ainsi dire, arrivé trop tôt pour que le *Health Data Hub* puisse démontrer toute son utilité.

À plus long terme, toutefois, **son interopérabilité avec, par exemple, le DMP ou les applications tierces de l'espace numérique de santé** pourrait s'avérer un atout considérable dans la gestion d'une crise sanitaire.

L'usage du SNDS dans le cadre de la crise du Covid-19

Bases de Données	Usages déjà identifiés
OSCOUR (Santé Publique France) : Résumés individuels des passages aux urgences depuis le 1er janvier 2020 à date	› Suivi de l'évolution de la crise › Analyse de la variation des motifs de passage aux urgences pendant le confinement › Analyse du non recours aux soins pendant la crise de la Covid-19
SNDS Fast Track (CNAM, ATIH, Établissements de santé) : Données issues du PMSI MCO concernant les séjours Covid-19 ("PMSI Fast Track") appariées avec les données du SNDS sur la consommation de soins (période de janvier à mai 2020)	› Analyse des parcours de soin des patients hospitalisés pour Covid-19 › Identification des facteurs de risque de formes plus ou moins sévères de la Covid-19 › Compréhension de l'impact des formes sévères de la Covid-19 sur les patients et anticipation des soins en sortie d'hospitalisation / de réanimation
SIVIC (DGS) : Données de prise en charge hospitalière des patients soignés pour la Covid-19 (transfert en cours)	› Suivi de la propagation de l'épidémie › Analyse des inégalités sociales de santé grâce au croisement avec d'autres sources
SIDEP (DGS) : Résultats des tests de dépistage de la Covid-19 remontant depuis le 16 mai 2020 (à venir)	› Suivi de la propagation de l'épidémie et développement de modèles prédictifs › Étude des antécédents médicaux des personnes atteintes de la Covid-19 grâce au croisement avec d'autres bases (par ex. SNDS) liés à l'infection à la Covid-19 › Analyse de l'impact à long terme de la Covid-19 sur la santé grâce au croisement avec d'autres bases (par ex. SNDS)

Source : rapport annuel 2020 du Health Data Hub

C. COMME SI LA CRISE N'ÉTAIT QUE SANITAIRE

Tous les développements qui précèdent concernent la mobilisation du numérique par la France dans le domaine sanitaire. **Mais une crise telle que celle du Covid-19 n'est pas seulement sanitaire : c'est une crise tout court, une crise « totale »**, une épidémie dont les implications dépassent largement le domaine habituel de la santé publique, et qui **appelle par conséquent à des mesures bien plus larges**.

De fait, des mesures ont été prises : un soutien massif à l'économie touchée de plein fouet, un basculement de nombreuses activités en télétravail, et surtout **des restrictions d'ampleur inédite en temps de paix aux libertés fondamentales, qu'il s'agisse de la liberté d'aller et venir, d'entreprendre ou de voyager** – sans parler de leurs conséquences sur des libertés plus « intimes » telles que celle de voir ses proches, de les enterrer le cas échéant, de faire la fête, de se cultiver ou de pratiquer un rite religieux.

Or, dans ce domaine, nulle trace ou presque d'une volonté de recourir aux outils numériques, qu'il s'agisse d'assurer le bon respect de ces restrictions, ou mieux encore, de leur substituer des modalités plus fines de gestion de l'épidémie, grâce à l'intervention au niveau individuel que permettent les nouvelles technologies.

Il n'en a, tout simplement, jamais été question en France[1]. Au prix, sans doute, de nombreux morts et d'un confinement qui n'est toujours pas entièrement levé à l'heure où sont écrites ces lignes.

1. Des restrictions générales, un contrôle dérisoire

Si les restrictions édictées par les pouvoirs publics sont aussi dures et pénibles à supporter (confinement généralisé, couvre-feu, etc.), c'est parce que **leur modèle même intègre le fait qu'elles ne seront pas entièrement respectées**. Pendant les deux mois du premier confinement (17 mars-11 mai 2020), près de 1,1 million de contraventions ont été dressées : le chiffre peut paraître important, mais il **représente en réalité une fraction tout à fait dérisoire des infractions**, c'est-à-dire du nombre de fois où quelqu'un, quelque part en France, est sorti de chez lui pour aller voir des amis, a retiré son masque dans la rue, s'est éloigné de plus d'un kilomètre de son domicile, etc. Il n'est évidemment **ni possible, ni souhaitable, de contrôler chacun des faits et gestes de la population**.

Ces sanctions ne visent donc pas à empêcher 100 % des infractions, mais à dissuader suffisamment la population de les commettre pour atteindre l'objectif recherché, en l'occurrence la diminution des interactions sociales. **Ainsi, la sanction doit être d'autant plus forte (ici 135 euros) que la « chance » de se faire prendre est faible**. D'un point de vue économique, cette logique se prête à une analyse en termes de coût d'opportunité et de bilan coût-bénéfice[2]. Concrètement, c'est entre autres le principe du contrôle fiscal ou du contrôle routier « à l'ancienne » : les agents du fisc ne surveillent pas la comptabilité de toutes les entreprises, et les forces de l'ordre ne sont pas présentes sur tous les ronds-points. En revanche, si une infraction est constatée, la sanction doit être forte pour dissuader non seulement son auteur, mais aussi les autres, « pour l'exemple ». **Toutefois, dans le cadre d'une crise sanitaire, une telle logique atteint vite ses limites**, puisque qu'il s'agit ici de chaque petit geste de la vie quotidienne, dans laquelle l'État ne peut s'immiscer, et qui au cas par cas sont porteurs d'un risque faible qui n'incite pas à une vigilance constante (on ne transmet évidemment pas le virus à chaque fois qu'on retire son masque).

---

[1] *Les développements de cette partie concernent bien les outils permettant spécifiquement de freiner la propagation de l'épidémie, par des mesures relevant davantage de l'ordre public que de la sécurité sanitaire. Dans un sens plus large, le numérique a bien entendu constitué un recours en France comme dans la plupart des pays : télétravail, école à la maison, etc.*

[2] *En 1968, l'économiste Gary Becker a proposé un modèle micro-économique de « l'offre de crime », en vertu duquel la décision de commettre un crime résulte d'un arbitrage rationnel entre le gain attendu et le coût attendu (arrestation, amende, etc.). En termes de probabilités, toute hausse de l'amende correspond à une hausse du coût attendu et donc à une baisse du gain net espéré.*

Le numérique permettrait d'adopter une toute autre logique : au lieu de repérer une fraction dérisoire des infractions mais de les sanctionner très sévèrement, il serait théoriquement possible d'atteindre un taux de contrôle de 100 %, et d'alléger les règles en conséquence.

Bien entendu, les règles seraient entièrement différentes : il n'est pas question de demander à chacun de prendre un *selfie* toutes les cinq minutes pour s'assurer qu'il porte bien son masque ou qu'il éternue dans son coude. Dans un tel modèle, fondé sur le suivi exhaustif des règles sanitaires plutôt que sur des sanctions inversement corrélées à la probabilité d'être contrôlé, **les mesures ont vocation à être ciblées au niveau individuel et très limitées dans le temps**.

Par exemple, **les seules personnes diagnostiquées positives, soit 65 000 personnes actuellement (0,1 % de la population)**[1], pourraient être astreintes à des mesures sanitaires spécifiques (quarantaine), dont le respect serait contrôlé (géolocalisation, etc.) et le cas échéant fortement sanctionné. **Aucune restriction ne serait par contre imposée aux 99,9 % du reste de la population** : les déplacements seraient libres, les magasins seraient ouverts, les écoles et les musées aussi. **Les forces de l'ordre pourraient quant à elles être employées à des tâches plus utiles** que la surveillance du port du masque dans la rue et le contrôle aléatoire du respect du confinement et du couvre-feu. **Enfin, et surtout, la progression de l'épidémie serait arrêtée rapidement**.

Il s'agit bien sûr d'un modèle théorique : les choses sont bien plus complexes en réalité, notamment, dans l'exemple précédent, parce que le nombre de cas diagnostiqués ne correspond pas au nombre de cas réels. Mais ces limites ne remettent nullement en cause la pertinence du raisonnement ni son efficacité potentielle. **Or de telles mesures n'ont tout simplement jamais été envisagées dans le débat public, car elles font trop peur : nous avons préféré rester confinés « libres » et « égaux » pendant un an et demi**, et compter 100 000 morts sûrs de ne pas être espionnés dans leur cercueil.

2. Une sous-exploitation des données disponibles

a) Les données agrégées

Au-delà des données strictement médicales, **de nombreuses autres données auraient pu être utilement exploitées** dans le cadre de la gestion de l'épidémie, et pas seulement des données personnelles, loin s'en faut. **Or tel n'a pas été le cas, sinon de manière marginale, en ce qui concerne les autorités chargées de la gestion de la crise.**

---

[1] *Correspondant au taux d'incidence de 100 pour 100 000 habitants constaté fin mai 2021, soit le nombre de cas positifs pour 100 000 habitants sur une période d'une semaine. Au plus haut de l'épidémie – mais les mesures évoquées ici auraient précisément pour but de ne pas en arriver là –, ce taux d'incidence était de 501 pour 100 000 habitants, soit 335 000 personnes (0,5 % de la population).*

Dans le domaine de la **recherche scientifique**, et notamment de **l'épidémiologie**, les chercheurs ont su mobiliser de nombreux jeux de données pour leurs travaux, dans la mesure de ce que permettaient l'urgence, leurs propres moyens et les obstacles matériels ou juridiques restreignant la disponibilité des données. À titre d'exemple, on pourra citer **l'utilisation par l'INSERM des données de l'opérateur téléphonique Orange** pour analyser la mobilité des Français pendant le confinement[1] (cf. encadré), qui a permis de montrer que 17 % des habitants du Grand Paris avaient quitté la région entre le 13 et le 20 mars 2020, ou encore **les données d'analyse des eaux usées suivies par le réseau Obépine[2]**

Exemple de l'utilisation des données de l'opérateur Orange pour les travaux de modélisation épidémiologique de l'Inserm

Nouvelle analyse de la mobilité des Français au cours de la première semaine du confinement

Depuis fin octobre, la France est entrée dans un deuxième confinement afin de ralentir la circulation du virus et le nombre d'hospitalisations. Bien que plus légères que lors du confinement mis en place au printemps, ces mesures restrictives ont un impact sur la mobilité des personnes à différentes échelles spatiales et temporelles.

***Une équipe de recherche, coordonnée par les chercheurs Inserm Vittoria Colizza et Eugenio Valdano en collaboration avec l'opérateur téléphonique Orange**, s'est appuyé sur les **données des téléphones mobiles** pour analyser la mobilité de la population française au cours de la première semaine ouvrée du confinement actuel (du 2 au 6 novembre 2020). Ces données rendent compte pour chaque journée des déplacements sur **1 436 différentes zones géographiques réparties sur tout le territoire français et sont stratifiées en fonction de l'âge des personnes et de l'heure de la journée à laquelle intervient le déplacement**.*

*Dans un nouveau rapport, les chercheurs présentent donc une **analyse spatiale (mobilité nationale, régionale et locale), temporelle (par semaine, par jour, par heure) et par classe d'âge (jeunes, adultes, seniors)** des déplacements au cours de la première semaine du confinement. De plus, la mobilité est comparée avec celle enregistrée au cours de la première semaine de travail du premier confinement (23-27 mars 2020).*

[1] *Des initiatives similaires existent dans d'autres pays, par exemple en Allemagne avec le partenariat entre Deutsche Telekom et l'Institut Robert Koch. La Commission européenne a également lancé un projet en ce sens avec les principaux opérateurs européens.*

[2] *Les différents acteurs français de l'eau et de l'assainissement, dont Eau de Paris, réunis au sein du réseau OBEPINE (Observatoire EPIdémiologique daNs les Eaux usées), ont mis en place le suivi de 150 stations d'épuration représentatives et réparties sur le territoire national. Ce suivi permet d'évaluer le niveau de circulation du virus dans les populations. Cet indicateur, publié toutes les deux semaines, est pris en compte par les pouvoirs publics. Voir à ce sujet : http://eaudeparis.fr/nc/lespace-culture/actualites/actualite/news/sebastien-wurtzer-nous-participons-activement-a-la-recherche-sur-le-coronavirus/*

***Les données suggèrent que la mobilité a bien diminué depuis l'annonce de ce deuxième confinement**. En effet, elle est inférieure de 33 % par rapport aux niveaux de mobilités observés en 2020 avant que la pandémie ne prenne de l'ampleur. **Elle est toutefois plus importante que celle observée en mars, au début du premier confinement (elle atteignait alors – 67% des niveaux de mobilité pré-pandémique)** et est caractérisée par de fortes disparités régionales.*

*Cette moindre réduction est notamment expliquée par les **mesures de confinement moins restrictives**, notamment le maintien de l'ouverture des écoles et d'un plus grand nombre de secteurs d'activité.*

*Autre résultat d'intérêt : les chercheurs mesurent aussi **une forte association entre la réduction de la mobilité et les indicateurs socio-économiques, indiquant que les restrictions de mobilité sont les plus prononcées parmi les catégories de population les plus aisées**, confirmant les résultats déjà trouvés lors du premier confinement, apparus sur Lancet Digital Health.*

*Cette première analyse constitue **un outil supplémentaire pour évaluer l'impact des politiques publiques** actuelles mises en place dans le contexte de la crise sanitaire et pour éclairer les futurs ajustements possibles.*

Source : communiqué de presse de l'Inserm du 3 novembre 2020

De même, **les entreprises** ont, d'une manière générale, exploité au mieux les données dont elles disposaient pour faire face à la pandémie. On pourra notamment citer le cas des entreprises de **transport public**, qui ont ainsi pu adapter leurs moyens à l'évolution des flux de passagers. La même remarque vaut pour les **hôpitaux** et établissements de santé.

En revanche, si ces mêmes données ont fort heureusement contribué à éclairer la décision publique, **elles n'ont presque jamais été utilisées par les pouvoirs publics pour *intervenir* de façon ciblée pour assurer le suivi des restrictions sanitaires**.

Certes, utiliser ces données afin de contrôler au niveau *individuel* le respect des mesures aurait de fait posé un problème d'acceptabilité politique. **Mais pourquoi ne pas les avoir, au moins, utilisées au niveau agrégé ?** Par exemple, et sans présumer de la pertinence de ces mesures puisqu'elles n'ont pas été testées, peut-être aurait-il été possible d'utiliser **les données des antennes GSM pour repérer des attroupements ou des rassemblements trop importants**, permettant le cas échéant d'intervenir, sans pour autant lever l'anonymat des personnes. Il aurait aussi été possible d'exploiter les données – publiquement disponibles – de **fréquentation des commerces ou des transports**, pour ajuster les mesures.

De même, **une exploitation plus systématique et en temps réel des données des eaux usées aurait pu permettre d'identifier un *cluster* à l'échelle d'un quartier**[1], et ne confiner que celui-ci.

Pourquoi les autorités en charge de la gestion de la crise sanitaires n'ont-elles pas exploité ces données ? **Pour une part, elles n'ont pas voulu le faire** : ce n'est pas dans leur culture. Mais quand bien même elles l'auraient souhaité, **les administrations n'auraient de toute façon pas été en capacité de le faire**, ne disposant sur le moment ni des ressources humaines et matérielles, ni des procédures, ni de l'expérience nécessaires.

b) Les données individuelles

S'agissant de mesures plus ciblées, au niveau individuel, celles-ci n'auraient **pas nécessairement été très intrusives** : par exemple, **l'envoi automatique d'un SMS de rappel à toute personne s'éloignant de sa zone de quarantaine**, sans levée de l'anonymat ni transmission des données à qui que ce soit.

Techniquement, il n'existe aucun obstacle à un tel dispositif, que les opérateurs téléphoniques pourraient mettre en œuvre rapidement. Du reste, il existe déjà dans certains pays, et notamment aux États-Unis depuis 2002 avec le dispositif ***Amber Alert***, l'équivalent de l'*Alerte Enlèvement* française, qui prévoit non seulement la diffusion de messages sur les canaux publics (radio, télévision, panneaux routiers, gares, etc.) mais aussi **l'envoi automatique d'un SMS à toute personne se trouvant dans la zone de l'enlèvement**. Depuis plus de 10 ans, les messages sont aussi diffusés directement par ***Facebook***, ***Google*** **et** ***Bing*** **à toutes les personnes géolocalisés dans la zone**.

L'utilité d'un tel dispositif est évidente, non seulement dans le cadre d'une crise sanitaire, mais aussi **en cas de catastrophe naturelle ou industrielle, ou encore d'attaque terroriste**. C'est d'ailleurs l'objet même de la fonction *Safety Check* de Facebook (cf. *supra*).

3. La coûteuse absence de l'identité numérique

Au-delà du strict domaine médical et sanitaire, où l'identifiant numérique de santé (INS) aurait pu, comme on l'a vu, se révéler précieux, **c'est l'identité numérique en général qui aurait pu constituer un atout précieux pour la gestion de crise**, entre autres bénéfices qui dépassent le cadre du présent rapport (cf. encadré).

---

[1] *À plus long terme, on pourrait même imaginer la mise en place de spectromètres de masse pour mesurer les eaux usées à l'échelle d'un immeuble ou d'une école, ou la quantité de virus en circulation dans l'air d'une salle de concert. La technologie, courante en laboratoire, est toutefois loin d'être mature pour une telle application.*

Les enjeux de l'identité numérique

L'identité numérique est la clé de voûte de l'État-plateforme. Celle-ci permettrait à chacun d'accéder à l'ensemble des services publics au moyen d'un identifiant unique prouvant son identité de façon certaine et sécurisée. Elle ouvrirait la voie non seulement à l'allègement considérable des démarches de la vie quotidienne, mais aussi au développement d'une offre de services nouvelle, venant aussi bien de l'État que des collectivités locales et de la sphère sociale, mais aussi du secteur privé ou associatif.

En Estonie, par exemple, l'identité numérique est obligatoire pour tous les citoyens depuis 2007, et l'ensemble de leurs données – santé, fiscalité, justice, éducation, etc. – sont rattachées à un même identifiant. Elle possède la même valeur juridique que la carte d'identité physique, à laquelle elle est adossée, et qui est tout à la fois un titre d'identité, une carte d'électeur, un permis de conduire, une carte Vitale, un abonnement pour les transports, et peut servir à tout autre chose (piscine, bibliothèque, etc.). En **Allemagne**, le titre d'identité électronique est universel et obligatoire depuis 2010. En **Belgique**, l'identité numérique est déployée depuis 2004, et permet à tous les citoyens d'accéder à une large gamme de services publics nationaux et locaux.

Au total, **près de 70 pays dans le monde** ont mis en place un dispositif similaire.

Le problème est que la France, contrairement à d'autres pays, s'est toujours refusée à franchir le pas décisif : il n'existe pas, à ce jour, d'identité numérique appuyée sur un numéro unique d'identification. Du reste, il n'est même pas obligatoire d'avoir une carte d'identité, une « liberté » théorique qui laisse songeur quand on considère qu'elle est *de facto* nécessaire pour ouvrir un compte, s'inscrire à un concours, voyager, etc.

L'opposition de la CNIL à l'utilisation du NIR dans le domaine de la santé, récemment assouplie avec l'INS, vaut *a fortiori* – et vaut toujours – pour les autres domaines de l'action publique. **Par conséquent, toutes les autres administrations attribuent à leurs usagers des identifiants sectoriels spécifiques** : administration fiscale, enseignement primaire et secondaire, enseignement supérieur, police, justice, permis de conduire, etc., sans compter les innombrables identifiants locaux ou particuliers.

D'une façon générale, cette position, qui n'est pas sans justifications historiques (cf. *infra*), fait obstacle à la mise en place d'un État-plateforme. **S'agissant plus particulièrement de la gestion d'une crise sanitaire, cela interdit de recourir de façon simple à des outils numériques** qui pourraient, par exemple, permettre d'alléger les restrictions (aux voyages, aux déplacements, etc.) pour les personnes ne présentant aucun risque, ou offrir à chacun un service public adapté.

Pourtant, l'idée selon laquelle un numéro unique serait en soi une menace pour les libertés est loin d'être partagée au-delà de nos frontières. **Il s'agit bien d'une spécificité française**, et d'une construction essentiellement doctrinale, qui n'a pas valeur législative[1]. Tout à fait **compatible avec le règlement général sur la protection des données (RGPD)**[2], l'identité numérique est même **au cœur du règlement européen « eIDAS » de 2014**[3], qui établit un socle commun pour les transactions et interactions sécurisées. À ce jour, 18 États-membres ont déjà notifié la mise en place d'un dispositif d'identification présentant un niveau de sécurité « substantiel » ou « élevé ».

Dès 2007, dans une étude de législation comparée portant sur onze pays européens[4], le Sénat relevait que sept d'entre eux possédaient déjà un numéro unique d'identification, ou un numéro sectoriel utilisé comme tel. Les autres ont largement évolué depuis, à l'instar de l'Allemagne, dont la Cour constitutionnelle interdisait l'identifiant unique au nom des droits à la dignité et à la liberté, protégés par la Loi fondamentale… et qui a rendu le titre d'identité obligatoire et universel en 2010.

Les choses sont toutefois en train de changer. Lancé en 2014, le service ***France Connect*** permet déjà à ses 20 millions utilisateurs d'accéder à quelque 700 services en ligne – mais il ne s'agit que d'une étape intermédiaire, un fédérateur d'identités multiples, qui n'est pas en soi une identité numérique et qui n'implique aucune interconnexion des services eux-mêmes. Du reste, *France Connect* n'offre pas le niveau de sécurité « élevé » qui permettrait d'accéder aux services les plus sensibles (banque, e-santé, recommandé électronique, etc.).

Quant à **la nouvelle carte d'identité (eCNI)** déployée cette année, celle-ci offre un niveau de sécurité inédit, notamment grâce aux données biométriques. Elle pourrait être le support d'une future identité électronique, mais le Gouvernement s'est toujours refusé à sortir de l'ambigüité à ce sujet.

---

[1] *Aux termes de l'article 30 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les traitements de données personnelles utilisant le NIR sont subordonnés à un avis motivé et publié de la CNIL : la quasi-interdiction de l'utilisation du NIR au-delà de la sphère sociale est donc bien le fait de cette dernière, et non du législateur.*

[2] *Fondé sur le principe de responsabilisation* a priori *des acteurs, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) a conduit le législateur à supprimer la quasi-intégralité des formalités préalables d'autorisation ou de déclaration auprès de la CNIL. Toutefois, comme l'y autorise le RGPD, la France a fait le choix de maintenir le régime d'autorisation préalable pour les traitements comportant le NIR.*

[3] *Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.*

[4] *Étude de législation comparée n° 181, Le numéro unique d'identification des personnes physiques, décembre 2007.*

Reste encore à franchir le pas décisif, celui d'une identité numérique universel et obligatoire, qui aurait, comme en Estonie et dans d'autres pays, pu se révéler précieuse face à la crise.

4. Les collectivités locales dans la crise

Dans une période de crise qui appelle au pragmatisme, **un accès facilité à certaines données aurait permis aux collectivités locales**, qui ont été des acteurs de terrain importants, de remplir plus efficacement leur mission. Le cadre juridique en vigueur, pourtant, n'a pas facilité les choses.

S'agissant des données épidémiologiques, le rapport de la mission Bothorel sur l'*open data* relève ainsi que « ***l'enrichissement de l'information des collectivités territoriales sur l'évolution des données épidémiologiques concernant leur territoire constitue une demande forte afin d'adapter la réponse locale à la crise sanitaire****. À titre d'exemple, disposer de données épidémiologiques à une maille géographique plus fine que la commune, ou de données ventilées selon les caractéristiques sociodémographiques de la population permettrait d'apporter une réponse plus ciblée en matière de prévention, d'implantation des barnums, etc.* »

« *Plus globalement, cela pose la question de l'anonymisation des données et du risque de réidentification : sans aller jusqu'à la mise à disposition du public de ces indicateurs,* ***la question du partage des données entre Santé publique France et les collectivités territoriales pourrait être envisagée dans un souci d'efficience de l'action publique****. Ce partage de données pourrait se faire dans le cadre du Health Data Hub* ».

S'agissant de l'action au niveau individuel, les collectivités locales ont joué un rôle important auprès des personnes vulnérables : distribution de masques (sur rendez-vous, à domicile ou par voie postale), visites à domicile pour garder le lien social, information individuelle, etc. **Toutefois, les communes n'ont pas pu s'appuyer sur un fichier fiable et exhaustif des coordonnées de leurs administrés**, le législateur n'ayant pas créé de tel « fichier de population » au bénéfice de celles-ci, comme le rappelle la CNIL[1].

Certes, au cas particulier et compte tenu des circonstances, **la CNIL a fait preuve de souplesse et estimé que d'autres fichiers pouvaient être utilisés**, et notamment :

- le fichier de la taxe d'habitation, dont la finalité est en principe la seule gestion de la fiscalité locale ;

---

[1] *CNIL,* « COVID-19 : les traitements de données associés aux opérations de distribution de masques », *1er mai 2020, https://www.cnil.fr/fr/covid-19-les-traitements-de-donnees-associes-aux-operations-de-distribution-de-masques*

- le fichier de communication municipale, destiné à informer les administrés des événements de la vie locale, dont la situation sanitaire fait évidemment partie ;

- les registres d'information et d'alerte des populations constitués par les communes, soit à titre obligatoire dans le cadre du « **plan départemental d'alerte et d'urgence au profit des personnes âgées et handicapées en cas de risques exceptionnels** », qui vise par exemple les cas de canicule, soit au titre d'un « plan communal de sauvegarde », qui permet de constituer un registre plus large et général, mais où l'inscription est facultative ;

- les fichiers liés aux services municipaux (par exemple, le fichier des inscriptions scolaires pour informer sur les horaires adaptés de la cantine, etc.).

Il reste qu'il s'agit là d'outils partiels, incomplets, et qui n'ont pas été prévus pour cela. Par exemple, comme le remarquait Véronique Guillotin lors d'une audition publique organisée dans le cadre du présent rapport, « *sur les territoires, il a fallu recenser les patients de plus de 75 ans dans les différentes communes. Certaines d'entre elles ont utilisé des fichiers constitués sur demande active des plus de 75 ans : ils se sont annoncés eux-mêmes comme personnes fragiles afin que les mairies puissent leur envoyer des courriers.* ***Mais dans ce système, une partie de la population de plus de 75 ans a échappé à l'information sur la vaccination***[1] ».

Lors de la même audition, Jean-Raymond Hugonet a cité **l'exemple des tests salivaires conduits dans les écoles primaires** : « *j'ai assisté à un événement kafkaïen où étaient présents l'inspecteur de l'Éducation nationale, le directeur du laboratoire qui gère le territoire, les enseignants et les représentants de la commune. Le Logiciel Onde, géré par l'Éducation nationale, permet de disposer des renseignements sur l'ensemble des enfants scolarisés. Cependant, alors que les parents avaient été prévenus de ce test salivaire, nous étions dans l'impossibilité de faire basculer le fichier de l'Éducation nationale vers le laboratoire parce que le ministère était tétanisé* » à l'idée d'utiliser le numéro de Sécurité sociale[2].

Toutes ces questions ne se seraient tout simplement jamais posées s'il avait existé, avant la crise, un identifiant unique. Celui-ci aurait permis, face à l'urgence, de communiquer les bonnes données aux bons acteurs et au bon moment, de façon sécurisée et comprise par la population.

---

[1] *Audition de Gilles Babinet, co-président du Conseil national du numérique,* digital champion *de la France auprès de la Commission européenne, le 18 mars 2021.*

[2] *Les communes ne peuvent ni demander, ni conserver, ni utiliser le numéro de Sécurité sociale (NIR) des enfants en école primaire. Voir à cet égard : https://www.cnil.fr/fr/cnil-direct/question/numero-de-securite-sociale-nir-des-enfants-en-ecole-primaire-une-mairie-peut*

II. LE PRIX DES EXIGENCES CONTRADICTOIRES

Face à la crise provoquée par l'épidémie de Covid-19, **la France s'est donc retrouvée dans l'incapacité de tirer pleinement parti des possibilités ouvertes par le numérique**. Comme les développements qui précèdent l'ont montré, cette incapacité est **en partie d'ordre technique** : quand bien même aurions-nous souhaité faire un usage plus grand de ces technologies, **les systèmes n'étaient pas prêts**, que ce soit dans le domaine sanitaire *stricto sensu* (INS, DMP, ENS, etc.) ou de manière plus générale (pour que les restrictions soient mieux respectées, et qu'elles durent moins longtemps).

Mais en réalité, bien plus fondamentalement, ce sont des raisons politiques qui expliquent cette situation, des raisons tenant à la méfiance profonde et ancienne de la population à l'égard du numérique (A) et au conservatisme juridique des autorités en matière d'utilisation des données personnelles (B). Ces blocages expliquent d'ailleurs une grande partie des retards accumulés au fil des années par les grands projets dans le domaine de la e-santé ou de l'État plateforme en général : **l'impréparation technique de la France n'est que le résultat de ses tabous politiques et idéologiques**.

Or cette sensibilité française est non seulement devenue coûteuse, en particulier face à une crise sanitaire, mais aussi mal placée (C) :

- d'abord, parce que les atteintes éventuelles à nos libertés « numériques » ne doivent pas s'apprécier dans l'absolu mais **au regard des atteintes autrement plus importantes portées à nos libertés « physiques »**, dans une logique de proportionnalité aujourd'hui mal comprise ;

- ensuite, **parce qu'elle confond les *fins* (protéger les droits et libertés) et les *moyens* (interdire les croisements de fichiers)**.

Il faut être clair : pour la gestion d'une épidémie comme en général, **il n'y a pas – et il n'y aura jamais – d'outils numériques efficaces sans utilisation des données, y compris personnelles. Progresser dans cette voie est un devoir.**

En revanche, il est tout à fait possible d'assurer un haut niveau de protection des droits et libertés dans ce cadre – pour peu que soient levés les multiples fantasmes et les incompréhensions sur le sujet. La quasi-totalité des auditions réalisées dans le cadre du présent rapport sont allées dans ce sens, et ont insisté sur **l'effort considérable de pédagogie qui doit être entrepris pour gagner la confiance des citoyens**. Car, pour citer les propos prononcés lors de l'une des auditions, « *c'est bien la peur absurde de* Big Brother *qui nous a rendus incapables de tracer réellement les contacts et de suivre correctement les patients* ».

A. UNE DÉFIANCE DE L'OPINION AUX RACINES ANCIENNES

La sensibilité française sur le sujet est ancienne et profonde, et elle n'est pas dénuée de toute justification historique. On rappellera par exemple « l'affaire des fiches » – ou « affaire des casseroles »… – qui avait conduit à la chute du gouvernement d'Émile Combes en 1904, après la révélation d'une opération de fichage politiques et religieux dans l'armée française, dans le contexte des suites de l'affaire Dreyfus. On pourrait aussi évoquer, bien sûr, le régime de Vichy, la guerre d'Algérie ou encore l'URSS – sans même parler de la littérature ou du cinéma.

Dans l'imaginaire collectif, la collecte des données est associée à l'idée d'un État policier et d'un « fichage » de la population, et c'est cette même idée qu'on retrouve à chaque fois qu'un gouvernement s'aventure sur ce terrain, qu'il s'agisse fichier SAFARI (« *ou la chasse aux Français* », avait titré *Le Monde* en 1974), du fichier TES, du dossier médical partagé et maintenant de *TousAntiCovid*.

B. UN CONSERVATISME JURIDIQUE LOURD DE CONSÉQUENCES

1. La question du rôle de la CNIL

À la méfiance de l'opinion et des responsables politiques répond **un conservatisme juridique des autorités** chargées de la protection des données personnelles. **La question du rôle de la CNIL**, en particulier, est revenue constamment au fil des auditions conduites pour le présent rapport.

Précisons d'emblée qu'**il ne s'agit en aucun cas de reprocher à la CNIL de faire son travail, et encore moins de remettre en cause le cadre juridique fixé** par la loi Informatique et libertés de 1978[1] et le règlement général sur la protection des données (RGPD) de 2016[2], **dont les grands principes (cf. encadré) sont particulièrement nécessaires en période de crise sanitaire**. En effet, les traitements de données que celle-ci impose portent sur des données médicales, qui constituent des « données sensibles » au sens du RGPD, et bénéficient à ce titre d'une protection particulière. La CNIL a rendu un avis sur tous les décrets relatifs aux fichiers « Covid » (SI-DEP, VAC-SI, etc.), et ses observations ont été très largement suivies.

---

[1] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Son article 6 prévoit que les informations collectées doivent être adéquates, pertinentes et non excessives au regard de la finalité poursuivie.*

[2] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).*

Les 5 grands principes
de la protection des données personnelles

1) **Le principe de finalité** : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans **un but bien précis, légal et légitime** ;

2) **Le principe de proportionnalité** : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier. Ce principe de proportionnalité (*existe-t-il un moyen moins intrusif ?*) comprend notamment le **principe de nécessité** (*quelle utilité sanitaire ?*) et le **principe de minimisation** (*seules les données nécessaires à la gestion de la crise sanitaire doivent être collectées*) ;

3) **Le principe de durée de conservation limitée** : il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie, afin d'éviter tout détournement ultérieur de ses finalités. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier ;

4) **Le principe de sécurité et de confidentialité** : le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient, et veiller en particulier à ce que seules les personnes autorisées y aient accès ;

5) **Les droits des personnes**, en particulier le **droit d'accès** aux données les concernant et le **droit de rectification**.

Source : CNIL

En revanche, on peut légitimement s'interroger sur *l'interprétation* conservatrice que la CNIL fait de ces principes, en particulier du principe de proportionnalité, et surtout dans un contexte de crise, alors qu'il apparaît que des traitements de données **plus intrusifs pour les individus, mais aussi plus limités dans le temps**, auraient pu permettre de sauver des vies et d'alléger les restrictions imposées à la société dans son ensemble.

La remarque est d'autant plus valable que **d'autres pays européens**, soumis comme la France au RGPD, n'en font pas une interprétation aussi restrictive, et bénéficient ainsi d'outils numériques qui se révèlent précieux dans le contexte actuel – sans même parler des pays, asiatiques notamment, qui n'y sont pas soumis.

Les propos tenus par Gilles Babinet, co-président du Conseil national du numérique (CNNum), lors de son audition publique par la délégation à la prospective[1], font ainsi écho à de nombreuses remarques formulées lors des auditions des rapporteurs : « *enfin, je veux dire ici clairement que* ***la CNIL est sortie du cadre réglementaire qui s'impose à elle,***

[1] *Audition de Gilles Babinet, co-président du Conseil national du numérique,* digital champion *de la France auprès de la Commission européenne, le 18 mars 2021.*

et qu'elle est un facteur de retard pour notre pays. *Son contrôle parlementaire est insuffisant. Elle est une institution nécessaire, mais pas sous cette forme. Le problème n'est pas au niveau du collège mais au niveau de son personnel administratif, qui n'est pas contrôlé et qui prend systématiquement le parti du principe de précaution absolue* ».

S'agissant de la réponse à la crise sanitaire actuelle et à celles à venir, les **deux principaux exemples** du rôle problématique de la CNIL sont :

- d'une part, son opposition à l'identité numérique unique, et même à l'identifiant national de santé jusqu'à ce que la loi de 2019 vienne remettre en cause cette doctrine, déjà évoquée dans la partie précédente ;

- d'autre part, son opposition à toute solution *contact tracing* qui permette une identification, une localisation ou des recoupements avec d'autres données de santé, compromettant par là-même son efficacité, comme cela sera détaillé dans la partie suivante (au sujet de l'application *TousAntiCovid*).

S'agissant du « pass sanitaire », dans sa forme « domestique » pour accéder à certains lieux ou comme document de voyage international, le laboratoire d'innovation numérique de la CNIL (LINC), son service de d'études prospectives, s'est **très tôt montré réticent à l'égard de ce qu'il qualifie de « *totem à risques* » dans un article de mai 2020**[1]. Les avancées européennes en la matière, puis les récents arbitrages du Gouvernement, ont conduit le collège de la CNIL à adopter une position finalement différente, mais avec des réticences de principe qui demeurent entières.

Au-delà de ces exemples principaux, on peut notamment citer les autres sujets suivants :

- l'usage de la vidéo avec les caméras intelligentes et les drones ;

- l'accès aux données par les chercheurs en cette période de crise.

2. Des caméras trop « intelligentes » ?

L'utilité des caméras dites « intelligentes » dans le cadre de la lutte contre l'épidémie est apparue évidente dans de nombreux pays, y comprise européens : prise automatique de température par des caméras thermiques, détection du port du masque, mesure du respect de la distanciation ou du couvre-feu, etc. Ces dispositifs peuvent être mis en place sur la voie publique, mais aussi dans les lieux de travail ou commerces.

En France, pourtant, si la CNIL reconnaît que les objectifs assignés à ces dispositifs sont « *le plus souvent légitimes* », elle considère aussi et surtout que « ***leur développement incontrôlé présente le risque de généraliser un sentiment de surveillance chez les citoyens, de créer un phénomène***

[1] *Régis Chatelier,* « Le passeport d'immunité : un totem à risques », *LINC, 5 mai 2020, https://linc.cnil.fr/fr/passeport-dimmunite-un-totem-risques*

d'accoutumance et de banalisation de technologies intrusives, et d'engendrer une surveillance accrue, susceptible de porter atteinte au bon fonctionnement de notre société démocratique[1] ». Elle considère en fait que « *la captation de l'image des personnes dans ces espaces* » est, en elle-même, « *incontestablement porteuse de risques pour les droits et libertés fondamentaux de celles-ci*[2] ».

C'est à partir de cette **position de principe, qui est aussi une opposition de principe,** que la CNIL procède ensuite à l'analyse juridique des dispositifs de « caméras intelligentes » envisagés en France, au cas par cas, au regard notamment des principes de **nécessité** et de **proportionnalité**[3].

Un encadrement textuel adéquat est en effet requis dès lors que ces dispositifs **traitent de données sensibles**, en l'espèce biométriques (visage) et/ou relatives à l'état de santé (température corporelle), ou qu'ils **ne permettent pas toujours l'exercice effectif du droit d'opposition** (du fait du « balayage vidéo » par une caméra située dans la rue ou dans le métro, etc.). Or, d'une manière générale, la CNIL a estimé « *nécessaire d'alerter sur le fait que, sous réserve d'une analyse au cas par cas, il lui apparaît qu'**une grande partie de ces dispositifs ne respecte pas le cadre légal applicable à la protection des données personnelles***[4] ».

En pratique, la CNIL a donc considéré que **ni les circonstances (la crise sanitaire), ni les garanties apportées par les dispositifs eux-mêmes**, n'étaient suffisantes pour justifier leur emploi – alors que d'autres pays arrivaient à la conclusion inverse.

Par exemple, en mai 2020, **la RATP a expérimenté l'usage de caméras de détection du port du masque**, avec six caméras à la station Châtelet-Les Halles, avant d'y renoncer moins de deux mois plus tard, en raison de **l'opposition de la CNIL**, laquelle considérait que toute captation d'image constituait *par définition* un traitement de données biométriques et comportait *par définition* un risque d'identification.

Pourtant, les caméras en question ne conservaient strictement aucune image, et ne transmettaient que des statistiques agrégées de taux de port du masque, une fois toutes les 15 minutes. Le seul traitement de données, effectué localement (sur la caméra), consistait à comparer l'image prise avec une image témoin portant un masque – afin, concrètement, de

---

[1] Caméras dites « intelligentes » et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter, *17 juin 2020 : https://www.cnil.fr/fr/cameras-dites-intelligentes-et-cameras-thermiques-les-points-de-vigilance-de-la-cnil-et-les-regles.* Cette situation se retrouve dans la plupart des avis et publications de la CNIL au sujet de la crise sanitaire : points d'étape, rapport annuel, etc.

[2] La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques, *17 juin 2020 : https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras*

[3] *Contrairement à la vidéoprotection, qui fait l'objet d'un encadrement législatif spécifique, l'usage des caméras « intelligentes » n'est pas aujourd'hui prévu par un texte spécifique*

[4] La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques, *17 juin 2020 : https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras*

détecter ou non un « rectangle blanc », et de mesurer jour après jour l'évolution du port du masque dans les transports en commun. Aucun traitement biométrique n'a lieu en dehors de la caméra elle-même, et aucun algorithme de reconnaissance faciale n'est mise en œuvre, et **aucune identification des personnes, même indirecte, n'est possible**.

S'agissant de l'usage des caméras thermiques, largement répandu dans le monde pour détecter le Covid-19, la CNIL s'y est opposée au motif que la fièvre n'est pas un symptôme systématique de la maladie[1] : le dispositif présente ainsi « *le risque de ne pas repérer des personnes infectées puisque certaines sont asymptomatiques et qu'il peut, en outre, être contourné par la prise de médicaments antipyrétiques (qui réduisent la température corporelle sans traiter les causes de la fièvre)* ». **Ce qui revient à dire qu'il vaudrait mieux ne rien détecter plutôt que de détecter certains cas seulement**.

3. Les drones ou le floutage juridique

Les mêmes remarques s'appliquent à l'usage des drones équipés de caméras, auxquels les forces de l'ordre ont eu recours à plusieurs reprises, dès mars 2020, pour **contrôler le respect du confinement** : repérage de la présence de contrevenants potentiels sur la voie publique, diffusion de consignes par haut-parleurs, etc. Cet **usage des drones à des fins de police sanitaire** a notamment été mis en œuvre par la préfecture de Police, par le commissariat de Cergy-Pontoise, et par le groupement de gendarmerie départemental de Haute-Garonne.

Toutefois le 12 janvier 2021, à l'issue d'une procédure de contrôle initiée en mai 2020, **la CNIL a sanctionné le ministère de l'Intérieur pour avoir utilisé ces drones « *en dehors de tout cadre légal* »**, assortissant cette sanction d'une mesure de publicité et d'une injonction à cesser « *l'utilisation des drones **par l'ensemble des forces de l'ordre** dès lors qu'elles agissent sous l'autorité du ministère, qu'il s'agisse de services de police ou de gendarmerie, **sur l'ensemble du territoire, et quelles que soient les finalités** poursuivies* ».

Le raisonnement de la CNIL se fonde sur le fait que **le pilote du drone est susceptible d'identifier les personnes**[2] : « *en juillet 2020, la CNIL s'est rendue dans les locaux de la préfecture de police de Paris et a fait procéder à un vol d'essai d'un des drones utilisés pour les finalités précitées. À cette occasion, elle a **constaté que les personnes filmées par ce type de dispositif étaient susceptibles d'être identifiées*** ». Cette possibilité d'identifier les personnes entraîne la qualification de **traitement de données à caractère personnel** – lequel n'a donc, en l'espèce, pas été autorisé. *A fortiori*, il n'a pas fait l'objet d'une étude d'impact, et ne permet pas l'information du public.

---

[1] Caméras dites « intelligentes » et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter, *17 juin 2020.*

[2] *Avis du 12 janvier 2021 : https://www.cnil.fr/fr/drones-la-cnil-sanctionne-le-ministere-de-linterieur et https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042960768*

Toutefois, et sans entrer dans le détail d'un sujet qui excède largement le cadre du présent rapport, on pourra relever que :

- d'une part, la qualification de traitement de données à caractère personnel n'avait rien d'évident : depuis 2011, la jurisprudence constante du Conseil d'État réservait cette qualification aux dispositifs donnant à la fois lieu à enregistrement et conservation des images et à la possibilité d'identifier les personnes, ce qui n'était pas le cas des drones. Ce n'est que dans son référé du 18 mai 2020 que le Conseil d'État a considéré que l'usage de drones constituait, au cas d'espèce, un traitement de données à caractère personnel au sens du RGPD. Le juge des référés enjoignait dès lors l'État à « *cesser, sans délai, de procéder aux mesures de surveillance par drone, du respect, à Paris,* ***des règles de sécurité sanitaire*** », la seule possibilité de zoomer créant un risque de traiter des données personnelles, et donc une atteinte « *grave et manifestement illégale au droit au respect de la vie privée* », quand bien même aucune exploitation ne serait faite de ces données individuelles ;

- d'autre part, cette qualification juridique aboutit à une impasse opérationnelle, non seulement dans le cadre de la crise sanitaire, mais aussi pour *l'ensemble* des cas d'usage de drones par les forces de l'ordre. En effet, le juge des référés **avait ouvert la voie à la reprise des opérations par drone, assortie de mesures techniques (floutage des images)** permettant de ne plus qualifier ces opérations de traitements de données à caractère personnel. Toutefois, la CNIL, dont l'avis s'étend à un périmètre beaucoup plus large, a considéré que le mécanisme de floutage mis en œuvre à partir du mois d'août n'était **pas suffisant, car des images non floutées sont transmises par le drone à son pilote *en direct***, c'est-à-dire *avant* traitement par le logiciel de floutage, qui n'est pas installé sur la caméra du drone mais sur les équipements de la préfecture. **Il n'est pourtant pas possible d'aller au-delà, les règles de sûreté aérienne étant *par nature* incompatibles avec un floutage en direct**, qui remettrait en cause la maîtrise de son aéronef par le télépilote. Du reste, quand bien même des logiciels embarqués permettraient de réaliser un floutage dès la captation, ceux-ci nécessiteraient une puissance de calcul obligeant à équiper les drones de batteries bien plus volumineuses, entraînant de facto l'impossibilité de les utiliser en milieu urbain de façon sécurisée[1].

Résumons : **un raisonnement juridique, dont l'objectif ultime est d'empêcher qu'un pilote puisse fortuitement reconnaître une personne dans une foule, sans pour autant enregistrer la moindre image, conduit à interdire tout usage des drones par les forces de l'ordre**, alors qu'il s'agit d'une nécessité opérationnelle évidente que ni le juge ni l'administration ne contestent, et ceci **bien au-delà de la seule crise sanitaire** ou même du

[1] *Voir à cet égard le projet de réponse du ministère de l'Intérieur au rapporteur de la CNIL dans le cadre de la procédure de sanction. Ces éléments ont été publiés par* Mediapart *le 8 mai 2021 : https://www.mediapart.fr/journal/france/080521/drones-comment-gerald-darmanin-voulu-echapper-toute-sanction*

maintien de l'ordre[1]. En effet, pour rester dans le champ du présent rapport, les drones présentent un intérêt évident pour le **secours aux personnes** (par exemple pour intervenir rapidement en cas de catastrophe, localiser les victimes et réaliser une cartographie).

Le référé du Conseil d'État et la décision de la CNIL ont conduit le Gouvernement à privilégier **l'élaboration d'un cadre juridique général** pour l'emploi des drones par les forces de l'ordre, au sein du projet de loi pour une sécurité globale préservant les libertés. En dépit d'améliorations apportées par le Sénat, **le dispositif a toutefois été censuré par le Conseil constitutionnel**. Comme le constatent les rapporteurs du projet de loi[2], « ***le Conseil constitutionnel a de fait interdit l'usage des drones par les forces de sécurité intérieure*** *(article 47) pour plusieurs finalités légitimes et* ***laisse, pour le moment, entière la question du régime*** *permettant aux policiers, gendarmes et policiers municipaux mais aussi aux pompiers de recourir à ces équipements nécessaires* ».

4. L'autorisation des projets de recherche

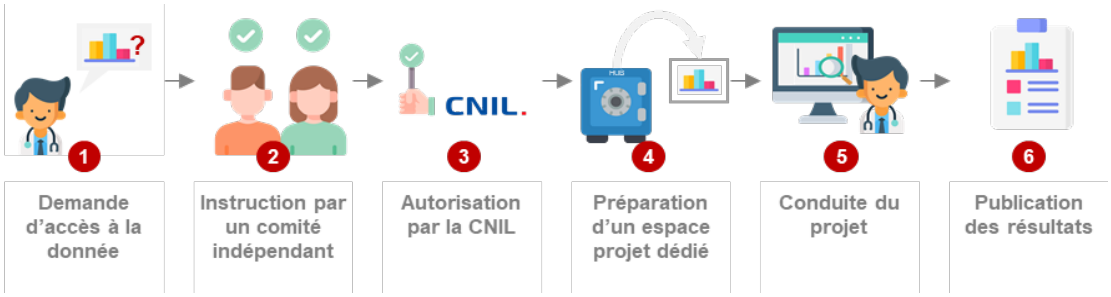
Dès le début de la crise sanitaire, de nombreux projets de recherche ont été lancés, non seulement dans le **domaine médical**, afin de mieux connaître le Covid-19, mais aussi dans le domaine des **sciences économiques et sociales**, afin par exemple de mesurer l'impact de la crise sur les inégalités ou d'évaluer le respect des mesures de distanciation ou de confinement. Ces travaux ont une importance fondamentale : ils permettent non seulement de faire **progresser la médecine**, mais aussi d'**éclairer la décision publique** et d'accroître la **confiance des citoyens** – qu'il s'agisse de justifier les restrictions et leur durée, ou d'organiser au mieux les campagnes de dépistage et de vaccination.

Or de nombreux projets dépendent de l'accès aux données à une maille relativement fine, le cas échéant individuelle, ce qui implique le traitement de données personnelles, y compris de nature médicale. L'accès aux données peut désormais se faire *via* le *Health Data Hub*, sous une forme pseudonymisée (cf. *supra*). **En matière de santé, tout projet de recherche doit auparavant faire l'objet d'une double autorisation**, par le Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES) d'abord, et par la CNIL ensuite, qui dispose de deux mois renouvelables pour répondre. La seule constitution des dossiers peut demander plusieurs mois aux chercheurs, et aucune procédure allégée n'est prévue pour le renouvellement d'un accès à la même base par un même chercheur.

---

[1] *Dans le cadre du maintien de l'ordre, les drones permettent en effet de faciliter la détection des mouvements de foule et de prévenir les incidents, de guider les effectifs pendant les interventions ou encore d'identifier les fauteurs de trouble. Ils peuvent également être utilisés dans le cadre de la sécurité routière.*

[2] *Communiqué de presse de François-Noël Buffet, président de la commission des lois, et de Marc-Philippe Daubresse et Loïc Hervé, rapporteurs, 20 mai 2021 :* https://www.senat.fr/presse/cp20210520b.html



Dans son point d'étape de novembre 2020, la CNIL indique s'être « *mobilisée pour instruire en priorité, dans des délais extrêmement courts, (…) parfois en quelques heures, (…) les demandes d'autorisation déposées (…) portant sur la Covid-19* ». **Tel ne semble pas être l'avis de la mission Bothorel**, dont le rapport évoque notamment le cas d'une chercheuse en sciences sociales qui avait formulé une demande d'accès aux données pseudonymisées de SI-VIC et SI-DEP *via* le *Health Data Hub* afin d'étudier le profil social des personnes infectées sur une zone géographique la plus fine possible. Six mois après sa demande, effectuée en avril 2020, son dossier était toujours en constitution auprès de la CNIL.

Il est toutefois délicat de tirer des conclusions générales d'un exemple individuel. Aussi se bornera-t-on à souligner que **la procédure d'autorisation, assez lourde, demeure de toute façon peu adaptée à une « recherche de crise »**. D'après la mission Bothorel, en novembre 2020, la CNIL avait autorisé 19 des 52 demandes relatives au Covid-19. Parmi les projets autorisés, seuls deux prévoient une utilisation du *Health Data Hub*, et ont été traités en respectivement 45 et 47 jours. Pour les autres, le délai moyen est de 20 jours, avec un maximum de 88 jours. **Les choses semblent toutefois s'être améliorées** : dans son rapport annuel publié le 18 mai 2021, la CNIL indique ainsi avoir accordé 89 autorisations de recherches sur le Covid-19, dont 45 % traitées en moins de deux jours et 63 % en moins d'une semaine.

À vrai dire, **s'agissant du *Health Data Hub*, la CNIL s'est surtout distinguée par son opposition au projet**[1], en raison du choix de Microsoft comme prestataire d'hébergement, faute d'une solution européenne, ce qui implique de potentiels transferts de données aux États-Unis et donc un accès direct par les autorités américaines. Si le Conseil d'État a finalement validé ce choix, la CNIL indique qu'elle « *restera vigilante* », compte tenu notamment de la décision « Schrems II » de la Cour de justice de l'Union européenne du 16 juillet 2020. Lors de son audition par la délégation à la prospective, Gilles Babinait déclarait : « *je rappelle que le choix de Microsoft comme prestataire est conforme à la loi. Le Conseil d'État a désavoué la CNIL sur ce point. (…) Le* Health Data Hub *a pris beaucoup de précautions sur les données confiées à ses algorithmes. (…) Je constate une instrumentalisation politique du sujet qui a surtout montré l'ignorance des personnes qui se sont engagées contre le* Health Data Hub. *J'ai défendu cet avis de façon très claire et je continuerai à le défendre* ».

[1] *Voir notamment son avis du 20 avril 2020.*

C. UNE SENSIBILITÉ COÛTEUSE ET MAL PLACÉE

Si la sensibilité française à toute collecte et croisement de données personnelles par les autorités peut se comprendre, au regard notamment de l'histoire, la crise sanitaire a aussi montré que cette sensibilité avait un prix élevé. **Mais surtout, cette sensibilité apparaît en réalité infondée, ou plus exactement décalée ou mal placée**, pour plusieurs raisons qu'il convient de détailler ici.

En effet, **ce n'est qu'en interrogeant les fondements mêmes de ce tabou qu'il sera possible de le dépasser**, pour s'attacher enfin à trouver d'autres solutions permettant à la fois de protéger la vie privée des citoyens et de bénéficier des avantages du numérique.

1. L'État et les GAFA, ou comment se tromper de *Big Brother*

Tout d'abord, cette sensibilité **apparaît de plus en plus décalée, pour ne pas dire complètement absurde, à l'heure où les géants du numérique** accumulent sur chacun d'entre nous davantage d'informations que l'État n'en aura jamais, à des fins qui n'ont rien à voir avec l'intérêt général, et sans aucune des garanties que procurent les mécanismes de contrôle démocratique, compte tenu notamment du « privilège » de l'extraterritorialité dont bénéficient les GAFA. Il existe **une disproportion manifeste** entre les obstacles imposés à l'État et aux institutions publiques en général – ici celles chargées de protéger notre santé – et les facilités qu'ont ces entreprises pour collecter et utiliser des données de manière autrement plus intrusive.

Le pire est que nous fournissons toutes ces données volontairement, en échange d'un peu de confort et d'une illusoire gratuité. Ironiquement, alors que les polémiques sur *TousAntiCovid* n'étaient pas encore éteintes, **Apple présentait le 23 avril dernier ses *AirTags***, des petites balises de la taille d'un porte-clés permettant, grâce au *Bluetooth* et en s'appuyant sur le milliard d'appareils de la marque en circulation dans le monde, de localiser tout objet auquel elles sont accrochées : un portefeuille, un sac à main, un vélo, un chien… et pourquoi pas un jeune enfant, un senior en perte d'autonomie, un conjoint infidèle, ou un employé pas assez modèle**. C'est exactement le même principe que pour la solution de *contact tracing*** proposée par Apple et Google, celle-là même que la France a fièrement refusée au profit de *TousAntiCovid* (cf. *infra*). Elle est même plus intrusive encore, car tout possesseur d'*iPhone* fait automatiquement partie du réseau de détection, sans possibilité de désactivation – et pourtant, on n'a pas entendu les mêmes cris d'orfraie. Il faut dire qu'avec les *AirTags*, au prix de 119 euros les quatre, la gravure d'un *emoji* personnalisé est offerte.

2. La mauvaise excuse des dictatures

L'un des arguments les plus fréquemment évoqués à l'encontre du recours au numérique dans la lutte contre le Covid-19 est **qu'il s'agirait de méthodes caractéristiques de régimes autoritaires et autres « dictatures numériques » que l'on trouve surtout en Asie**. Cet argument, à la subtilité douteuse, appelle deux réponses.

Premièrement, c'est faux : les pays qui se sont appuyés sur des outils numériques puissants, souvent très intrusifs et obligatoires, sont dans leur majorité **des pays démocratiques, avec des élections libres et un État de droit**. C'est le cas du Japon, de Taïwan (qui a connecté ses bases de données sanitaires avec celles de la police aux frontières) ou encore de la Corée du Sud (qui a institué un *contact tracing* obligatoire et utilisant la géolocalisation, croisant de multiples données non sanitaires et permettant d'identifier les individus). Sans être de « pures » démocraties à l'occidentale, Hong Kong et Singapour n'en sont pas pour autant des dictatures.

Ces pays ne sont d'ailleurs **pas seulement asiatiques** – citons par exemple **Israël ou l'Estonie**, sans compter les nombreux autres qui ont très tôt fait le choix d'un pass ou d'un passeport sanitaire, et que la France s'apprête à rejoindre. À l'inverse, **les régimes les plus autoritaires n'ont attendu ni la révolution numérique ni la crise sanitaire** pour s'en prendre aux droits et libertés de leurs citoyens.

Les risques de dérives, bien sûr, sont tout à fait réels – et ce n'est pas pour rien que les technologies numériques les plus intrusives, comme la géolocalisation ou la reconnaissance faciale, sont strictement encadrées. Dans un pays comme la **Chine, le système du « crédit social », la vidéosurveillance et l'usage des codes couleur en fonction de l'immunité** contribuent en effet à **une forme de surveillance généralisée**, comme l'a montré l'audition publique organisée sur le sujet[1] par la délégation à la prospective le 11 février 2021.

Mais ces dérives ne tiennent pas aux technologies elles-mêmes, elles tiennent à l'usage qui en est fait, à l'absence de contre-pouvoirs notamment, et aussi à des facteurs politiques et culturels. En lui-même, le progrès technique est neutre, porteur du pire comme du meilleur. Il n'est ni souhaitable, ni même possible, de l'entraver – et ce n'est certainement pas en laissant les régimes les moins démocratiques prendre une avance décisive en ce domaine, ou en abandonnant aux GAFA le soin de lutter contre les épidémies (et quoi d'autre demain ?), que nous pourrons défendre nos valeurs.

[1] *Audition de Mme Séverine Arsène, chercheuse associée au Médialab de Sciences Po et enseignante à l'Université chinoise de Hong Kong, sur le crédit social en Chine, 11 février 2021.*

Deuxièmement, tout ceci n'est pas le problème. Si une « dictature » sauve des vies pendant qu'une « démocratie » pleure ses morts, la bonne attitude n'est pas de se réfugier dans des positions de principe, mais de **s'interroger sur les moyens concrets, à la fois techniques et juridiques, de concilier efficacité et respect de nos valeurs**.

Or tout est affaire de proportionnalité : a-t-on les mêmes « valeurs absolues », universelles et non négociables, quand il s'agit de sauver 1 000 vies ou 100 000 vies ? Ou, face à une menace plus grave, un million, voire dix millions ? Nos « lignes rouges » ont déjà beaucoup évolué en un an.

3. Une étrange conception de la proportionnalité

Le cœur du problème est en effet la proportionnalité. **Le principe lui-même ne fait pas débat**, et le RGPD prévoit d'ailleurs la possibilité de mettre en œuvre des traitements de données personnelles **intrusifs et dérogatoires, y compris au regard du consentement explicite des individus**, lorsque les circonstances le justifient – ce qui est typiquement le cas d'une crise sanitaire. Dans son point d'étape de novembre 2020, la CNIL précise ainsi que sa mission a consisté à « ***concilier la protection des données à caractère personnel et des libertés, dont elle est garante, et la protection de la santé qui sont toutes deux des objectifs à valeur constitutionnelle*** ».

C'est bien le placement du curseur qui pose problème, c'est-à-dire le sens des priorités. Dans le contexte de la crise, la priorité absolue[1] donnée à la protection des *individus* contre *toute* mesure susceptible de compromettre leur anonymat ou de déboucher sur une quelconque « obligation » ou « discrimination » est problématique à deux égards :

- d'une part, en raison du rapport entre bénéfices *individuels* et risques *collectifs* ;

- d'autre part, en raison de la disproportion entre atteinte aux libertés « numériques » et atteinte aux libertés « physiques ».

S'agissant du premier point, rappelons que la spécificité d'une crise sanitaire est d'**impliquer des externalités (positives ou négatives) liées aux comportements individuels** : les atteintes à la vie privée d'un *individu* ne sont donc pas seulement justifiées par la nécessité de le protéger lui-même, mais par la nécessité de **protéger *l'ensemble de la société***, compte tenu du risque de contamination. Or la propagation d'une épidémie est par définition exponentielle dès lors que le taux de reproduction (R0) est supérieur à 1. Par conséquent, **l'impact d'un comportement individuel peut être considérable**, ce qui justifie des mesures obligatoires et intrusives, quitte à ce qu'elles soient limitées dans le temps et assorties de fortes garanties.

---

[1] *Au-delà de la doctrine de la CNIL, cette priorité, quoique déjà entamée en pratique, est toujours au centre du discours du Gouvernement. Ce discours n'est d'ailleurs pas propre à la France : la remarque vaut pour la plupart des pays occidentaux.*

Du reste, il existe déjà – et fort heureusement – des maladies à déclaration obligatoire, sans que personne ne s'en scandalise. Outre les exigences relatives aux voyages internationaux, déjà évoquées, il existe en France une liste de 34 maladies à déclaration obligatoire (MDO)[1] :

1. Botulisme
2. Brucellose
3. Charbon
4. Chikungunya
5. Choléra
6. Dengue
7. Diphtérie
8. Fièvres hémorragiques africaines
9. Fièvre jaune
10. Fièvre typhoïde et fièvres paratyphoïdes
11. Hépatite aiguë A
12. ***Infection aiguë symptomatique par le virus de l'hépatite B***
13. ***Infection par le VIH quel qu'en soit le stade***
14. Infection invasive à méningocoque
15. Légionellose
16. Listériose
17. ***Mésothéliomes***
18. Orthopoxviroses dont la variole
19. Paludisme autochtone
20. Paludisme d'importation dans les départements d'outre-mer
21. Peste
22. Poliomyélite
23. Rage
24. Rougeole
25. Rubéole
26. Saturnisme chez les enfants mineurs
27. Schistosomiase (bilharziose) urogénitale autochtone
28. Suspicion de maladie de Creutzfeldt-Jakob et autres encéphalopathies subaiguës spongiformes transmissibles humaines
29. ***Tétanos***
30. Toxi-infection alimentaire collective
31. Tuberculose (incluant la surveillance des résultats issus de traitement)
32. Tularémie
33. Typhus exanthématique
34. Zika

S'agissant du second point, il faut rappeler que « *la réflexion sur les libertés "numériques" doit aussi être conduite au regard des restrictions extrêmement importantes qui ont été portées aux libertés "physiques", et notamment à la liberté d'aller et venir* ». La citation provient de la CNIL elle-même, dans son point d'étape de novembre 2020 : là encore, ce n'est pas le principe qui est en cause, mais son application. Il est vrai que, six mois après le point d'étape, les restrictions ne sont toujours pas levées, et la France compte désormais plus de 100 000 décès.

C'est tout le paradoxe de la situation : les restrictions « physiques » **sont bien plus lourdes, durent bien plus longtemps, et s'appliquent à tous de manière « aveugle »**. Elles sont aussi **bien plus difficiles à faire respecter**, et sans doute *in fine* **bien moins efficaces –** quoique la France n'ait jamais eu l'occasion de les comparer avec des mesures « numériques ».

---

[1] *Cette liste est fixée par décret du ministre chargé de la Santé, après avis de Santé Publique France. Actuellement, 30 MDO relèvent de la catégorie 1 : elles nécessitent une intervention urgente locale, nationale ou internationale, et une surveillance pour la conduite et l'évaluation des politiques publiques. Seules 4 MDO, signalées en* ***gras italique****, relèvent de la catégorie 2 : pour celles-ci, seule une surveillance est nécessaire.*

À cet égard, l'appréciation par la CNIL du principe de nécessité (*quelle utilité sanitaire de la mesure ?*) interroge. Tout d'abord, celle-ci n'a pas de compétence médicale – c'est sans doute un problème, mais il serait injuste de lui en faire le reproche, car telle n'est pas sa vocation, et la remarque vaudrait tout aussi bien, par exemple, pour le juge administratif.

En revanche, sur le strict plan du **raisonnement juridique**, il est plus légitime de s'interroger. S'agissant par exemple des **caméras thermiques** (cf. *supra*), la CNIL développe un raisonnement pour le moins curieux : « *l'efficacité et l'opportunité* » de la prise de température seraient contestables parce que celle-ci n'est pas un symptôme systématique du Covid-19, et parce que la consommation de produits antipyrétiques (aspirine, etc.) permet de faire baisser la fièvre sans pour autant en traiter les causes, ce qui limite les possibilités de détection dans certains cas[1]. **En d'autres termes, la CNIL préfère ne détecter personne plutôt que de risquer de ne pas détecter tout le monde…**

Cette position de principe est certes louable sur le plan de l'égalité mais bien peu adaptée à un contexte de crise sanitaire, où tout cas identifié est une victoire sur la maladie. La crise a livré plusieurs autres exemples de cette approche, par exemple lorsque la CNIL a émis des réserves au sujet d'un « passeport vaccinal », au motif qu'il n'existe « *aucune certitude concernant la capacité des vaccins commercialisés actuellement à rendre 100 % des vaccinés sans danger pour autrui* ». Faudrait-il, pour autant, se priver de leur efficacité *importante* pour permettre la réouverture des frontières et des commerces ?

4. Le totem de la discrimination

Ce type de raisonnement montre une chose : derrière la sensibilité française à la protection des données personnelles se trouvent non seulement un attachement à la *liberté* individuelle (par la protection de la vie privée), qui est la mission de la CNIL et s'accommode somme toute assez bien du principe de proportionnalité, mais aussi à ***l'égalité* entre les citoyens**.

Plus précisément, **la doctrine de la CNIL semble opposée à toute mesure conduisant à une « *discrimination en raison de l'état de santé* »**, expression apparue plusieurs fois au cours de la crise, et chargée d'un poids symbolique important.

Mais, dans la lutte contre une épidémie, **l'objectif des mesures est *très précisément* de discriminer les individus en fonction de leur état de santé**, pour leur propre protection et celle de la collectivité, et **soutenir le contraire n'a strictement aucun sens**.

---

[1] Caméras dites « intelligentes » et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter, *17 juin 2020*, *https://www.cnil.fr/fr/cameras-dites-intelligentes-et-cameras-thermiques-les-points-de-vigilance-de-la-cnil-et-les-regles*

Le refus par principe de toute « discrimination », par la seule magie du mot, ne contribue pas à la sérénité des débats sur des mesures telles que le pass ou le passeport sanitaire, pourtant indispensables.

Plusieurs intellectuels en ont aussi appelé à **Michel Foucault et à ses concepts de biopouvoir ou de biopolitique**[1], **qui suffisent à discréditer *ab initio*** toute mesure impliquant une contrainte imposée sur les corps des individus, dont font partie le confinement, hériter des quarantaines, ou les applications conditionnant l'accès à certains lieux.

Un autre exemple est la tribune[2] publiée le 13 avril 2020 dans le *New York Times* par Kathryn Olivarius, professeure d'histoire à Stanford, intitulée « **La dangereuse histoire de l'immunoprivilège** ». À propos de l'épidémie de fièvre jaune qui toucha le Sud esclavagiste des États-Unis au 19e siècle, causant quelque 150 000 morts, elle souligne que les discriminations liées à l'état de santé venaient aggraver les discriminations existantes fondées sur l'origine ethnique : les « *Blancs acclimatés* », c'est-à-dire immunisés[3], se situaient au-dessus des « *Blancs étrangers non-acclimatés* », eux-mêmes situés au-dessus des autres catégories ethniques, et notamment des Noirs. **Faudrait-il, en suivant ce raisonnement, refuser toutes les mesures sanitaires fondées sur l'immunité (et donc la contagiosité) des personnes**, au motif qu'elles ont, par le passé et dans un tout autre contexte, été associées à des discriminations raciales ?

Ces débats n'ont pas eu lieu en France. Toutefois, ils rappellent que de mauvaises raisons peuvent parfois conduire à refuser de bonnes mesures, ce qui n'est pas étranger aux polémiques nationales.

5. Une préférence pour l'inefficacité

Enfin, la défiance historique de la société française à l'égard de la collecte des données personnelles, dont la doctrine actuelle de la CNIL est le reflet, tient à **une confusion, rarement formulée en tant que telle, entre les *fins* (protéger les droits et libertés) et les *moyens* (interdire les croisements de fichiers)**.

---

[1] *Sur le concept de biopouvoir, voir notamment Michel Foucault,* Histoire de la sexualité, *1976. Sur le concept de biopolitique, voir notamment Michel Foucault,* Surveiller et punir, *1975.*

[2] https://www.nytimes.com/2020/04/12/opinion/coronavirus-immunity-passports.html.
Kathryn Olivarius est l'auteure de l'ouvrage à paraître Necropolis: Disease, Power, and Capitalism in the Cotton Kingdom. *Cette tribune est citée par le LINC dans son article du 5 mai 2020 sur le passeport d'immunité :* https://linc.cnil.fr/fr/passeport-dimmunite-un-totem-risques

[3] *Notamment par la pratique des* chickenpox parties, *où les Blancs aisés étaient incités à se contaminer volontairement pour atteindre l'immunité de groupe. Au 20e siècle, sur le même principe, les* pox parties *(fêtes de la varicelle) réunissaient des enfants afin de les contaminer et de développer leurs défenses immunitaires.*

Il est vrai que dans les années 1970, au moment du débat sur le fichier SAFARI qui allait donner naissance à la CNIL, **l'interdiction du croisement des fichiers apparaissait légitimement comme le moyen le plus évident de prévenir les atteintes à la vie privée**, dans un contexte où de tels croisements évoquaient essentiellement les dérives des services de police et de renseignement. La Seconde guerre mondiale était un souvenir récent, la guerre d'Algérie plus encore, et l'URSS n'offrait guère un modèle enviable à ce titre. **Dans le même temps, les immenses bénéfices résultant de tels croisements ne pouvaient être imaginés**.

Il en va bien différemment aujourd'hui : à l'heure de la révolution numérique, du *big data* et de l'intelligence artificielle, on ne peut plus raisonnablement soutenir que l'intérêt principal des croisements de fichiers est la surveillance policière, ou l'instauration d'un État totalitaire fantasmé. Fort heureusement, les applications reposant sur l'exploitation des données se sont aujourd'hui généralisées dans le secteur privé, allant des domaines les plus importants (dont la recherche médicale) aux plus triviaux – qui ne sont pas les moins lucratifs.

Pourtant, dès lors qu'il s'agit de l'État ou du secteur public, la méfiance demeure : en somme, **tout se passe comme si la meilleure garantie possible pour nos droits et libertés était de maintenir l'inefficacité de l'administration**, quel qu'en soit le prix en termes de qualité du service public, et en l'occurrence de vies humaines. Si la crise sanitaire doit servir de révélateur, ce problème est bien plus général, et concerne la « réforme de l'État » et la « transformation du service public » dans leur ensemble. Les obstacles à l'utilisation du NIR ou à la mise en place de l'identité numérique en sont d'excellents exemples.

La persistance de ce blocage est d'autant moins compréhensible qu'**il existe aujourd'hui des solutions techniques permettant de garantir un très haut niveau de confidentialité et de sécurité**, sans pour autant renoncer aux bénéfices ouverts par le numérique. Il est donc impératif que le débat public dépasse les oppositions de principe et les arguments binaires (pour ou contre le croisement), pour **s'intéresser aux solutions techniques**.

Naturellement, passer des principes à la technique **demandera un effort pédagogique immense**. Ce devoir incombe d'abord aux responsables politiques qui, notamment faute de disposer d'une culture technique dans ce domaine, optent souvent pour le *statu quo*.

Il faut, en particulier, **insister sur le fait qu'un croisement de données ne pose pas *en soi* un problème de « sécurité »**, même s'il peut le cas échéant poser un problème pour la protection de la vie privée. La protection de la vie privée, mission de la CNIL, et la cybersécurité, mission de l'ANSSI, sont en effet deux choses différentes. **Il est donc impératif que celle-ci se dote de capacités d'analyse technique en matière de cybersécurité**, et non pas seulement de capacités d'analyse juridique, en

travaillant notamment davantage avec l'ANSSI. C'est tout le sens des recommandations n° 14 et n° 15 du rapport de la mission Bothorel, qui proposent, de façon certes moins frontale :

- de prévoir **au sein du collège de la CNIL deux personnalités qualifiées compétentes, l'une en matière de sécurité des systèmes d'information** et l'autre sur les nouveaux usages de la donnée ;

- d'ouvrir la **possibilité pour la CNIL de saisir l'ANSSI** pour avis en cas de doute sérieux en matière de sécurité des systèmes d'information.

Quelles sont ces solutions techniques permettant de garantir la sécurité et la confidentialité des traitements de données personnelles ? Sans entrer ici dans le détail, on peut citer les deux exemples suivants :

- l**a *blockchain*** : cette technologie de validation décentralisée permet tracer tous les accès et modifications aux données, sans qu'aucune autorité – étatique ou autre – ne puisse les falsifier. L'Estonie l'a introduite au cœur de la X-Road dès 2011. Ainsi, chaque citoyen a non seulement accès immédiatement à l'intégralité de ses données, mais aussi au nom de tous les fonctionnaires qui y ont accédé, avec la date et l'heure, et une fonctionnalité native permet de porter plainte en cas d'utilisation suspecte, avec de forte sanctions – de sorte que les abus sont presque inexistants ;

- l'***open source*** : rendre publics les algorithmes de l'administration est la meilleure façon de protéger les citoyens contre le mésusage de leurs données. C'est par exemple le cas du **protocole ROBERT**, sur lequel est construite l'application *TousAntiCovid*, et qui garantit un très haut niveau de protection.

Ce très haut niveau de protection, pourtant, n'a pas empêché l'échec de *TousAntiCovid*. Au contraire, le choix du Gouvernement de porter son discours sur la protection absolue de l'anonymat a sans doute aggravé les choses et conduit à de mauvaises décisions. ***TousAntiCovid* apparaît ainsi comme un cas d'école des contradictions françaises**, et une illustration des développements qui précèdent.

III. L'ÉCHEC DE TOUSANTICOVID : UN CAS D'ÉCOLE

À partir de l'été 2020, et comme de nombreux pays dans le monde (cf. *supra*), **la France a décidé d'utiliser une application de *contact tracing*** pour briser les chaînes de contamination, suivant en cela l'avis du Conseil scientifique du 20 avril, qui estimait cette solution « *indispensable* » en complément du dispositif humain des « brigades de traçage » (cf. *supra*).

Pourtant, le bilan de l'application *StopCovid*, lancée le 2 juin 2020 et devenue *TousAntiCovid* le 22 octobre suivant, apparaît très décevant non seulement en comparaison des applications similaires utilisées ailleurs, mais aussi en général – toutes ces applications ayant *in fine* montré une efficacité très limitée en comparaison des dispositifs plus intrusifs utilisés notamment en Asie.

Comment expliquer cet échec ? À vrai dire, ***TousAntiCovid* illustre parfaitement les contradictions françaises à l'égard du numérique**, dans le contexte de la crise sanitaire et au-delà : **en refusant de trancher entre efficacité et confidentialité, la France a finalement perdu sur les deux tableaux**, s'infligeant de longs mois d'intenses polémiques pour développer finalement un outil certes très sécurisé, mais aussi très peu utilisé, et dont l'impact sur la progression de l'épidémie est plus que douteux.

***TousAntiCovid* rappelle que l'enfer est pavé de bonnes intentions** : les spécificités de l'application ont été justifiées par le « respect des valeurs européennes », mais elles relevaient aussi de choix techniques discutables et perturbés par de mauvaises considérations politiques.

Ces remarques concernent la **fonctionnalité initiale** de l'application, le *contact tracing*. Ses **fonctionnalités ultérieures** (passeport et pass sanitaires notamment), distinctes, ouvrent des perspectives plus encourageantes – mais n'échappent pas à la répétition des polémiques.

A. LE CONTACT TRACING *À LA FRANÇAISE*

1. Une genèse douloureuse

Il est vrai que l'idée même d'une application de *contact tracing* s'est, d'emblée, **heurtée à la sensibilité de l'opinion** sur le sujet des données personnelles. Sans surprise, **la CNIL n'a pas non plus fait preuve d'un enthousiasme excessif**, prévenant fin avril 2020 que « *l'utilisation d'une application sur la base du volontariat ne devrait pas conditionner ni la possibilité de se déplacer, dans le cadre de la levée du confinement, ni l'accès à certains services, tels que par exemple les transports en commun* », et précisant que le volontariat signifiait « *qu'aucune conséquence négative* » ne serait attachée à l'absence de téléchargement ou d'utilisation de l'application.

Compte tenu de la sensibilité du sujet, on ne peut que **saluer l'effort de pédagogie du secrétaire d'État chargé de la transition numérique, Cédric O**. Dans un texte très argumenté publié le 3 mai 2020[1], il explique ainsi que « *l'architecture du système est pensée de telle manière que* ***personne, pas même l'État, n'ait accès ni à la liste des personnes contaminées ni au "graphe" des interactions sociales*** *("qui a rencontré qui ?"). L'application ne demande absolument aucune donnée personnelle à l'utilisateur : ni le nom, ni l'adresse, ni même le numéro de téléphone mobile. C'est bien simple, elle ne demande rien à part le consentement de l'utilisateur de l'utiliser* ». **De fait, la priorité absolue a été accordée, dès le départ et au-dessus de toute autre considération, à la préservation de l'anonymat des utilisateurs, notamment face à « l'État ».**

Bruno Sportisse, président-directeur général d'Inria[2], explique cela dans les mêmes termes : « *une telle application n'est* ***pas une application de surveillance : elle est totalement anonyme****. Pour être encore plus clair : sa conception permet que PERSONNE, pas même l'État, n'ait accès à la liste des personnes diagnostiquées positives ou à la liste des interactions sociales entre les personnes. La seule information qui m'est notifiée est que mon* smartphone *s'est trouvé dans les jours précédents à proximité du* smartphone *d'au moins une personne qui a, depuis, été testée positive et s'est déclarée dans l'application.*

« *Une telle application* ***n'est pas une application de délation*** *: dans le cas où je suis notifié, je ne sais pas qui est à l'origine de la notification. Lorsque c'est moi qui me déclare positif, je ne sais pas qui est notifié.*

« *Une telle application* ***n'est pas obligatoire****. Ses utilisateurs choisissent de l'installer. Ils choisissent d'activer le* bluetooth*. Ils peuvent, à tout moment, désactiver le* bluetooth *ou désinstaller l'application* ».

D'emblée, le Gouvernement a donc écarté toutes les propositions consistant à conditionner certaines activités à l'utilisation de *StopCovid*, alors même que le Conseil scientifique l'envisageait expressément, et que d'autres pays en avaient décidé ainsi.

Par exemple, dans une lettre ouverte adressée le 25 mai au secrétaire d'État chargé du numérique, le député de la majorité Damien Pichereau avait par exemple estimé qu'il serait « *judicieux de coupler l'utilisation de l'application* StopCovid *à* ***une contrepartie****, comme par exemple une légère baisse des restrictions en cette période de sortie du confinement (on peut notamment penser à une augmentation du périmètre de déplacement de 100km à 150km). Cet allègement* ***permettrait sans aucun doute d'inciter un plus grand nombre de nos concitoyens à télécharger l'application****, renforçant ainsi notre capacité à retracer les chaînes de contamination* ». Cette idée, dont l'esprit n'est pas si éloigné des récents arbitrages, avait été immédiatement rejetée.

---

[1] https://cedric-o.medium.com/stopcovid-ou-encore-b5794d99bb12

[2] *Dans une présentation détaillée, quoique très accessible aux non-spécialistes, du fonctionnement de l'application, publiée sur le site d'Inria le 18 avril 2020 :* https://www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux

2. Le choix isolé du protocole « centralisé » ROBERT

Au nom de la préservation absolue de l'anonymat, **la France a fait un choix technique qui la distingue des autres pays : celui du protocole ROBERT** (*ROBust and privacy-presERving proximity Tracing*), développé par l'Inria et l'Institut allemand Fraunhofer. Il est lui-même dérivé du **protocole PEPP-PT**[1], issu de recherches menées par des équipes allemandes, italiennes et suisses.

Pour simplifier, le principe du protocole ROBERT est le suivant :

- lorsque l'application est activée par l'utilisateur, **son *smartphone* reçoit un crypto-identifiant éphémère** généré par un algorithme, qui change toutes les 15 minutes ;

- le *smartphone* collecte les crypto-identifiants des *smartphones* restés « à proximité » pendant une certaine durée (initialement fixée à 15 minutes) et sur lesquels l'application est également activée ;

- si l'utilisateur est diagnostiqué positif et qu'il le signale dans l'application, et seulement dans ce cas, celle-ci **fait remonter au serveur central *l'intégralité* des crypto-identifiants, y compris les siens, dans un paquet global, de sorte qu'il est impossible pour le serveur de savoir lequel de ces identifiants correspond à un cas positif, et encore moins d'établir un lien entre un identifiant et un individu** ;

- tous les identifiants ainsi remontés vers le serveur font l'objet d'une **évaluation du niveau de risque au regard, notamment, des données relatives à la durée d'exposition**. Cette évaluation se fait en fonction des modèles épidémiologiques, le cas échéant être améliorés par des modèles d'apprentissage automatique ;

- par ailleurs, chaque *smartphone* interroge à intervalle régulier le serveur pour vérifier si son crypto-identifiant figure dans la liste des identifiants à risque. Si tel est le cas, **l'utilisateur reçoit une notification l'informant qu'il est « cas contact », sans qu'il puisse en aucune façon faire le lien avec une autre personne**. La notification est le cas échéant accompagnée d'une invitation à s'isoler, à effectuer un test, etc. – ces éléments relevant de la politique de santé publique.

Un autre exemple d'architecture « centralisée » est le protocole *BlueTrace*, développé par Singapour pour son application *TraceTogether* disponible depuis le 20 mars 2020, et adopté ensuite par l'Australie (*CovidSafe*) et Hong Kong (*LeaveHomeSafe*).

[1] Pan-European Privacy-Preserving Proximity Tracing *(PEPP-PT)*

3. Le succès de l'architecture « décentralisée » proposée par Apple et Google

À cette architecture « centralisée », où le travail d'identification des risques est effectué par un serveur unique, peut s'opposer **une architecture « décentralisée », où ce sont les crypto-identifiants des personnes positives qui sont envoyés par le serveur vers les *smartphone*s, au sein desquels la mise en correspondance est effectuée**. Le serveur, quant à lui, n'a jamais accès à l'historique des contacts, à la différence du protocole ROBERT.

C'est notamment le choix retenu par Apple et Google, qui ont développé conjointement *Exposure Notification*, une solution de *contact tracing* compatible avec leurs systèmes d'exploitation respectifs, basée sur le protocole DP-3T, lui aussi issu de recherches européennes[1]. Présentée le 10 avril 2020, *Exposure Notification* **n'est pas une application, mais seulement une interface de programmation (API)**, c'est-à-dire un « kit » de fonctionnalités prédéfinies à destination des développeurs, qui peuvent ensuite les intégrer librement dans les différentes applications nationales.

Du fait de sa simplicité, de son interopérabilité et de sa sécurité, **la solution d'Apple et Google a très vite été adoptée par la majorité des pays du monde**.

Au sein de l'Union européenne, seules la France et la Hongrie font exception. **L'Allemagne**, qui avait initialement soutenu le protocole PEPP-PT, a finalement annoncé rejoindre *Exposure Notification* le 26 avril, suivie de peu par l'Irlande et l'Italie, laissant la France isolée. Le **Royaume-Uni**, autre soutien initial, a fait de même. Le 25 mai, la Suisse devenait le premier pays au monde à lancer une application basée sur la solution d'Apple et Google.

Il convient ici de préciser qu'en réalité, **les solutions « centralisée » comme « décentralisée » offrent toutes les deux un très haut niveau de sécurité et de confidentialité[2]** : ni le protocole ROBERT, ni le protocole DP-3T et sa déclinaison par Apple et Google ne permettent d'établir un lien entre un crypto-identifiant et un individu. Tous les protocoles sont **publiés en *open source*** et librement accessibles à quiconque souhaite les examiner ou les améliorer[3].

---

[1] Decentralized Privacy-Preserving Proximity Tracing *(DP-3T)*.

[2] *En réalité, les termes de « centralisation » et de « décentralisation », simplificateurs et marqués idéologiquement, n'ont pas contribué à la sérénité du débat. L'architecture dite « décentralisée » peut tout aussi bien être vue comme une « centralisation locale » des identifiants à risque. Comme l'indique Bruno Sportisse, tous les projets comportent une composante centrale (un serveur) et une composante décentralisée (les* smartphone*s). Il n'existe pas de solution entièrement décentralisée fondée sur une seule communication de « pair-à-pair » entre les* smartphone*s, qui présenterait des risques incomparablement plus élevés pour la confidentialité des données.*

[3] *Comme le veulent les standards du secteur, les publications scientifiques et le code-source sont disponibles sur* Github *:* https://github.com/ROBERT-proximity-tracing *pour ROBERT et* https://github.com/google/exposure-notifications-server *pour* Exposure Notification*. Dans ce*

Du reste, il n'existe en matière de sécurité informatique aucune solution parfaite, et au niveau mondial, **la sécurité du protocole centralisé PEPP-PT a globalement fait face à davantage de critiques**[1] de la part de la communauté scientifique que celle du protocole décentralisé DP-3T.

4. Un choix lourd de conséquences : la désactivation du *Bluetooth* et l'absence d'interopérabilité

En réalité, le problème du choix isolé de la France n'est pas tant une question de *sécurité* qu'une question d'*efficacité*.

À cet égard, il semble que le refus du Gouvernement d'utiliser la solution d'Apple et Google ait **d'abord été dicté des considérations d'ordre politique** – afficher une solution « souveraine » à tout prix –, **et non par des arguments techniques liés à la confidentialité des données, qui tiennent en l'occurrence du prétexte**.

Or, par son refus, la France s'est privée des avantages cruciaux qu'offrait le protocole décentralisé, condamnant *StopCovid* à l'inefficacité avant même sa sortie. Les risques étaient pourtant bien identifiés au sein de l'écosystème numérique[2], et l'arbitrage du Gouvernement s'est fait à l'issue d'un débat houleux en interne, conduisant notamment à écarter la direction interministérielle du numérique (DINUM) de la gouvernance du projet[3].

Le refus d'adopter la solution décentralisée est problématique pour deux raisons principales.

D'une part, ce choix empêche l'application de fonctionner en tâche de fond sur les *iPhones*, soit la majorité du temps, car Apple restreint l'accès des applications tierces à la puce *Bluetooth* des terminaux sous *iOS*, afin de protéger la vie privée de ses utilisateurs, ainsi que la capacité de la batterie. ***StopCovid* puis *TousAntiCovid* fonctionnent donc uniquement lorsque l'application est ouverte au premier plan par l'utilisateur, ce qui les condamne en pratique à l'inefficacité.** Le problème est moindre pour les *smartphone*s fonctionnant sous *Android*, qui autorise un accès plus large aux paramètres *Bluetooth*, sans pour autant être total[4]. **À l'inverse, la solution développée par Apple et Google fonctionne avec le *Bluetooth* en arrière-plan, c'est-à-dire en permanence**, sauf si l'utilisateur l'a désactivé.

---

dernier cas, il s'agit d'un exemple d'application basée sur l'API – le code-source relatif aux systèmes d'exploitation n'étant en toute logique pas entièrement accessible.

[1] *En particulier sur l'ampleur des « remontées » d'identifiants, l'application du seuil minimal d'exposition annoncé de 15 minutes, d'ailleurs variable, se faisant sur le serveur.*

[2] *Voir par exemple : https://www.numerama.com/tech/619446-stopcovid-vs-apple-pourquoi-la-france-sest-mise-dans-une-impasse.html*

[3] *Voir à ce sujet : https://www.acteurspublics.fr/evenement/recours-aux-gafam-centralisation-les-choix-techniques-sur-stopcovid-ont-attise-les-tensions-au-sein-de-letat*

[4] *La nécessité de contourner les restrictions sous* Android *explique notamment le retard de près d'un mois pour le déploiement de* StopCovid*, annoncé pour le 11 mai et finalement lancé le 2 juin.*

Face à ce blocage, la France avait décidé de porter le sujet à un niveau politique, en annonçant qu'elle conditionnerait le déploiement de *StopCovid* à l'obtention d'une dérogation spéciale de la part d'Apple pour l'accès à la puce *Bluetooth*, espérant que l'entreprise n'oserait pas s'opposer à une telle demande faite au nom de la protection de la santé de la population. **Mais Apple n'avait aucune raison de céder, et ne l'a pas fait**. En effet, une telle décision aurait créé un précédent, que d'autres États auraient ensuite pu invoquer, dans le cadre de la lutte contre le Covid-19 ou pour toute autre raison plus ou moins légitime – or, rappelons-le, Apple n'a pas même cédé aux pressions du FBI, sur son propre territoire, pour des faits de terrorisme[1]. Pour Apple, **la fermeture de son système d'exploitation constitue en effet la meilleure manière de protéger la vie privée de ses utilisateurs**, un argument d'autant plus recevable en l'espèce que l'entreprise proposait, avec Google, une solution sécurisée permettant d'atteindre les mêmes objectifs.

Ce n'est pas la moindre des contradictions françaises : quoique sécurisé, **le protocole ROBERT suppose en effet de faire confiance à un acteur unique, « l'État »** – celui-là même auquel nous sommes si réticents à transmettre la moindre information par ailleurs.

D'autre part, le choix français d'un protocole « souverain » interdit toute interopérabilité avec les applications des autres pays, alors que la gestion d'une pandémie requiert par définition un effort coordonné à l'échelle internationale. **Toutes les autres applications européennes sont compatibles entre elles** : une personne voyageant dans un autre pays n'aura pas à télécharger une nouvelle application, et l'identification des chaînes de contamination ne sera pas entravée. À l'inverse, **un voyageur ou frontalier arrivant en France devra télécharger *TousAntiCovid***… qui, s'il veut bien s'en donner la peine, ne sera de toute façon d'aucun secours s'il arrive déjà porteur du virus, ou s'il rentre dans son pays après avoir été contaminé.

Tout ceci est *a minima* **une importante occasion manquée** : que les infrastructures informatiques des différents systèmes de santé ne soient pas compatibles entre elles est un fait contre lequel on ne peut pas grand-chose à court terme, en revanche, les *smartphone*s sont les mêmes partout, et ne pas en avoir tiré profit est un choix difficilement justifiable.

---

[1] *Suite à la fusillade de San Bernardino (Californie) en décembre 2015, Apple avait refusé le déblocage des deux iPhone du terroriste, qui avait fait quatorze victimes, en dépit du bras de fer engagé par le FBI et le procureur général des États-Unis. Voir à cet égard le message de Tim Cook, PDG d'Apple, le 16 février 2016 : https://www.apple.com/customer-letter/*

B. TOUT ÇA POUR (PRESQUE) RIEN ?

1. Une adoption insuffisante

Le discours politique du Gouvernement, insistant plus que tout sur la préservation de la confidentialité, a-t-il, au moins, permis de gagner la confiance des citoyens ? **Il est possible, au contraire, que cette stratégie ait contribué à accroître encore davantage la défiance**. En tout cas, un mois après son lancement, *StopCovid* n'avait été téléchargée que **1,7 million de fois, soit environ 2 % de la population française**… Environ la moitié des téléchargements avaient eu lieu les deux premiers jours. Par comparaison, l'application allemande *Corona Warn App* avait été téléchargée 6 millions de fois en seulement 30 heures.

Reconnaissant l'utilité « *relative* » d'un outil aussi peu téléchargé, le secrétaire d'État chargé du Numérique a annoncé **la transformation de *StopCovid* en *TousAntiCovid*.** Lancée le 22 octobre 2020, cette version plus est plus interactive et comprend des fonctionnalités supplémentaires, qui ont été progressivement enrichies :

- des informations générales, notamment sur les gestes barrière ;

- des statistiques sur l'épidémie au niveau national, affinées par la suite au niveau local ;

- la possibilité de télécharger l'attestation préremplie pour le confinement et le couvre-feu ;

- une carte des centres de dépistage et de vaccination.

Si, d'un point de vue technique, la transformation de *StopCovid* en *TousAntiCovid* ne change strictement rien – les faiblesses sont les mêmes, qu'il s'agisse du *Bluetooth* ou de l'absence d'interopérabilité –, cet épisode livre toutefois des enseignements importants, déjà évoqués plus haut **: la qualité de « l'expérience utilisateur » (ergonomie, fonctionnalités, etc.) et la réponse à la demande d'informations des citoyens constituent de puissants leviers de mobilisation**, qu'il convient de ne pas ignorer.

De fait, le lancement de *TousAntiCovid* a permis de rattraper une partie du retard et, au 20 avril, l'application avait été téléchargée 15 millions de fois. Ce chiffre, qui correspond à environ un Français sur cinq, demeure toutefois **inférieur à ce que l'on constate dans de nombreux pays européens**, par exemple l'Allemagne (31 % de la population) ou le Royaume-Uni (31 % également).

Surtout, ce chiffre est en lui-même peu significatif : il inclut en effet les – nombreuses – **mises à jour successives**, et ne signifie donc pas qu'un Français sur cinq a téléchargé l'application. Il ne signifie pas non plus, *a fortiori*, que ces personnes utilisent *effectivement* l'application, puisque celle-ci doit être activée, et le *Bluetooth* également. Enfin, ce chiffre est

susceptible d'être faussé par l'ajoute des nouvelles fonctionnalités à l'application, qui peuvent conduire à une hausse des téléchargements, sans que les utilisateurs aient pour autant l'intention d'activer le *contact tracing*.

2. Une efficacité douteuse

Reste la question principale : **cette application a-t-elle été utile ? À ce jour, on peut considérer que non, ou presque.**

Il convient ici de distinguer entre :

- **d'une part, ce qui relève spécifiquement des choix de la France ;**

- d'autre part, ce qui est inhérent à toutes les applications de ***contact tracing***.

a) Un problème français

S'agissant du premier point, **la comparaison avec l'application *NHS Covid-19 App* utilisée au Royaume-Uni** permet de mesurer, en creux, l'échec de *TousAntiCovid*.

Comparaison des applications de *contact tracing* française et britannique

TousAntiCovid **(France – Protocole ROBERT)**	**NHS Covid-19 App** **(Royaume-Uni – API Apple/Google)**
15 millions de téléchargements, soit **22** % de la population.	**21 millions** de téléchargements, soit **31** % de la population.
172 000 de notifications* : **1,1** % des utilisateurs ont été avertis.	**1,7 million** de notifications : **8** % des utilisateurs ont été avertis.
Aucune étude d'impact.	**600 000 infections évitées** +1 % d'utilisateurs → -2,6 % des contaminations

** Le nombre de notifications envoyées en France était de 194 000 au 20 mai 2021.*
Sources : TousAntiCovid (fin avril 2021) et Institut Alan Turing (fin janvier 2021).

Trois enseignements peuvent être tirés de cette comparaison.

Premièrement, et sans surprise, **l'efficacité d'une telle application est directement corrélée à son degré d'adoption par la population**, du fait de l'effet de réseau. Or **l'adoption a été bien plus massive au Royaume-Uni** qu'en France, et également bien plus précoce.

En outre, activer l'application ne suffit pas : **encore faut-il que les personnes positives au Covid-19 jouent le jeu.** Or, début mars 2021, seuls 175 000 utilisateurs s'étaient déclarés dans *TousAntiCovid*, **soit à peine 4,5** %

des quelque 3,9 millions de cas recensés à ce moment-là[1]. Dans ces conditions, **il n'est guère étonnant que le nombre de personnes averties *via* l'application soit si peu élevé** (1,1 % de la population, contre 8 % au Royaume-Uni). Tous ces éléments font dire à Aymeril Hoang, ancien directeur de cabinet du secrétaire d'État chargé du numérique, Mounir Mahjoubi, au moment de son développement, que « ***StopCovid est une application aveugle, peut-être la plus aveugle qui ait jamais existé***[2] ».

Deuxièmement, **le choix du protocole ROBERT a sans doute joué un rôle**, en rendant l'application inutile pour les utilisateurs d'*iPhone* (25 % du parc) et en la privant des bénéfices de l'interopérabilité. **L'application britannique, quant à elle, est fondée sur le protocole d'Apple et Google**. À vrai dire, les chercheurs d'Inria, qui ont développé le protocole ROBERT, avaient depuis l'origine fait preuve de nuance dans la défense de celui-ci, en insistant bien sur le fait qu'aucune solution ne l'emportait nettement sur l'autre. C'est sans doute ainsi qu'il faut comprendre la réponse de Bruno Sportisse, PDG d'Inria, à la question posée par René-Paul Savary dans le cadre de la commission d'enquête sénatoriale sur la gestion de la crise sanitaire[3] : « *Mon seul regret est de ne pas avoir réussi à instaurer un dialogue serein, qui aurait permis à la société de* ***sortir de la naïveté et des fantasmes sur le numérique****. Notre responsabilité d'institut de recherche sera à l'avenir de porter des actions majeures en ce sens* ».

Troisièmement, l'application britannique a fait l'objet d'une étude scientifique visant à évaluer son efficacité à partir de modèles statistiques, publiée par l'Institut Alan Turing[4]. Elle estime que **600 000 contaminations ont pu être évitées grâce à l'application**. Plus précisément, elle estime qu'une hausse de 1 % du nombre d'utilisateurs correspond à une baisse de 2,3 % des contaminations. Quelles que soient les limites méthodologiques

---

[1] *D'après les chiffres cités dans les médias, ces quelque 175 000 auto-déclarations correspondent à 100 000 notifications envoyées aux cas contacts : on voit ici les limites du modèle épidémiologique sous-jacent, avec bien moins d'un cas contact averti par déclaration enregistrée. Or en principe, le déclarant fait lui-même partie des destinataires, puisque le protocole ROBERT ne fait pas la différence entre les différents crypto-identifiants du « paquet ». Cela signifie donc que, dans la grande majorité des cas,* TousAntiCovid *n'envoie aucune notification aux personnes à risque. Voir par exemple : https://www.bfmtv.com/tech/depuis-son-lancement-l-application-tous-anti-covid-a-alerte-100-000-cas-contacts_AN-202103100026.html*

[2] *Cité par* Le Monde *du 21 mai 2021 : https://www.lemonde.fr/pixels/article/2021/05/21/covid-19-l-impossible-mesure-de-l-utilite-des-applications-de-tracage-des-cas-contacts_6080953_4408996.html*

[3] *Commission d'enquête pour l'évaluation des politiques publiques face aux grandes pandémies à la lumière de la crise sanitaire de la covid-19 et de sa gestion, table ronde sur les aspects numériques, 22 septembre 2020 : https://www.senat.fr/compte-rendu-commissions/20200921/covid.html*

[4] *Mark Briers, Chris Holmes et Christophe Fraser, «* Demonstrating the impact of the NHS COVID-19 App – Statistical analysis from researchers supporting the development of the NHS COVID-19 App *», 9 février 2021, https://www.turing.ac.uk/blog/demonstrating-impact-nhs-covid-19-app. L'étude a été soumise à validation par les pairs et n'a pas encore fait l'objet d'une publication formelle.*

d'une telle étude[1], il semble donc bien que **l'application britannique ait eu un effet tangible**, conduisant les chercheurs à conclure : « *utilisez l'application – ça marche* ».

Déplorant l'absence d'une telle étude en France prouvant « *l'impact effectif de ce dispositif dans la lutte contre l'épidémie* », la CNIL a beau jeu d'appeler, dans sa délibération du 10 septembre 2020[2], à son « *évaluation indispensable et urgente au regard notamment des risques inhérents à ces traitements pour les droits et libertés des personnes* ». On pourra relever le paradoxe qu'il y a à déplorer l'inefficacité d'une solution dont les limitations s'expliquent, précisément, par la volonté de se conformer strictement à la doctrine de la CNIL…

De fait, l'étude d'impact de l'Institut Alan Turing a été rendue possible parce que **les chercheurs britanniques sont les seuls à avoir eu accès aux résultats des tests**, enregistrés dans l'application et associés à un lieu de résidence, ce qui permet ensuite de les exploiter dans un modèle épidémiologique. Les autres pays dont l'application enregistre ces données n'y ont pas donné accès aux chercheurs, et l'application française ne permet tout simplement pas de les enregistrer. Pourtant, **il serait théoriquement possible de contourner, quoique partiellement, cette difficulté** : avec ses nouvelles fonctionnalités, TousAntiCovid transmet aux « autorités de santé » des « *statistiques liées à l'identifiant de l'application (nombre d'attestations, nombre de preuves de test, saisie du code postal pour le lieu d'intérêt, etc.)* » ainsi que des statistiques sur « *le niveau de risque de l'utilisateur, date de dernier contact, date de test, date de premier symptôme* », comme l'indique l'analyse d'impact sur les données personnelles (AIPD) du 21 avril (non publique)[3].

Au final, pourquoi toutes ces difficultés ? D'après Aymeril Hoang, « *nous devions verrouiller politiquement le sujet de manière conforme à l'idée qu'on se fait des valeurs européennes en termes de protection des données personnelles* ». Avec une conséquence inévitable : « ***les indicateurs d'efficacité et d'épidémiologie ont été écartés, ce qui a complètement tué le dispositif*** ». Simon Cauchemez, épidémiologiste à l'Institut Pasteur, va dans le même sens : « *on s'est orienté vers une réponse très sûre mais avec très peu de recueils de données, ce qui fait qu'ensuite, il devient plus compliqué d'évaluer et de bien calibrer l'outil* ».

---

[1] *Celle-ci fait notamment l'hypothèse qu'une personne ayant reçu une notification qui se fait ensuite tester le fait pour cette raison, ce qui revient à exclure les autres motifs : apparition de symptômes, enquêtes manuelles, obligation liée à un voyage ou à un déplacement professionnel, etc.*

[2] *Considérants n° 40 et n° 41.*

[3] *On relèvera incidemment le paradoxe : d'immenses efforts ont été faits pour limiter la collecte de données par le volet* contact tracing *de l'application, alors que les mêmes données, et d'autres, sont nécessairement collectées par son volet* pass sanitaire*…*

b) Un problème mondial

Toutefois, au-delà des spécificités françaises, **c'est bien l'efficacité des applications de *contact tracing* en en général qui pose question**. Comme évoqué plus haut, cette technologie est soumise à des limitations intrinsèques, tenant à la **capacité du *Bluetooth***, à l'absence de prise en compte de **l'environnement** et de **l'état de santé des personnes**, et enfin à l'incertitude des **modèles épidémiologiques**.

D'ailleurs, la relativement large adoption de la *NHS Covid-19 App* **n'a pas empêché le Royaume-Uni d'être le pays le plus endeuillé d'Europe**, avec 128 000 morts à ce jour. Quant à l'application *TraceTogether*, pourtant obligatoire et déployée très tôt, elle **n'a pas permis à Singapour d'échapper à un confinement particulièrement strict**. À elle seule, cette technologie ne constitue en aucun cas une réponse miracle à la pandémie.

Une enquête menée par plusieurs grands médias européens[1], portant sur 23 applications de *contact tracing*, est récemment venue confirmer l'efficacité plus que douteuse de ces solutions, dès lors que leur utilisation reste facultative et que leurs données ne sont pas croisées avec d'autres, au nom de la préservation de l'anonymat.

On y apprend que, dans le pays concernés, **22 % de la population a téléchargé ces applications** (soit 90 millions de personnes), une proportion comparable à celle de la France, mais insuffisante pour garantir une véritable efficacité. Surtout, on y apprend que **les résultats des tests positifs signalés dans les applications représentent seulement 4,7 % des cas détectés dans la même période** (soit 1,1 million de cas) : comme en France, la population ne joue généralement pas le jeu… alors même qu'il serait **techniquement très simple d'atteindre un taux de signalement de 100 % en interconnectant les fichiers** (équivalents à SI-DEP), pour une efficacité incomparablement plus élevée de l'application.

Ces deux chiffres sont les seuls à être publiés par l'ensemble des gouvernements : **ce manque de transparence** ne suggère rien de très positif quant à l'efficacité réelle de ces applications, et explique la quasi-absence d'études d'impact. **Seuls trois pays publient une estimation du nombre de personnes utilisant *réellement* l'application** après l'avoir téléchargée : la Suisse, le Portugal et l'Irlande – cette dernière comptant 1,3 million d'utilisateurs actifs pour 2,5 millions de téléchargements. Appliqué à la

---

[1] *Simon Auffret (*Le Monde*) avec Dorien Vanmeldert et Tim Verheyden (*VRT, *Belgique), Markus Sehl (*Die Zeit, *Allemagne), Manon Dillen et Daan Marselis (*The Investigative Desk, *Pays-Bas). Cette enquête a été réalisée par quatre médias européens, dont Le Monde, dans le cadre de l'opération* « Spooky Mayfly ». *Coordonné par* The Investigative Desk *aux Pays-Bas, ce projet a pour but d'interroger les conséquences des nouvelles technologies déployées en Europe pour lutter contre le Covid-19. Ses conclusions ont été publiées dans* Le Monde *du 21 mai 2021 : https://www.lemonde.fr/pixels/article/2021/05/21/covid-19-l-impossible-mesure-de-l-utilite-des-applications-de-tracage-des-cas-contacts_6080953_4408996.html*

France, ce ratio correspondrait à 7,8 millions d'utilisateurs actifs, soit 11 % de la population et la moitié des personnes ayant téléchargé l'application – mais la réalité est sans doute bien en deçà.

Quant à la mesure de l'efficacité de ces applications, celle-ci est à peu près impossible, puisqu'il n'existe aucun moyen de savoir si une personne alertée a effectivement suivi la recommandation de s'isoler, ou est allée se faire tester – ce que des recoupements avec les fichiers de tests permettraient là encore très facilement.

En fait, c'est donc fondamentalement le choix fait par l'ensemble des pays occidentaux de s'appuyer sur une solution facultative, préservant l'anonymat et ne recourant pas à la géolocalisation qui est en cause.

Quelles qu'en soient les modalités précises, le *contact tracing* reste fondamentalement une solution peu efficace au regard des possibilités ouvertes par des technologies plus intrusives.

IV. LE PASS SANITAIRE : ENFIN UNE BONNE NOUVELLE ?

A. L'OUTIL PRINCIPAL DE LA SORTIE DE CRISE

Le 25 mai, l'Assemblée nationale a définitivement adopté le projet de loi relatif à la gestion de la sortie de crise sanitaire, dont l'article 1er contient **la base législative nécessaire à la mise en œuvre du « pass sanitaire »**, *via* la possibilité donnée au Premier ministre de **subordonner l'accès à certains lieux, établissements ou événements** impliquant de grands rassemblements de personnes, pour certaines activités, à la présentation :

- **d'un résultat de dépistage négatif** ;

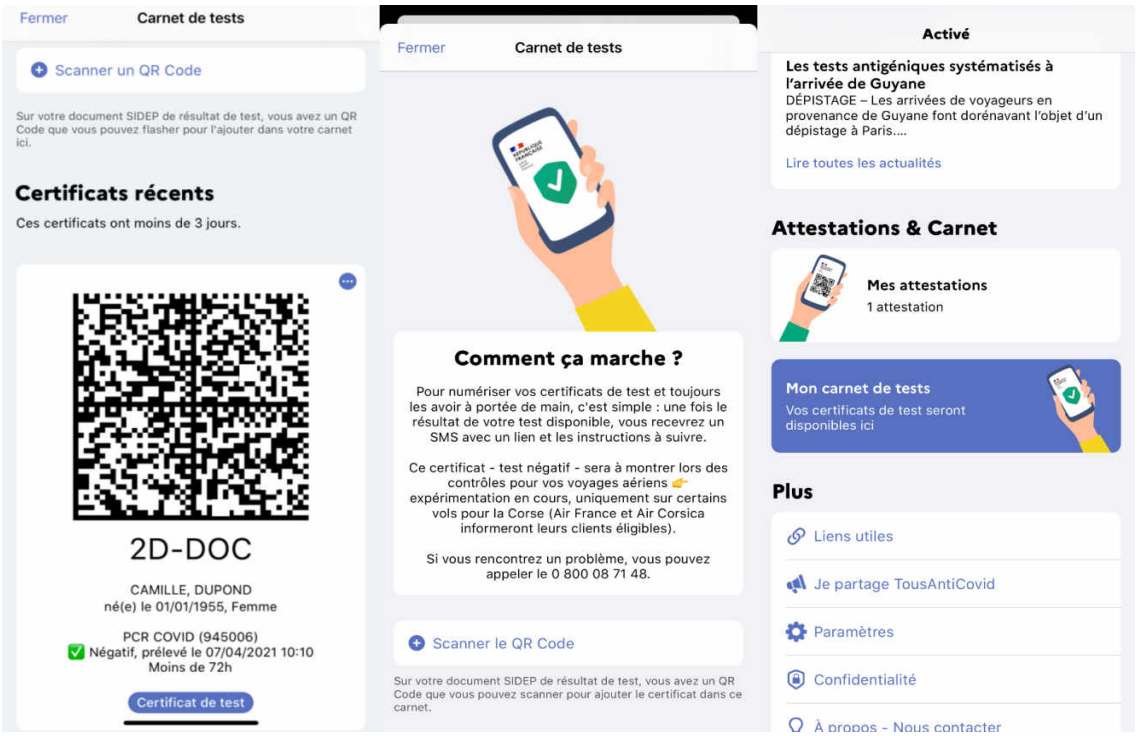
- **d'un justificatif de vaccination** ;

- **ou d'une attestation de rétablissement** après une contamination, soit en pratique un test de dépistage positif ancien.

Un mois plus tôt, le 19 avril, le Gouvernement avait présenté les modalités de ce dispositif dans le cadre de la mise en œuvre du **« certificat vert numérique » (cf. *supra*), c'est-à-dire du passeport sanitaire européen** : la France, initialement opposée au dispositif, devenait ainsi le premier État-membre à présenter une application pour le mettre en œuvre.

Concrètement, **le pass sanitaire « interne » et le passeport sanitaire correspondent à la même fonctionnalité de *TousAntiCovid*, le « *Carnet* »**, qui permet de stocker de manière électronique et sécurisée dans un *smartphone*s les certificats de tests ou de vaccination. L'utilisateur peut **télécharger manuellement ces certificats à partir de la base SI-DEP**, pour les tests et **à partir de la base VAC-SI** pour la vaccination. L'application en elle-même, qui ne connaît pas l'identité de l'utilisateur, n'a pas accès à ces deux fichiers. Le téléchargement permet ensuite de générer **un *QR code* (ou *Datamatrix*)**, qui contient la date et le type de test ou de vaccin, le nom de la personne et un identifiant, chiffré, du médecin ou de l'institution à l'origine de l'acte. C'est ce QR code que le voyageur peut présenter aux autorités, qui le **comparent ensuite à un fichier centralisé alimenté par les praticiens et géré par le ministère de la Santé**.

Captures d'écran de la fonctionnalité « Carnet » de *TousAntiCovid*



Source : Le Monde *du 19 avril 2021, d'après les images fournies par le secrétariat d'État chargé de la Transition numérique.*

B. DES CONTRADICTIONS QUI SE RÉPÈTENT

Le pass sanitaire constitue, bien entendu, un outil précieux dans le cadre de la sortie de la crise actuelle. Les Français d'ailleurs ne s'y trompent plus : **60 % d'entre eux se déclarent désormais favorables au dispositif** et prêts à s'y conformer[1], afin de retrouver une « vie normale ».

Ce dispositif est complémentaire de la vaccination – et même indissociable de celle-ci, puisqu'il permet d'en apporter la preuve, laquelle doit pourvoir être vérifiée par les autorités dès lors qu'il s'agit de voyager au sein de l'Union européenne. Surtout, et quoi que cela ne soit pas évoqué par le Gouvernement, **il s'agit d'un outil qui pourrait désormais être activé facilement à l'occasion d'une nouvelle crise sanitaire** : c'est donc un grand progrès.

Toutefois, les conditions de son adoption montrent que la France n'en a pas fini avec ses contradictions. Il suffit, pour s'en convaincre, de rappeler que les débats parlementaires ont été particulièrement houleux, et que l'essentiel des discussions n'a pas porté sur l'utilité du dispositif, mais sur l'ampleur des garanties et limitations dont il convenait de l'assortir.

---

[1] *D'après un sondage* Odoxa-Backbone Consulting *pour* Le Figaro *et* Franceinfo *publié le 13 mai 2021 : https://www.francetvinfo.fr/sante/maladie/coronavirus/covid-19-pour-retrouver-une-vie-normale-une-majorite-de-francais-approuvent-l-instauration-du-pass-sanitaire-selon-notre-sondage_4622593.html*

On peut, aussi, rappeler la chronologie des prises de position du Gouvernement sur le sujet :

– **en décembre 2020**, la France se déclarait opposée à la proposition de passeport sanitaire faite par certains de ses partenaires européens. Le directeur général de la Santé, Jérôme Salomon, estimait alors que « ***la liberté de circulation des personnes ne devrait pas être conditionnée à un certificat*** ». La France comptait alors 60 000 morts liés au Covid-19. Il n'était nullement question d'un pass sanitaire interne, sinon pour dénoncer le caractère intrusif du modèle chinois ;

– **fin janvier 2021**, le Premier ministre déclarait qu'il s'agissait d'un « *débat qui n'a pas lieu d'être* », tandis que le secrétaire d'État chargé des Affaires européennes, Clément Beaune, voyait dans le passeport vaccinal un dispositif « ***injuste et paradoxal*** », qui « ***créé une société à deux vitesses***[1] ». La France comptait alors 80 000 morts ;

– **fin avril**, la France devenait donc le premier pays européen à présenter un passeport sanitaire, avant d'en faire l'un des piliers du déconfinement. Elle comptait alors 100 000 morts ;

Dans son interview à la presse quotidienne régionale du 30 avril, le Président de la République estimait ainsi que, « *dans des lieux où se brassent les foules, comme les stades, festivals, foires ou expositions,* ***il serait absurde de ne pas l'utiliser*** ». Non sans ajouter, dans la même phrase, que « ***le pass sanitaire ne sera jamais un droit d'accès qui différencie les Français****. Il ne saurait être obligatoire pour accéder aux lieux de la vie de tous les jours comme les restaurants, théâtres et cinémas* ». « *Jamais* », jusqu'à ce qu'une crise plus grave ne vienne décider du contraire ?

Certes, La CNIL, quant à elle, a validé le pass sanitaire dans son avis du 12 mail[2] : on mesure le chemin parcouru en seulement quelques mois par l'institution, dont le département de prospective – qui n'est certes pas son collège – y voyait en mai 2020 un « *totem à risques* ». Là encore, la CNIL insiste notamment sur le **caractère temporaire** du dispositif (ce qui semble aller de soi) et sur son accessibilité sous **format papier**.

Surtout, la CNIL insiste à nouveau sur **son caractère facultatif** : à propos du passeport sanitaire, dans son avis du 22 avril[3], elle souligne que « *le caractère volontaire (…) doit rester une garantie essentielle du dispositif. L'utilisation de cette application* ***ne peut donc constituer une condition à la libre circulation des personnes*** ». Toutefois, si l'exigence est la même que pour le *contact tracing*, sa portée est en réalité bien plus limitée : **les « vraies » restrictions à la libre circulation sont les conditions sanitaires décidées par**

---

[1] *Précisons toutefois que le secrétaire d'État était alors interrogé sur un passeport* vaccinal*, et non pas* sanitaire *(avec trois critères), à un moment où la campagne de vaccination n'avait pas encore débuté. L'argument de l'inégalité peut donc s'entendre, même si cela n'a rien à voir avec l'efficacité.*

[2] https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-le-projet-de-passe-sanitaire

[3] https://www.cnil.fr/fr/la-cnil-precise-les-garanties-que-doit-respecter-la-fonctionnalite-tousanticovid-carnet

les États : tests, vaccination, quarantaine, etc. Dès lors, la seule chose vraiment facultative est l'usage du *smartphone* par rapport au papier : les mots sont bien forts pour défendre la liberté d'imprimer. Notons qu'une telle ambiguïté n'est pas l'apanage de la CNIL, loin s'en faut : la Commission européenne elle-même utilise les mêmes termes.

La CNIL insiste également sur l'impossibilité pour les autorités chargées du contrôle des voyageurs d'accéder aux données médicales. Dans le même esprit, **certains appellent notamment à restreindre le dispositif en raison du risque de « *rupture du secret médical* »**, à l'instar du professeur Emmanuel Rusch[1], président du comité de contrôle et de liaison Covid-19, qui propose par exemple que le terminal d'un policier ne lui indique qu'un statut (« vert » ou « rouge »), plutôt que le statut vaccinal ou les résultats des tests, pour permettre de « *laisser entre les mains de la personne le choix de ce qu'elle veut montrer* ». Là encore, pour louable qu'elle soit, cette proposition **risquerait de se révéler rapidement contreproductive**, compte tenu de l'hétérogénéité des critères appliqués par les différents pays : un feu « rouge » ou « vert » ne veut rien dire si tous ne reconnaissent pas les mêmes vaccins ou n'imposent pas les mêmes délais. Naturellement, le mieux serait encore d'harmoniser ces critères, mais ce qui semble déjà improbable au niveau européen est tout à fait irréaliste au niveau mondial.

Quant à la **Défenseure des droits**, elle a, dans son avis du 17 mai adressé au Parlement[2], **sévèrement jugé le dispositif présenté par le Gouvernement**. Cette sévérité est motivée par le faite que « *les atteintes portées aux droits et libertés doivent être temporaires et encadrées, strictement limitées et proportionnées à l'objectif poursuivi, à savoir la protection de la santé publique et la lutte contre la pandémie de Covid-19* », ce que pourtant nul ne conteste. Par conséquent, elle « *appelle les autorités à une extrême prudence dans la mise en place du dispositif du "pass sanitaire" qui n'aura vocation à être utilisé que le temps strictement nécessaire pour répondre à la situation sanitaire* ». Les « *préoccupations* » exprimées, relatives notamment aux conditions du débat parlementaire et à l'absence de concertation préalable, ainsi qu'à l'application du dispositif aux enfants, aux risques de discrimination et aux incertitudes concernant la durée d'immunité, sont légitimes et contribuent utilement à éclairer le législateur et le citoyen. **Mais elles ne remettent nullement en cause le bien-fondé de la mesure elle-même**.

---

[1] *Cité dans* Le Monde *du 19 avril 2021 : https://www.lemonde.fr/planete/article/2021/04/19/avec-son-passe-sanitaire-la-france-ouvre-la-voie-au-dispositif-europeen_6077338_3244.html*

[2] *https://www.defenseurdesdroits.fr/fr/communique-de-presse/2021/05/la-defenseure-des-droits-sinquiete-des-risques-datteintes-aux-droits-et*

TROISIÈME PARTIE :
LE *CRISIS DATA HUB*, BOÎTE À OUTILS POUR UNE RIPOSTE NUMÉRIQUE GRADUÉE

I. LE CHOIX DU NUMÉRIQUE : PROTÉGER LA SANTÉ PUBLIQUE ET PRÉSERVER LES LIBERTÉS INDIVIDUELLES

A. L'INCONCEVABLE RECONFINEMENT CHRONIQUE

Depuis près d'un an et demi, les Français vivent au rythme des confinements et couvre-feu successifs, entre autres bouleversements de leurs existences et restrictions de leurs libertés. **Ces mesures ont permis de sauver des vies**, mais elles n'ont pas empêché d'en perdre plus de 100 000, et se sont faites au prix d'une récession historique, et d'une **« bombe à retardement » dont on mesure à peine l'ampleur des conséquences, notamment sur le plan psychologique** (hausse des symptômes de dépression et d'anxiété, voire des suicides[1], etc.) et sur le **plan sanitaire** (retards de prise en charge, etc.), mais aussi sur le **plan économique**.

Et ces mesures ne sont plus supportables, ni par les individus, comme en témoigne le relâchement constaté l'été dernier et à nouveau cette année à l'approche des beaux jours et du déconfinement, **ni par les entreprises**, qui ne peuvent éternellement dépendre des aides publiques, **ni par l'État lui-même**, qui évoque de plus en plus ouvertement le prix du « quoi qu'il en coûte ».

Pour la première fois, la vaccination offre la perspective d'une sortie de crise bien réelle et relativement rapide : on n'insistera jamais assez sur l'immense succès collectif que représentent le développement de vaccins très innovants et leur production massive dans un temps aussi court. Il ne faut pas, pour autant, négliger le reste : la vaccination est le pilier principal de la sortie de crise, mais elle ne saurait être le seul, et doit s'inscrire dans un ensemble plus large de mesures. **Mais surtout, il ne s'agit que de la sortie de *cette* crise, alors que la probabilité de prochaines épidémies, peut-être plus graves encore, fait consensus au sein de la communauté scientifique**, et que rien ne permet d'affirmer que nous disposerions alors d'un vaccin

[1] *La corrélation entre crises et vagues de suicides est bien documentée depuis la crise de 1929, mais celle-ci se constate souvent avec plusieurs mois ou années de retard. Elle est toutefois déjà visible au Japon, où le nombre de suicides, déjà l'un des plus élevé au monde, a augmenté de 750 en 2020 (soit 21 000 suicides au total). Il s'agit de la première hausse depuis 11 ans, particulièrement forte chez les plus jeunes. La France, qui compte également l'un des taux de suicide les plus élevés d'Europe (9 000 suicides par an), a également connu une hausse pendant la crise sanitaire, mais les chiffres précis ne sont pas encore disponibles. D'après une étude Ipsos publiée en janvier 2021, 18 % des personnes interrogées se sentent toujours ou souvent seules, contre 13 % en 2018, et 63 % des individus souffrant de solitude ont eu des pensées suicidaires.*

efficace. Il n'existe même pas de certitude quant à la durée d'immunité procurée par les vaccins actuels contre le Covid-19, ni quant à leur efficacité sur les nouveaux variants – et on ne parle ici que de coronavirus.

Nous ne pouvons pas nous permettre de reconfiner chroniquement le pays, de mettre la société et l'économie sous cloche, à chaque nouvelle menace.

C'est d'autant plus inacceptable qu'il existe des moyens de faire autrement, grâce au numérique. Les choses ont déjà beaucoup évolué en un an seulement, comme en témoigne, entre autres, l'inversion complète du discours politique et médiatique sur le pass sanitaire. Il faut maintenant aller plus loin. **Aujourd'hui, le risque est celui d'un retour de l'insouciance**. Profitons plutôt des circonstances favorables de la sortie de crise pour nous préparer sereinement à l'avenir.

B. UN COMPROMIS À ASSUMER : DES MESURES INTRUSIVES MAIS PLUS CIBLÉES ET LIMITÉES DANS LE TEMPS

Le présent rapport propose donc **de recourir bien plus fortement aux outils numériques dans le cadre de la gestion des crises sanitaires** ou des crises comparables (catastrophe naturelle, industrielle, etc.), **notamment en vue de contrôler au niveau individuel le respect des mesures imposées par la situation, et y compris si cela implique d'exploiter des données de manière intrusive et dérogatoire**.

En contrepartie, ces mesures pourraient être bien plus limitées, à la fois dans leur nature, dans le nombre de personnes concernées, et dans la durée, épargnant à la société les conséquences de confinements prolongés et de restrictions générales. Pour reprendre l'exemple évoqué au début de la deuxième partie du présent rapport, on pourrait imaginer que **seules les personnes diagnostiquées positives, soit environ 0,1 % de la population fin mai 2021**, soient soumises à des mesures d'isolement, mais que ces mesures soient **étroitement contrôlées** (par une géolocalisation en direct par exemple) et **sévèrement sanctionnées** (par une amende prélevée automatiquement, par exemple). **Aucune autre restriction ne serait imposée** au reste de la population ni à la vie économique et sociale en générale, et **l'épidémie pourrait être freinée plus vite**.

Dans un tel exemple, des **technologies intrusives** sont nécessaires, et des **traitements de données dérogatoires** aussi : il s'agit en effet de croiser des données personnelles, y compris des données sensibles relatives à l'état de santé, avec des données de géolocalisation et des données bancaires. **Rien d'impossible techniquement, et rien de très exceptionnel en comparaison de ce que font les GAFA à des fins purement commerciales** mais, s'agissant de l'État, de l'intérêt général et de la santé publique, il s'agirait d'une grande nouveauté.

Il ne s'agit là que d'un exemple parmi de multiples possibilités, dont l'opportunité doit être appréciée au cas par cas, en fonction de la gravité de la menace et au regard des autres restrictions imposées. En toutes circonstances, **il faut raisonner en termes de *proportionnalité* et de *rapport coûts-bénéfices*, en comparant les atteintes aux libertés « numériques » à celles portées aux libertés « physiques »**.

Comme l'avait déclaré le secrétaire d'État chargé du numérique, Cédric O, à l'époque du développement de l'application française de *contact tracing*[1] : « ***StopCovid n'est pas une application de temps de "paix". Un tel projet n'existerait pas sans la situation créée par le Covid-19*** ». Cette remarque vaut d'une manière générale.

Reste, concrètement, à répondre à cette question : **comment avoir les *avantages* du numérique** (l'efficacité du ciblage individuel en temps réel) **sans ses *inconvénients*** (son caractère intrusif et le risque d'utilisation détournée) ? Les propositions qui suivent proposent quelques pistes.

C. LES CHANTIERS DE LONG TERME

Plutôt que de multiplier les recommandations, nécessairement moins fortes et plus techniques, le présent rapport formule **une seule grande proposition, pragmatique, qui permettrait de répondre efficacement aux situations de crise – et qui ne ferait que cela**. C'est le « *Crisis Data Hub* », présenté dans la partie suivante.

Cette proposition est **complémentaire des chantiers plus généraux, de plus longue haleine**, qu'il faut continuer à mener avec détermination, en surmontant les obstacles et en gagnant la confiance des citoyens. Parmi les chantiers les plus importants, déjà évoqués, on peut notamment citer celui de **l'identité numérique**, du **numérique en santé**, et plus largement de tout ce qui permet d'aller vers un **État-plateforme**, dont la flexibilité permettra de réagir plus efficacement à toute situation de crise, entre autres bénéfices.

[1] https://cedric-o.medium.com/stopcovid-ou-encore-b5794d99bb12

II. LE *CRISIS DATA HUB* : UNE PLATEFORME DE CRISE

A. LE PRINCIPE : NE PAS COLLECTER LES DONNÉES, MAIS ÊTRE EN CAPACITÉ DE LE FAIRE EN CAS D'URGENCE

Le problème peut être résumé ainsi : si l'on veut à l'avenir sauver des vies humaines et éviter de mettre la vie économique et sociale sous cloche à chaque nouvelle crise, **il faudra inévitablement s'appuyer à ce moment-là sur des croisements de données massifs et dérogatoires**.

Or les données en question sont susceptibles d'être à la fois :

- **des données personnelles et sensibles qu'il est absolument inconcevable d'exploiter en temps « normal »**, par exemple des données de géolocalisation croisées avec des données médicales à des fins de maintien de l'ordre public sanitaire ;

- **des données produites par des entreprises privées** (opérateurs télécom, entreprises technologiques, établissements financiers, laboratoires pharmaceutiques, transports publics, employeurs, etc.) qui n'ont souvent **aucune raison économique ni obligation juridique de les fournir par ailleurs, ni même de s'y préparer matériellement**. Une partie des difficultés rencontrées lors de la crise actuelle s'explique d'ailleurs par cela : même avec la meilleure volonté du monde, et même pour des données *non* personnelles ne nécessitant pas de dérogation au cadre juridique en vigueur, les acteurs dont les données auraient pu être utilement exploitées n'étaient tout simplement pas en capacité de les fournir telles quelles immédiatement[1]. Du reste, il aurait encore fallu savoir à qui les fournir, or **les pouvoirs publics n'étaient pas équipés pour pouvoir les exploiter correctement**, voire pour avoir ne serait-ce que *l'idée* de les exploiter.

Il n'y a là rien de spécifique à la France : **ces choses ne s'improvisent pas, à moins d'une « agilité » particulièrement forte** – laquelle n'est pas la caractéristique première des grandes structures administratives, peut-être robustes et efficaces dans la gestion de l'existant, mais souvent démunies lorsque tout ne se passe pas comme prévu.

Du reste, il est impossible de savoir *a priori* quelles données pourraient être utiles face à une nouvelle crise, tant cela dépend de sa *nature* (une épidémie, une catastrophe naturelle ou industrielle, etc.), de son *intensité*, de son *extension géographique* (localisée, nationale, internationale) et de l'*acceptabilité politique* des mesures, au cas par cas. Seules les données relatives à **l'identification** des personnes et à leur **géolocalisation** semblent constituer un dénominateur commun à l'ensemble des cas envisageables.

---

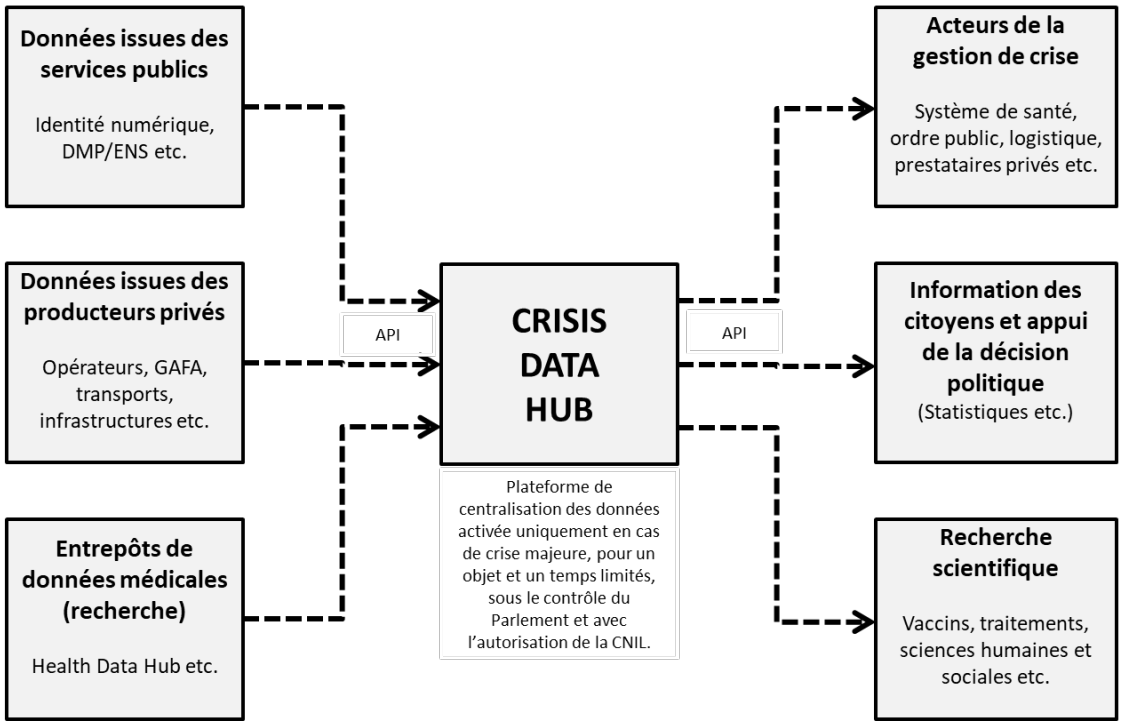
[1] *L'utilisation des données d'Orange à des fins de modélisation épidémiologique constitue à cet égard une exception.*

Pourtant, rien ne serait pire que l'improvisation, à la fois inefficace et potentiellement bien plus attentatoire aux libertés individuelles, qui sont moins faciles à « protéger » dans l'urgence.

Dans ces conditions, le présent rapport propose donc non pas de collecter une multitude de données sensibles à l'utilité hypothétique, mais tout simplement de *nous mettre en capacité de le faire, pour ainsi dire en appuyant sur un bouton*, si jamais les circonstances devaient l'exiger.

Concrètement, cela implique de mettre en place **une plateforme sécurisée spécifique, qui ne serait activée qu'en temps de crise**. Celle-ci permettrait de **centraliser** les données nécessaires à la réponse des pouvoirs publics, permettant de faire **remonter** les informations immédiatement, et de les **redistribuer** ensuite aux acteurs concernés pour remplir leurs missions – soit, selon les circonstances, les établissements et professionnels de santé, la sécurité civile voire les forces de l'ordre, les collectivités locales, les gestionnaires d'infrastructures, etc.

Présentation simplifiée du *Crisis Data Hub*



Source : délégation sénatoriale à la prospective

Ce « *Crisis Data Hub* » rappelle le modèle du *Health Data Hub* – à cela près que le *Health Data Hub* ne centralise que des données médicales et pseudonymisées mais qu'il le fait massivement et en permanence, alors que le *Crisis Data Hub* (CDH) centraliserait des données plus diverses (géolocalisation, etc.) et le cas échéant nominatives, mais qu'il le ferait **de**

façon plus ciblée et surtout pendant une période plus limitée. Seules les données pertinentes au regard de telle ou telle crise seraient concernées, qu'il s'agisse de la nature des données ou d'un « filtre » géographique ou individuel, en application du **principe de riposte graduée**.

Le CDH serait ainsi à la gestion numérique d'une crise sanitaire ce que l'Établissement de préparation et de réponse aux urgences sanitaires **(EPRUS) aurait dû être sa gestion logistique** – si cet établissement public créé au lendemain de l'épidémie de H1N1 n'avait pas été dissous en 2016, avec les lourdes conséquences identifiées depuis[1].

B. LES MODALITÉS : UNE PLATEFORME NUMÉRIQUE ET UNE OBLIGATION JURIDIQUE

1. Le volet technique : une plateforme sécurisée et une API

Sur le plan technique, le *Crisis Data Hub* consiste donc en une **plateforme** permettant de connecter entre elles différentes bases de données et d'exécuter les traitements nécessaires. Le lien avec les producteurs ou utilisateurs de données se fait par **une interface de programmation, ou *Application Programming Interface* (*API*)**.

À cette fin, il convient avant tout d'investir dans **une solution *cloud* d'hébergement sécurisée,** capable de monter très rapidement en capacité. Par rapport à un hébergement « en propre » sur les serveurs physiques d'une organisation, le *cloud* présente en effet de nombreux avantages, qui deviennent cruciaux dans un contexte de gestion de crise[2] :

- la flexibilité dans l'utilisation des capacités : principal avantage du *cloud*, cette « *scalabilité* » est indispensable pour un dispositif qui a vocation à être activé en urgence et pour traiter des données dont ni la nature, ni la quantité ne peuvent être précisément déterminées à l'avance ;

---

[1] *Mis en place en 2007 à la suite de l'épidémie de grippe aviaire, l'Établissement public de préparation et de réponse aux urgences sanitaires (EPRUS) avait pour mission principale « l'acquisition, la fabrication, l'importation, le stockage, la distribution et l'exportation des produits et services nécessaires à la protection de la population face aux mesures sanitaires graves », y compris donc les traitements, vaccins et maques FFP2 qui ont tant fait défaut au début de la pandémie de Covid-19. Ses moyens budgétaires ont toutefois été progressivement réduits et, en 2016, l'EPRUS a été supprimé et ses missions confiées à Santé Publique France, qui en avait déjà bien d'autres.*

[2] *Cette liste est issue du livre blanc sur le Coud européen publié le 4 mai 2021 par le cabinet KPMG, à partir notamment de plus de 250 entretiens avec des décideurs publics et privés européens. Elle contient un sixième critère, celui de la flexibilité des coûts, qui est directement lié à la flexibilité des capacités mais qui est secondaire dans un contexte de gestion de crise majeure. D'une manière générale, 82 % des décideurs interrogés par le cabinet KPMG ont d'ailleurs augmenté leur utilisation du cloud en réponse directe à la pandémie. Cf. https://home.kpmg/fr/fr/home/media/press-releases/2021/05/cloud-europeen-marche-enjeux-economiques.html*

- la collaboration entre les équipes et l'échange de données sécurisées : le CDH a vocation à traiter de données sensibles, et celles-ci devront pouvoir être échangées rapidement entre des acteurs qu'il n'est, là non plus, pas possible de prévoir à l'avance ;

- l'agilité et la fluidité du déploiement : le *cloud* permet notamment aux développeurs d'utiliser des « briques » logicielles standard, prêtes à l'emploi et constamment enrichies par les acteurs du secteur, qui se trouvent être les entreprises les plus performantes du monde en matière d'intelligence artificielle ;

- la sécurité et la résilience ;

- l'agilité de déploiement des activités stratégiques.

Les trois services du *cloud computing*

Infrastructure as a Service (IaaS) : **le client loue, par abonnement, une infrastructure informatique** (serveurs, stockage, sauvegarde, virtualisation, réseaux, etc.) qui se trouve dans les locaux physiques du fournisseur, lequel est aussi responsable de la sécurité. **Le client paie en fonction de sa seule consommation**, par opposition au modèle traditionnel où il supporte les coûts d'investissement et de maintenance de sa propre infrastructure, y compris si celle-ci se trouve en sous-capacité ou surcapacité. Le client demeure en revanche responsable de la partie logicielle (*software*), c'est-à-dire les applications de traitement des données hébergées sur le *cloud*.

Software-as-a-Service (SaaS) : **les logiciels sont développés par le fournisseur et installés sur les serveurs de ce dernier**. Le client peut les utiliser librement en échange d'un abonnement, plutôt que d'une licence. Parmi les principaux exemples, on peut notamment citer les services de messagerie, de collaboration, de gestion de la relation client (CRM) ou des ressources humaines (GRH), de visioconférence ou encore de création de sites de e-commerce.

Platform-as-a-Service (PaaS) : le client développe et maîtrise lui-même ses applications, tandis que le fournisseur de *cloud* lui offre **un environnement d'exécution rapidement disponible** (infrastructure, logiciels de base tels que les systèmes d'exploitation, base de données, etc.), qui lui épargne notamment les tâches de configuration. Ce modèle est particulièrement adapté aux applications « métier » spécifiques – parmi lesquelles on peut trouver la recherche médicale et épidémiologique, ou encore la gestion d'une campagne de dépistage ou de vaccination.

Ces trois types de services sont naturellement **cumulables**, et tous sont proposés par les principaux acteurs du secteur, notamment *Amazon Web Services* (AWS), *Microsoft Azure* et *Google Cloud*. Leur point commun est d'être proposés **sur demande** (*as a Service – aaS*) et donc de s'adapter en temps réel aux besoins du client.

En temps « normal », aucune donnée ne serait bien sûr échangée dans ce cadre. **En revanche, ce temps serait mis à profit pour la construction, la maintenance et l'amélioration du système**, qui ont cruellement fait défaut lors de la crise actuelle.

2. Le volet juridique : une obligation de disponibilité des données

D'un point de vue juridique, la mise en place du *Crisis Data Hub* se traduirait par **la création d'une obligation légale, pour certaines entreprises et organisations, de maintenir des bases de données dont le contenu et le format seraient fixés à l'avance, et de se tenir prêtes à les connecter** à la plateforme, *via* l'API, en cas de nécessité.

La seule nouveauté ici concerne le fait de *se préparer* à transmettre les données. La demande de transmission effective, formulée le cas échéant par les pouvoirs publics, s'inscrit quant à elle soit dans le cadre du **droit commun de la réquisition administrative**[1], soit en application d'un **article spécifique de la loi relative à l'État d'urgence sanitaire**. Ces réquisitions font l'objet d'une indemnisation.

Le pouvoir de réquisition au titre de l'état d'urgence sanitaire

Bien qu'ils n'aient pas été utilisés à des fins de réquisition des données lors de la crise du Covid-19, plusieurs articles relatifs au pouvoir de réquisition ont été introduits dans le code de la santé publique par la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de Covid-19 :

- l'article L. 3131-1 pose un principe général : « *En cas de menace sanitaire grave appelant des mesures d'urgence, notamment en cas de menace d'épidémie, le ministre chargé de la santé peut, par arrêté motivé, prescrire dans l'intérêt de la santé publique toute mesure proportionnée aux risques courus et appropriée aux circonstances de temps et de lieu afin de prévenir et de limiter les conséquences des menaces possibles sur la santé de la population. (…) Le ministre peut habiliter le représentant de l'État territorialement compétent à prendre toutes les mesures d'application de ces dispositions, y compris des mesures individuelles. Ces dernières mesures font immédiatement l'objet d'une information du procureur de la République* » ;

- l'article L. 3131-15 précise quant à lui que « *dans les circonscriptions territoriales où l'état d'urgence sanitaire est déclaré, le Premier ministre peut, par décret réglementaire pris sur le rapport du ministre chargé de la santé, aux seules fins de garantir la santé publique : (…)* ***7° Ordonner la réquisition de toute personne et de tous biens et services nécessaires à la lutte contre la catastrophe sanitaire****. L'indemnisation de ces réquisitions est régie par le code de la défense* ».

[1] *En pratique, de très nombreux textes portent sur le pouvoir de réquisition, qui peut être exercé par le Premier ministre ou le préfet sur le territoire de son département. Le régime général de la réquisition s'exerce habituellement au titre du pouvoir de police du préfet, en application du 4° de l'article L.2215-1-4° du code général des collectivités territoriales :* «En cas d'urgence, lorsque l'atteinte constatée ou prévisible au bon ordre, à la salubrité, à la tranquillité et à la sécurité publiques l'exige et que les moyens dont dispose le préfet ne permettent plus de poursuivre les objectifs pour lesquels il détient des pouvoirs de police, celui-ci peut, par arrêté motivé (…) **réquisitionner tout bien ou service**, requérir toute personne nécessaire au fonctionnement de ce service ou à l'usage de ce bien et prescrire toute mesure utile jusqu'à ce que l'atteinte à l'ordre public ait pris fin ou que les conditions de son maintien soient assurées ».

C'est notamment sur le fondement de ce dernier article qu'il a été procédé à la **réquisition des masques FFP2** au début de la crise sanitaire, ou encore des personnels médicaux et des pompes funèbres.

Ce n'est pas la première fois qu'un tel pouvoir de réquisition est utilisé dans le cadre d'une crise sanitaire : en 2006, les locaux et personnels des cliniques privées avaient été réquisitionnés pour assurer la prise en charge des patients atteints du chikungunya, et en 2009, des locaux, personnels médicaux et personnels administratifs l'avaient été dans le cadre de la crise H1N1. Le code de la santé publique contient d'ailleurs plusieurs autres articles en ce sens :

- l'article L. 3131-8 concerne le pouvoir de réquisition du préfet : « *Si l'afflux de patients ou de victimes ou la situation sanitaire le justifie, sur proposition du directeur général de l'agence régionale de santé, le représentant de l'État dans le département peut procéder aux réquisitions nécessaires de tous biens et services, et notamment requérir le service de tout professionnel de santé, quel que soit son mode d'exercice, et de tout établissement de santé ou établissement médico-social* ».

- l'article L. 3131-9 autorise, dans les mêmes conditions, l'exercice du pouvoir de réquisition par les préfets de zone de défense (par arrêté) ou par le Premier ministre (par décret).

Ainsi, rien n'interdit que des données nécessaires à la gestion d'une crise sanitaire puissent faire l'objet d'une réquisition administrative si les circonstances l'exigent.

Compte tenu de la sensibilité potentielle de certaines données et du caractère dérogatoire des traitements mis en œuvre, il est important que la transmission se fasse sous le régime de **la réquisition : celui-ci évite en effet aux entreprises d'en assumer la responsabilité face à leurs clients**. De fait, cette responsabilité incombe aux seuls pouvoirs publics, qui agissent ici au nom de l'intérêt général et doivent justifier des mesures prises devant les citoyens.

La liste des acteurs soumis à ce régime spécifique serait fixée par décret. Pour la définir, **il serait possible de s'inspirer de la liste des opérateurs d'importance vitale (OIV)**, lesquels sont soumis à des obligations particulières, notamment en matière de systèmes d'information, et bénéficient à ce titre d'un **accompagnement de l'ANSSI** (la comparaison a bien sûr ses limites, la finalité des deux régimes étant notamment différente).

Les opérateurs d'importance vitale (OIV)

Les **opérateurs d'importance vitale (OIV)** sont les acteurs publics ou privés dont les activités sont considérées comme **indispensables à la survie de la nation** ou dangereuses pour la population. Leur protection contre les actes de malveillance (terrorisme, sabotage, etc.) et les **risques naturels, technologiques et sanitaires** relève de la politique de **sécurisation des activités d'importance vitale (SAIV)**, conçue et pilotée par le secrétariat général de la défense et de la sécurité nationale (SGDSN).

La liste compte **environ 250 OIV, répartis en 13 secteurs d'activité** : santé, transport, gestion de l'eau, industrie, énergie, finances, communications, activité militaire, activité civile de l'État, activité judiciaire, alimentation, espace et recherche. Pour des raisons de sécurité nationale, cette liste n'est pas publique.

Une fois désignés, les **OIV bénéficient d'une protection particulière et sont soumis** à **des obligations spécifiques** : la désignation d'un délégué pour la défense et la sécurité (interlocuteur privilégié de l'autorité administrative, habilité « Confidentiel défense ») ; la rédaction d'un plan de sécurité d'opérateur (PSO) qui décrit l'organisation et la politique de sécurité de l'opérateur ; la rédaction de plans particuliers de protection (PPP) pour chacun des points d'importance vitale identifiés. La procédure de « criblage » permet aux OIV de demander à l'autorité administrative de vérifier que les caractéristiques de la personne souhaitant accéder à son PIV ne sont pas incompatibles avec la sécurité du site concerné.

Face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leurs impacts potentiellement destructeurs, il a été décidé, à la suite du Livre blanc sur la défense et la sécurité nationale de 2013, de **compléter ce dispositif par un important volet relatif à la cybersécurité**, prévu par l'article 22 de la loi de programmation militaire de 2013.

L'Agence nationale de sécurité des systèmes d'information (ANSSI) est ainsi chargée d'accompagner les OIV dans la mise en œuvre de leurs **obligations spécifiques en matière de sécurisation de leurs systèmes d'information**[1].

Sources : délégation à la prospective, d'après les informations de l'ANSSI et du SGDSN.

Dans de nombreux cas, les entreprises concernées sont par ailleurs **délégataires d'une mission de service public** (transport, etc.), quand elles ne sont pas tout simplement des entreprises publiques. Beaucoup exercent une activité dans un **secteur règlementé**, et sont familières des discussions avec les pouvoirs publics. Tout cela pourrait faciliter l'élaboration et la mise en place de l'obligation proposée.

Toutefois, certaines données potentiellement cruciales dans le cadre d'une gestion de crise **sont produites par des entreprises qui ne sont pas françaises, ce qui pose la question de la portée extraterritoriale effective de la mesure**. L'exemple-type est celui des données de géolocalisation, que Facebook utilise pour son *Safety Check*, mais qu'il est peu probable que la France puisse obtenir sur simple demande. Le verrouillage du *Bluetooth* par Apple dans le cadre du développement des applications de *contact tracing* doit nous inviter à ne pas faire preuve de naïveté.

Dans de pareils cas, une attitude pragmatique s'impose :

- t**out d'abord**, si le *Crisis Data Hub* pouvait *au moins* accéder aux données produites par des acteurs français, ce serait déjà un progrès immense. L'enrichissement du « catalogue » de la plateforme sera de toute façon progressif ;

[1] *Décret n° 2015-351 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et décret n° 2015-350 relatif à la qualification des produits de sécurité et des prestataires de services de confiance pour les besoins de la sécurité nationale.*

- e**nsuite**, s'il est très peu vraisemblable que les GAFA acceptent de participer au dispositif, il est incontestable que ceux-ci, par ailleurs, ont **agi de façon volontariste et proactive dans le cadre de la gestion de la crise du Covid-19**, développant des outils spécifiques et partageant certaines données avec des chercheurs dans le cadre de partenariats (cf. *supra*). **Une approche partenariale est donc possible, et même prometteuse** compte tenu de la réactivité de ces entreprises, de leur sens de l'innovation et de leurs moyens considérables ;

- e**nfin, et surtout, l'idéal serait de mettre en place un *Crisis Data Hub* européen (ECDH)** : celui-ci permettrait non seulement de convaincre davantage d'entreprises, mais aussi d'utiliser et de partager davantage de données pour gérer des crises qui, par nature, ont une dimension transnationale. **Naturellement, le chemin est encore long** : c'est pourquoi le présent rapport se concentre sur un ***Crisis Data Hub* national, comme premier pas mais aussi « preuve du concept »**, comme l'est du reste dans son domaine le *Health Data Hub*.

L'obligation juridique faite aux *producteurs* de données pourrait se doubler d'une **obligation symétrique pour les *utilisateurs* (potentiels)** de ces données, c'est-à-dire les acteurs de la gestion de crise (établissements de santé, prestataires logistiques, gestionnaires d'infrastructures, etc.).

On notera que les acteurs de la gestion de crise, producteurs comme utilisateurs potentiels de données, peuvent aussi être des **administrations publiques** (hôpitaux, sécurité civile, forces de l'ordre, autorités de régulation diverses, etc.). Ceci rappelle qu'au-delà de la création d'un régime juridique *ad hoc*, **l'enjeu est aussi celui de la préparation opérationnelle** : disposer des bonnes données est une chose, avoir la capacité de bien les utiliser au bon moment – et ne serait-ce que d'y penser – en est une autre.

C. LES GARANTIES DÉMOCRATIQUES : UN RÉGIME PROTECTEUR, ACCEPTÉ EN AMONT, ACTIVÉ EN TOUTE TRANSPARENCE, ET CONTRÔLÉ EN CONTINU

Compte tenu de sa portée potentielle, le dispositif proposé ici peut légitimement soulever des interrogations s'agissant de la protection des droits et libertés. À cet égard, il convient tout d'abord de rappeler que **rien n'est pire que l'improvisation, qui est à la fois bien moins efficace et potentiellement bien plus attentatoire aux libertés individuelles**.

Ensuite, il doit être rappelé que **se préparer à collecter des données n'implique nullement que cette collecte aura forcément lieu**, ni le cas échéant qu'elle aura lieu dans ses proportions maximales. Il s'agit bien d'un dispositif de **réponse graduée** à la menace.

Enfin, et surtout, la préparation en amont d'un dispositif de collecte et d'exploitation des données **est, en réalité, la meilleure garantie qui puisse être apportée aux droits et libertés**. En effet, cette préparation en amont rend possible :

- d'une part, l'élaboration d'un cadre juridique adapté et réfléchi, spécifique aux situations de crise, et permettant de concilier la protection de la vie privée et celle de la santé ;

- d'autre part, une activation sous la forme d'une « loi-cadre », qui permette à la fois d'obtenir un **consensus politique** et de préserver la **marge de manœuvre** de l'administration, dont la contrepartie serait un mécanisme *ad hoc* de **contrôle en continu**.

L'urgence est l'ennemie de la démocratie : le *Crisis Data Hub* est un moyen de ne pas être pris au dépourvu.

1. Un cadre juridique spécifique, prévu à l'avance et protecteur des droits et libertés

Face à la pandémie de Covid-19, la construction du cadre juridique de protection des données personnelles **s'est faite au fil de l'eau**, au fur et à mesure de la mise en place *effective* des dispositifs (fichiers sanitaires, pass sanitaire, etc.), car ceux-ci n'avaient pas été envisagés ni débattus auparavant. La création en amont d'une « boîte à outils » ayant *éventuellement* vocation à être utilisée **permettrait, dans la mesure du possible, de décorréler la réflexion juridique de la mise en œuvre des mesures**, et de réduire ainsi la place des inévitables tâtonnements, incertitudes et contradictions propres à une période de crise.

Cela vaut, d'abord, pour le **Parlement**, où les débats sur les contours du dispositif pourraient se dérouler sereinement, en prenant **le temps nécessaire à l'expertise et à la pédagogie**, et non pas sous la pression des circonstances et des contingences politiques.

S'agissant en particulier des données personnelles, cela permettrait aussi à **la CNIL d'établir *en amont* une doctrine d'autorisation précise et graduée en fonction du niveau de la menace**, plutôt que d'avoir à se prononcer au cas par cas – ce qu'elle a toutefois fait, il faut le souligner, avec une grande rapidité.

La même remarque vaut pour **le juge administratif et judiciaire**. Lors de la crise, et comme d'habitude, les recours ont été traités au cas par cas – avec, là encore, une véritable rapidité, notamment grâce à la procédure du référé, mais au prix, parfois, d'une remise en cause des dispositifs utilisés par l'administration. On peut citer le cas des **drones**, sur lequel le juge comme la CNIL se sont prononcés : sans contester le fond de cette décision, chacun pourra reconnaître qu'**il aurait été préférable pour tout le monde de savoir avant si cela était possible**.

La mise en place du *Crisis Data Hub* implique de réfléchir à l'avance à toute une série de mesures, de la plus légère à la plus intrusive, au regard de menaces théoriques. Lancer ce chantier **permettrait ainsi au juge de se prononcer *en amont* sur certaines mesures**, sans attendre leur hypothétique mise en œuvre effective, mais en leur garantissant un haut niveau de sécurité juridique. Naturellement, cela n'exclurait en rien la possibilité d'un recours sur le moment, et compte tenu de circonstances spécifiques : les deux voies sont complémentaires.

Du reste, la voie juridictionnelle n'est pas la seule possible : la « boite à outils » du *Crisis Data Hub* **se prête particulièrement bien au développement d'une procédure de « rescrit »**, que pourraient en l'espèce solliciter les associations de défense des libertés publiques, les citoyens, ou encore les opérateurs dont les données pourraient être requises.

Les craintes – légitimes – que suscite le recours à des technologies intrusives ne portent pas seulement sur les *règles* juridiques encadrant les traitements de données, mais aussi sur **la *réalité* de ces traitements : comment peut-on avoir la certitude que les données ne seront pas ensuite utilisées de manière abusive, volontairement ou par manque de sécurité ?**

C'est le dernier grand avantage du *Crisis Data Hub* : celui-ci peut être développé en *open source*, de sorte que chacun aura non seulement la possibilité, mais aussi le temps, d'examiner chaque ligne de code, chaque champ de chaque base de données, pour être sûr que le dispositif ne fait rien d'autre que ce qu'il est censé faire. Faisons confiance à la société civile pour se saisir pleinement de cette possibilité. **Aucune modalité de gestion de la crise du Covid-19 ne présente un tel niveau de garantie des droits et libertés, ni en France, ni ailleurs dans le monde**. La France n'a certes pas à rougir de sa situation : l'algorithme de *TousAntiCovid*, par exemple, est en *open source*, mais il ne s'agit là que d'un outil parmi d'autres, là où le *Crisis Data Hub* permettrait l'*open data* par défaut.

2. Une procédure d'activation favorisant le consensus et l'union nationale plutôt que les polémiques

Élaborer en amont un cadre juridique applicable à la mise en œuvre *éventuelle* de certaines mesures est une chose ; **décider de leur mise en œuvre *effective* lors d'une crise en est une autre**, qui relève de la responsabilité du Gouvernement et du Parlement, mais **ne peut se faire sans un soutien de l'opinion, c'est-à-dire sans un consensus démocratique**.

À cet égard, la gestion de la crise du Covid-19 n'a pas bénéficié d'un climat particulièrement apaisé, mais a plutôt souffert d'une **succession de polémiques et de revirements dans l'opinion publique, mais aussi dans les médias et au sein de la classe politique**. Citons par exemple le cas de la

vaccination[1] ou, pour rester dans le domaine du numérique, celui l'adhésion à *TousAntiCovid* ou au pass sanitaire (cf. Partie II), d'abord accueillis avec circonspection voire rejetés, puis réclamés ensuite pour hâter le retour à la normale.

Dans le même temps, il a souvent été reproché au Gouvernement de ne pas en faire assez contre l'épidémie, ou de ne pas agir en fonction des seuls impératifs sanitaires ni même économiques et sociaux, mais de décider des restrictions « en fonction des sondages ». Le reproche est trop facile : en démocratie, il est **tout à fait logique de prendre en compte, parmi d'autres critères, l'acceptabilité politique des mesures envisagées**, sans laquelle elles seraient de toute façon vouées à l'échec. Plus généralement, la France se distingue par le **très faible niveau de confiance que les citoyens accordent au Gouvernement** pour faire face à la crise[2].

Ce qui a si souvent manqué, c'est donc un consensus politique sur les mesures à prendre, au cas par cas, sur le moment, faute de les avoir anticipées bien sûr, mais aussi faute de disposer d'une procédure adaptée, avec l'équivalent d'une **« loi-cadre » pour le recours aux outils numériques, c'est-à-dire une « boîte à outils » préalablement définie** au sein de laquelle le Gouvernement aurait pu « piocher » en fonction des circonstances, sans devoir à chaque fois justifier le principe même de chaque mesure, expliquer pourquoi ce qui n'était pas nécessaire hier l'est devenu aujourd'hui, et pourquoi le calendrier promis ne serait finalement pas tenu. **Le *Crisis Data Hub* est précisément cette boîte à outils.**

À l'avenir, la procédure pourrait être la suivante :

- **d'une part**, l'activation du CDH, acte politique fort, devrait revêtir **un caractère solennel, par exemple par un article spécifique dans la loi proclamant l'état d'urgence sanitaire**. Ceci permettrait à la fois d'**obtenir une majorité claire** et de **fixer les limites** propres aux circonstances, en application du principe de proportionnalité (limitation dans le temps, dans la possibilité d'utiliser ou non certains outils, etc.) ;

---

[1] *En mai 2021, 69 % des Français souhaitaient se faire vacciner, contre seulement 45 % en décembre 2020. Ce chiffre reste toutefois très en deçà de la plupart des pays occidentaux (par exemple, 90 % des Britanniques et 78 % des Allemands souhaitent se faire vacciner). Source :* Kekst CNC Covid-19 Opinion Tracker, *8ème édition, 12 mai 2021 : https://www.kekstcnc.com/insights/covid-19-opinion-tracker-edition-8*

[2] *Au-delà des sondages régulièrement publiés à l'échelle nationale, l'étude* Kekst CNC Covid-19 Opinion Tracker *précitée permet de comparer différents pays, à partir d'un indicateur « net » de confiance (nombre de « confiance » – nombre de « pas confiance »). En France, le Président de la République a un score de confiance de -24 %, le Premier ministre de -26 %, et le Gouvernement de -20 %. Par contraste, au Royaume-Uni, le Premier ministre bénéficie d'un score de -4 % et le gouvernement de +2 %. En Allemagne, la Chancelière bénéficie d'un score de confiance de -1 %, les Länder de -1 % et le gouvernement fédéral de -12 %. Enfin, aux États-Unis, 32 % des citoyens font confiance au Président, 20 % au gouvernement fédéral, et 19 % aux États fédérés.*

- d'autre part, et en contrepartie de cette marge de manœuvre, la mise en œuvre de ces outils par l'exécutif ferait l'objet d'une **procédure *ad hoc* de contrôle en continu**, sans pour autant gêner sa réactivité. Ce contrôle, qui incombe d'abord au **Parlement**, pourrait prendre la forme d'une commission de suivi spécifique du CDH, dès l'instant où celui-ci est activé. La **CNIL** devrait aussi avoir les moyens – y compris matériels – de vérifier en continu le respect du cadre juridique qu'elle aura validé « par temps calme ».

Les citoyens et la société civile bénéficieraient aussi d'un tel système : parce que le *Crisis Data Hub* est *par construction* un agrégateur de données, il serait **beaucoup plus facile de prévoir une publication par défaut, en *open data*, des principaux indicateurs** – et beaucoup plus difficile, le cas échéant, de justifier un refus. Le débat démocratique s'en trouverait renforcé, les mesures légitimées, et le Gouvernement responsabilisé.

D. UNE EXPÉRIMENTATION POSSIBLE

La *scalabilité* propre aux outils numériques ne permet pas seulement une montée en charge rapide : elle est aussi **particulièrement propice à l'expérimentation**. Certains outils pourraient ainsi être testés, soit en période de crise, soit même en période de « veille », pour faire la « preuve du concept », facilitant ensuite, et en cas de besoin, leur généralisation.

Cette expérimentation pourrait d'abord se faire sur la base du **volontariat individuel**. On a trop négligé, dans la gestion de la crise du Covid-19, les avantages du ***crowdsourcing*** (ou production participative) et de ses extensions possibles : si beaucoup d'énergie a été dépensée pour *empêcher* l'identification des personnes et le croisement des données, **nombreux sont ceux qui, moins rétifs à l'égard du numérique, auraient été sans doute été heureux de pouvoir *volontairement* contribuer à la lutte contre la pandémie**, en donnant leur consentement éclairé à l'exploitation de leurs données pour faire avancer la recherche épidémiologique ou médicale, pour aider à mieux calibrer les mesures, ou tout simplement pour bénéficier, en échange, de contraintes allégées ou plus courtes. **Peut-être aurait-on pu, au minimum, le leur proposer ?**

L'expérimentation pourrait aussi être « **sectorielle** », et ne porter que sur certaines données ou certains outils dans un premier temps – c'est d'ailleurs l'esprit même du dispositif dans son ensemble. Le **dossier médical partagé (DMP)**, par exemple, pourrait avoir une place importante dans certains cas d'usage : une expérimentation pourrait concerner les Français qui en disposent déjà à ce jour.

Enfin, l'expérimentation pourrait être **locale** : de même que l'on peut imaginer des confinements ou des couvre-feux locaux, on peut imaginer **des outils numériques déployés à l'échelle locale**. Cela apparaît d'autant plus pertinent que **les collectivités territoriales pourraient être amenées à jour un rôle important dans certains cas de figure**, non seulement en tant que « producteurs » mais aussi en tant que « destinataires » des données, par exemple s'il s'agit de porter assistance à des personnes vulnérables isolées, d'adapter l'offre de mobilité, ou encore d'apporter un soutien ciblé à certains acteurs économiques ou activités culturelles. **La région Grand Est, particulièrement avancée dans le déploiement de la fibre optique**, pourrait même lancer des expérimentations plus poussées, par exemple avec la remontée d'informations issues d'objets connectés, permettant une véritable « télémédecine de crise ».

*

* *

Le présent rapport, quoi qu'il en soit, ne propose ou ne défend aucun outil numérique en particulier.

Il considère, précisément, que de tels choix abstraits n'ont guère de sens, et que le recours à une technologie ou à une autre doit s'apprécier au cas par cas, en fonction de la situation, et au regard des restrictions apportées aux libertés « physiques ». **En revanche, il est nécessaire de nous préparer dès maintenant à toutes les possibilités**, car nul ne sait de quoi seront faites les prochaines crises. **Si nous ne nous préparons pas, nous ne pourrons que subir –** subir les conséquences d'une crise sans avoir les outils pour la combattre, ou subir ces outils que d'autres auront développés à notre place, sans pouvoir alors défendre nos valeurs.

EXAMEN EN DÉLÉGATION

I. RÉUNION DU JEUDI 6 MAI 2021

M. Mathieu Darnaud, président. – Je suis très heureux de vous retrouver ce matin, physiquement ou à distance, pour l'examen du rapport de nos collègues Véronique Guillotin, Christine Lavarde et René-Paul Savary consacré aux outils numériques dans la prévention et la gestion des pandémies. Ce rapport est attendu. Il s'inscrit dans la suite de deux précédents rapports de la délégation sur les pandémies : d'abord, un rapport de Fabienne Keller de juillet 2012 intitulé « *Les nouvelles menaces des maladies infectieuses émergentes* », qui avait identifié dix leviers d'action pour lutter contre les nouvelles menaces liées à ces maladies. Puis, trois ans plus tard, en mai 2015, un rapport de Fabienne Keller et Roger Karoutchi intitulé « *Mieux prévenir et gérer les crises liées aux maladies infectieuses émergentes* ». Le premier de ces rapports s'inscrivait dans le contexte de la sortie de l'épidémie de grippe H1N1, le second dans celui de l'épidémie d'Ebola.

En juillet dernier, Christine Lavarde nous avait indiqué qu'elle souhaitait actualiser ces rapports et surtout regarder si les enseignements que la délégation avait alors essayé de tirer de ces pandémies avaient été, pour partie au moins, suivis. Elle a été rejointe cet automne par Véronique Guillotin et René-Paul Savary. Je sais qu'ils ont ensemble mené de nombreuses auditions et je les en remercie. Vos investigations vous ont conduits à approfondir la question de l'utilisation des outils numériques dans la gestion des pandémies. C'est évidemment une question centrale, comme on l'a vu lors de l'audition sur le système de crédit social en Chine, ou comme on le perçoit dans le cadre du débat actuel sur le passeport ou pass sanitaire.

Je sais que votre rapport est à la fois riche et dense. C'est donc sans plus tarder que je vous donne la parole.

M. René-Paul Savary, rapporteur. – En mai dernier, il y a un an, 25 000 personnes étaient mortes du Covid-19 en France : on n'avait pas alors de mots assez durs, ou assez condescendants, pour toutes ces « dictatures numériques » qui, en Asie, prétendaient lutter contre le virus avec des technologies « liberticides ». La Commission nationale de l'informatique et des libertés (CNIL) nous mettait en garde contre les dangers du passeport sanitaire, ce « totem à risques ». En décembre, nous en étions à 60 000 morts, et la France se déclarait opposée à la proposition faite par nos partenaires européens, estimant que « *la liberté de circulation des personnes ne devrait pas être conditionnée à un certificat* » (Jérôme Salomon). Fin janvier, 80 000 morts, c'était encore « *un débat qui n'a pas lieu d'être* » (Jean Castex), un dispositif « *injuste et paradoxal* », qui « *créé une société à deux vitesses* » (Clément Beaune).

Quatre mois plus tard, et passé le seuil de 100 000 morts, la France toujours confinée devenait le premier pays européen à mettre en place un « certificat vert » pour voyager, et faisait du « pass sanitaire » l'un des piliers de sa stratégie de déconfinement. Le Président de la République estime aujourd'hui qu'il serait « *absurde de ne pas l'utiliser* » dans les lieux de brassage, tout en affirmant dans la même phrase que, pour les lieux de la vie de tous les jours, « *le pass sanitaire ne sera jamais un droit d'accès qui différencie les Français* ». « *Jamais* »… jusqu'à la prochaine fois ?

On pourrait multiplier les exemples de tels revirements. Quand il s'agit de masques ou de vaccination, cela peut à la limite s'expliquer par l'évolution des connaissances scientifiques, ou tout simplement par la gestion de la pénurie. Mais quand il s'agit d'outils numériques, et donc de données personnelles et de vie privée, tout devient instantanément une affaire de grands principes, de « valeurs universelles » non négociables, de « lignes rouges » absolues. Souvenons-nous des polémiques sur *TousAntiCovid* : la technique ne fait pas bon ménage avec les tabous. Or, si cette crise doit nous apprendre une chose, c'est bien qu'il faut savoir faire preuve d'humilité. À quoi bon invoquer des « lignes rouges », si c'est pour les franchir quelques semaines plus tard, parfois quelques semaines trop tard ?

La situation actuelle n'est tout simplement plus tenable : face à une crise qui a déjà causé plus de 100 000 morts et la plus grande récession économique en temps de paix, nous sommes soumis à des restrictions dont l'effet est désastreux sur nos entreprises, nos libertés individuelles, notre santé mentale et psychique, et qui sont de moins en moins supportées par nos concitoyens. Or tous les spécialistes s'accordent à dire que cette crise n'est ni la dernière, ni sans doute la plus grave des années à venir.

Il faut absolument trouver les moyens de ne pas reconfiner chroniquement le pays et la société. Pour cela, notre rapport propose d'utiliser bien plus fortement les possibilités du numérique, en assumant des mesures plus intrusives mais aussi plus courtes et plus ciblées, en échange d'une liberté retrouvée plus vite dans le « monde réel ».

Nous assumons de dire que le refus de la France, et plus largement des pays occidentaux, de considérer sérieusement ces options a coûté des vies humaines, et que loin de protéger nos libertés, il a conduit à les restreindre bien au-delà du nécessaire.

Le sujet sensible concerne bien sûr l'utilisation des outils numériques pour contrôler le respect des mesures sanitaires au niveau individuel, dans une logique qui tient plus de l'ordre public que du soin médical. Je laisse ici de côté son rôle – majeur – dans la continuité de la vie économique et sociale (télétravail, école à la maison…) et dans la recherche scientifique.

Il n'y a malheureusement pas de mystère : plus les outils sont intrusifs, plus ils sont efficaces. Face à cet arbitrage, certains pays, notamment asiatiques, n'ont pas hésité longtemps. Leur exemple, à défaut d'être directement transposable, est instructif.

En Chine, un « code couleur » en fonction de l'immunité conditionne l'accès à certains lieux, les cas positifs sont géolocalisés sur une carte, et chacun peut enquêter directement sur trois individus. Tout passe par les incontournables applications *WeChat* et *AliPay*. À Taïwan, les données médicales sont croisées avec les fichiers de la police aux frontières et des entreprises de transport. À Singapour, l'utilisation de l'application *TraceTogether*, la première du genre, est obligatoire. Les enquêtes sont très intrusives, reposent sur la collaboration des hôtels et des entreprises, et s'appuient volontiers sur la vidéosurveillance. À Hong Kong, les personnes en quarantaine doivent porter un bracelet électronique, et la police n'hésite pas à intervenir. En Corée du Sud, les autorités utilisent toutes les données disponibles, y compris bancaires, et le voisinage est alerté par SMS de la présence des cas confirmés. Au début, leur identité et leur localisation précises étaient rendues publiques.

C'est intrusif et liberticide, oui, mais ça marche. Ces pays ont la plus faible mortalité du monde : avec 12 décès seulement, Taïwan compte 3,5 morts par million d'habitants, au 3e rang mondial, suivi de peu par la Chine (6e rang) puis Singapour (10e rang, avec 31 décès, soit 5,5 morts par million d'habitants). Tout en bas du tableau, on trouve la France, au 136e rang mondial sur 155, avec 1 573 morts par million d'habitants, non loin des États-Unis (142e) et du Brésil (146e).

On peut douter des chiffres officiels de la Chine, mais pas de ceux de Taïwan, de Singapour ou de la Corée du Sud. Or, même en tenant compte de tous les autres facteurs possibles – démographie, insularité, urbanisation, génétique… –, il est impossible d'expliquer de tels résultats sans reconnaître le rôle majeur joué par les outils numériques.

C'est peu dire que la France ne s'est pas donné les mêmes moyens de réussir. Notre propos n'est pas de dire qu'il aurait fallu tout faire comme la Chine, ni de nier les facteurs politiques et culturels qui conditionnent l'acceptabilité de telles mesures, ni de les présenter à elles seules comme des solutions miracle. Par contre, nous regrettons que la France ne se soit pas posé la question de l'opportunité de certains dispositifs, adaptés à notre contexte et assortis de garanties démocratiques. Sans faire de politique fiction, on peut imaginer toute une gamme de mesures proportionnées à la gravité de la situation.

Dans un cas extrême, les données médicales d'un individu positif pourraient être croisées avec ses données de géolocalisation, et en cas de violation de sa quarantaine, conduire à une information des forces de l'ordre, ou, par exemple, à une désactivation de ses moyens de paiement ou à une

amende automatiquement prélevée sur son compte bancaire : c'est la garantie d'une épidémie stoppée en une semaine. Et l'individualisation permise par le numérique permettrait de limiter les mesures aux seules personnes à risque, plutôt que de confiner à l'aveugle un pays tout entier.

Dans la gamme des mesures les moins intrusives, on pourrait par exemple imaginer l'envoi automatique d'un SMS à toute personne qui s'éloignerait de son domicile pendant le couvre-feu, à simple titre de rappel, sans transmettre aucune donnée. Techniquement, les opérateurs nous ont confirmé qu'il n'y avait pas de difficulté. Bref, il s'agit de se donner les moyens de réagir dans une logique de riposte graduée.

Tout cela peut faire peur, j'en conviens, et l'on peut à bon droit se demander si la crise du Covid-19, pour grave qu'elle soit, mérite d'aller jusque-là. À cela, je répondrai deux choses. D'une part, il faut se préparer au pire, et s'il y a un endroit pour le faire, c'est bien à la délégation à la prospective. Rien ne garantit que la prochaine épidémie ne sera pas beaucoup plus grave que le Covid-19, qui, rappelons-le, a un taux de létalité relativement faible, autour de 1 %. Qu'en sera-t-il si, demain, nous étions frappés par une maladie plus virulente, ou qui touche en priorité nos forces vives et notre jeunesse, comme ce fut le cas avec la grippe espagnole, avec ses 100 millions de morts (5 % de l'humanité) et son taux de létalité de 3 % ?

D'autre part, si nous ne nous préparons pas, d'autres le feront à notre place. Veut-on défendre nos « valeurs démocratiques » ? Ce n'est certainement pas en laissant les régimes les plus autoritaires prendre une avance décisive en ce domaine, ou en abandonnant aux GAFAM (Google, Amazon, Facebook, Apple, Microsoft) le soin de lutter contre les épidémies (et quoi d'autre demain ?), que nous règlerons le problème.

Mme Véronique Guillotin, rapporteure. – Tout cela permet de mesurer à quel point la France est restée en retrait, tout au long de cette crise, sur la question des outils numériques. En retrait non seulement par rapport à la stratégie des pays asiatiques, mais aussi par rapport aux possibilités des technologies actuelles, sans même parler de celles, vertigineuses, des technologies de demain. Que s'est-il passé ? Il faut, en réalité, distinguer deux types de raisons : des raisons techniques et matérielles d'une part, et des raisons plus politiques et idéologiques, d'autre part.

S'agissant des raisons techniques, les choses sont simples : nous n'étions tout simplement pas prêts à affronter une telle crise, faute d'avoir conduit auparavant les efforts de modernisation de nos systèmes d'information.

Il a donc fallu improviser. D'abord, pour gérer le flux de malades arrivant dans les hôpitaux, le fichier SI-VIC, initialement conçu pour prendre en charge les victimes d'attentats terroristes, a été adapté en urgence à l'ampleur de la crise. Ensuite, dans le cadre de la stratégie « Tester, alerter,

protéger », deux fichiers ont été spécialement créés : SI-DEP pour les tests de dépistage, et *Contact-COVID* pour la réalisation des enquêtes sanitaires. Enfin, depuis le début de l'année, le fichier *Vaccin Covid* permet de suivre la campagne de vaccination au niveau national.

Commençons par l'aspect positif : dans ces circonstances difficiles, la France a su faire preuve d'une grande réactivité. Le fichier SI-DEP, en particulier, a été développé en moins d'un mois, alors qu'un projet identique porté par Santé Publique France était bloqué depuis 8 ans… Il n'y a pas de secret : avec de la volonté politique, une gouvernance forte et des financements à la hauteur, ça marche ! Bien sûr, ces fichiers ont connu des débuts un peu chaotiques, avec des remontées concurrentes voire contradictoires, et un vrai problème du côté des EHPAD, dont le retard en matière d'informatisation est alarmant. Mais de nombreux pays ont connu des « ratages » – au Royaume-Uni, par exemple, la remontée des données s'arrêtait à cause du nombre limité de lignes sur les tableurs *Excel* !

Sauf que – voilà l'aspect négatif – tout cela ne suffit pas. Avec des fichiers *ad hoc* créés dans l'urgence, on peut faire des statistiques pour voir l'étendue des dégâts, on peut décider de confiner telle région ou de vacciner telle classe d'âge, mais pour briser les chaînes de contamination et sauver des vies, c'est autre chose… En effet, ces fichiers ne sont pas interconnectés – ni avec le reste du système de santé, ni même entre eux ! Résultat : impossible de savoir, par exemple, si les « cas contacts » d'une personne ont été effectivement contaminés, ou s'ils sont vaccinés. Impossible, aussi, de savoir s'ils courent un risque particulier (maladie, comorbidité, etc.), faute de pouvoir accéder à leur dossier médical. Nous avons mobilisé des milliers d'agents au sein des « brigades de traçage » pour passer des appels téléphoniques et effectuer des visites à domicile, mais la réalité, c'est qu'au lieu de briser les chaînes de contamination, ils étaient condamnés à jouer aux devinettes avec le premier maillon.

Dans tout cela, des acteurs indispensables ont été exclus de la circulation des informations – je pense notamment aux collectivités locales, dont on a tant vanté, pourtant, le rôle dans cette crise.

Devant les défaillances du système public, des acteurs privés, au sein de la société civile notamment, ont parfois pris le relais au pied levé. Toutes ces initiatives témoignent d'un véritable dynamisme dont il faut se féliciter – mais enfin, est-il bien normal que l'État soit incapable de produire des chiffres fiables, quand un informaticien de 24 ans – avec le site *CovidTracker* – peut le faire, avec en prime des outils de visualisation performants ? Est-il normal que des initiatives comme *CovidListe* ou *ViteMaDose* fassent davantage pour éviter les doses perdues que les services des ARS ou de l'Assurance maladie ?

Voilà pour ce qui s'est passé. D'où cette grande question : aurait-on pu faire mieux si nous avions disposé des bons outils ? La réponse est très claire : oui. À vrai dire, peut-être même s'en est-il fallu de quelques années à peine pour qu'on dispose d'outils autrement plus efficaces dans ce genre de situations. En effet, un tournant majeur a eu lieu en 2019, avec la reprise en main du chantier du numérique en santé, dont la crise a brutalement rappelé la nécessité et, sans doute, accéléré le rythme.

Un petit détour s'impose pour bien le comprendre : les pays dont le système de santé est organisé autour d'une « plateforme », où chaque usager dispose d'un identifiant unique et où tous les services sont liés entre eux, ont disposé d'un atout précieux face à la crise sanitaire. Modèle du genre, l'Estonie a par exemple pu déployer très rapidement de nombreux services spécifiquement liés à la crise (outils de diagnostic, suivi du parcours de soin, coordination de la campagne de dépistage et de vaccination, etc.), et cela se retrouve dans les statistiques de cas et de décès, très inférieurs à ceux de ses voisins baltes. Plus généralement, ce modèle de « plateforme » simplifie drastiquement les échanges de données entre professionnels et avec l'usager, au bénéfice direct de sa santé.

C'est précisément l'objectif poursuivi en France, mais cet immense chantier s'est longtemps heurté à la complexité de l'existant, à l'éclatement des acteurs, au poids de l'histoire. Très concrètement, trois outils principaux auraient pu changer la donne, s'ils avaient été déployés lorsque la crise est arrivée.

Premier outil : l'espace numérique de santé (ENS), et sa pierre angulaire qu'est le dossier médical partagé (DMP), un chantier mille fois enterré et mille fois relancé depuis… 2004. Avec le DMP, il aurait été possible de faire un traçage efficace, en ayant au même non seulement les données de SI-DEP, *Contact-COVID* et *Vaccin Covid*, mais aussi tout l'historique médical du patient, avec ses facteurs de risque et ses comorbidités. Nous aurions aussi disposé d'une messagerie sécurisée, d'une application de prise de rendez-vous pour les tests et les vaccins, et d'un outil de e-prescription. Enfin, grâce au catalogue d'applications tierces, d'autres acteurs auraient pu proposer leurs solutions : téléconsultation et télésuivi, données d'objets connectés (poids, ECG, etc.).

Deuxième outil : l'identifiant national de santé (INS). Aujourd'hui, nous sommes tous associés à une multitude d'identifiants « locaux », à l'hôpital, chez le généraliste, chez le dentiste, au laboratoire, etc., sources de multiples erreurs et de démarches administratives au détriment du « temps médical ». En temps de crise, alors que les hôpitaux sont surchargés, les conséquences peuvent être dramatiques. Le paradoxe, c'est que tout le monde dispose pourtant d'un numéro unique et fiable, le numéro de Sécurité sociale, mais la CNIL s'est toujours opposée à son utilisation dans le domaine de la santé, sans même parler des autres domaines, au nom de la protection de la vie privée. Ce n'est qu'en 2019 que la loi Santé a permis

d'utiliser le NIR comme base de l'INS, mais les choses prennent du temps et son utilisation, en théorie obligatoire depuis le 1er janvier, est encore loin d'être généralisée.

Troisième outil : le *Health Data Hub*. L'enjeu ici est celui de l'exploitation des données agrégées et pseudonymisées, à des fins de recherches médicale et épidémiologique. Créé en 2019, le *Health Data Hub* est un outil très prometteur, qui fera de la France un pays *leader* en la matière. Son intérêt dans le cadre d'une crise comme celle du Covid-19 est évident, et quelques projets de recherche ont d'ailleurs bénéficié d'un accès aux premières bases disponibles. Mais le *Health Data Hub* n'en est qu'à ses balbutiements, et à vrai dire, on a surtout parlé jusqu'à maintenant en raison de l'opposition de la CNIL, qui conteste l'hébergement par Microsoft – hébergement temporaire, de certaines données seulement, et de façon toujours anonyme, mais c'était visiblement une question de principe.

Ceci m'amène à la deuxième grande raison du retard de la France, sans doute beaucoup plus fondamentale que les aspects techniques qui n'en sont que la conséquence : sa profonde défiance à l'égard du numérique dès lors que cela implique l'État ou des pouvoirs publics. On l'a vu avec *StopCovid*, devenu *TousAntiCovid*, qui constitue un cas d'école des contradictions françaises à l'égard du numérique : en refusant de choisir entre efficacité et confidentialité, nous n'avons pas eu la première, sans pour autant mieux protéger la seconde, et nous avons finalement perdu sur les deux tableaux.

Au nom de ses « valeurs » et de la préservation de l'anonymat, la France a fait le choix isolé d'une architecture dite « centralisée », fondée sur le protocole ROBERT développé par l'Institut national de recherche en sciences et technologies du numérique (Inria), tandis que la quasi-totalité des autres pays optaient pour le protocole « décentralisé » d'Apple et Google.

Or, en réalité, le protocole centralisé ne protège pas mieux l'anonymat : la solution décentralisée est tout aussi sécurisée, si ce n'est davantage. L'argument tient du prétexte, et la France, lâchée par ses partenaires européens, semble surtout s'être obstinée dans sa volonté d'afficher une solution « souveraine » à tout prix. Par contre, le protocole centralisé a privé l'application française d'une grande partie de son efficacité, en lui coupant l'accès au *Bluetooth* des *iPhone* d'une part, et en lui interdisant toute interopérabilité avec les autres applications d'autre part, face à une pandémie qui requiert précisément une réponse coordonnée.

Comme si cela ne suffisait pas, l'application est peu utilisée : 1,7 million de téléchargements de *StopCovid* un mois après son lancement, soit 2 % de la population, quand l'Allemagne en était à 6 millions en moins de deux jours. Sa transformation en *TousAntiCovid* n'a rien changé sur le fond, mais a permis de rattraper une partie du retard, grâce à des fonctionnalités plus interactives. 20 % de la population l'a désormais

téléchargée, ce qui reste loin des 30 % de l'Allemagne ou du Royaume-Uni. Mais encore faut-il ensuite l'utiliser, et surtout jouer le jeu – or seules 4,5 % des personnes déclarées positives dans SI-DEP se sont effectivement signalées dans *TousAntiCovid*… Doit-on s'étonner, dans ces conditions, que *TousAntiCovid* n'ait permis d'envoyer que 172 000 notifications (soit à 1 % de la population française), quand l'équivalent britannique, qui utilise le protocole d'Apple et Google, a déjà permis d'avertir 8 % de la population (1,7 million de notifications) ?

Mais au fond, ces comparaisons n'ont qu'un intérêt limité. En effet, toutes ces applications ont un point commun : le choix, par les pays occidentaux, de s'en tenir à des dispositifs strictement volontaires et strictement anonymes, quitte à ce qu'ils restent largement inefficaces. C'est bien à ce problème que nous avons essayé d'apporter une réponse.

Mme Christine Lavarde, rapporteur. – Avant d'en venir à notre proposition, je souhaiterais revenir un instant sur le rôle de la CNIL, car cette question est revenue constamment au fil de nos auditions. Nombre des obstacles évoqués par Véronique Guillotin découlent très directement de sa doctrine très conservatrice en matière de croisements de fichiers : ce ne sont pas des raisons techniques, mais bien des obstacles juridiques, qui ont empêché de croiser les fichiers SI-DEP, *Contact-COVID* et *Vaccin Covid*. C'est bien elle qui a, en 2007, refusé l'utilisation du numéro de Sécurité sociale pour accéder au DMP, et qui freine toujours la mise en place d'une identité numérique unique permettant d'accéder à l'ensemble des services publics, pourtant condition *sine qua non* de l'État-plateforme.

On pourrait ajouter, entre autres exemples, son opposition à l'utilisation par la RATP de caméras de détection du port du masque, au motif qu'il s'agirait de données biométriques permettant l'identification des individus… alors même que ces caméras ne renvoient rien d'autre que des statistiques.

Soyons clairs : il ne s'agit pas ici de remettre en cause le cadre juridique de la protection des données personnelles, fixé aujourd'hui par le règlement général sur la protection des données (RGPD). En revanche, on peut légitimement s'interroger sur l'interprétation qu'en fait la CNIL, beaucoup plus conservatrice que chez nos voisins européens. D'autant que cette interprétation s'appuie parfois sur des raisonnements curieux : par exemple, les caméras thermiques ne seraient pas justifiées pour détecter les malades du Covid-19, au motif que la fièvre n'est pas un symptôme systématique. Autrement dit, la CNIL préfère ne détecter personne plutôt que de ne pas détecter tout le monde… Mais dans une crise sanitaire, tout cas détecté est une victoire contre la maladie !

Plus généralement, nous pensons qu'il faut avoir le courage de s'attaquer à ce tabou français qu'est la collecte de données par l'État. La sensibilité française sur le sujet est ancienne et profonde, et doit être prise au

sérieux. Elle n'est pas dénuée de toute justification historique, de « l'affaire des fiches » qui fit chuter un gouvernement en 1904 aux abus du régime de Vichy, pour ne citer que ces deux exemples. Dans l'imaginaire collectif, la collecte des données est associée à l'idée d'un État policier et d'un « fichage » de la population, et c'est cette même idée qu'on retrouve à chaque fois que les gouvernements successifs souhaitent avancer sur le sujet, du fichier SAFARI en 1974 à *TousAntiCovid*.

Mais à l'heure de la révolution numérique, du *big data* et de l'intelligence artificielle (IA), on ne peut plus raisonnablement soutenir que le seul intérêt des croisements de fichiers est l'instauration d'un État totalitaire ! Or la crise a montré que cette idée pouvait s'avérer coûteuse – en vies humaines, en libertés publiques, en croissance économique –, d'autant qu'elle repose en réalité sur un certain nombre de fantasmes et d'incompréhensions qu'il est temps de lever.

Tout d'abord, cette méfiance apparaît de plus en plus décalée, pour ne pas dire absurde, à l'heure où les géants du numérique accumulent sur chacun d'entre nous bien plus de données que l'État n'en aura jamais, pour des finalités qui n'ont rien n'à voir avec l'intérêt général, et sans aucune des garanties qu'offre le contrôle démocratique.

Ensuite, l'excuse des « dictatures », souvent entendue pendant l'a crise, est un peu trop facile. D'une part, c'est faux – sauf à démontrer que le Japon, la Corée du Sud, l'Estonie ou Israël sont des dictatures. Bien sûr, les dérives sont réelles, et notre audition de février sur le « crédit social » en Chine l'a montré. Mais les abus ne tiennent pas aux technologies elles-mêmes, ils tiennent à l'usage qui en est fait, à l'absence de contre-pouvoirs notamment. D'autre part, tout ceci n'est pas le problème : si une « dictature » sauve des vies pendant qu'une « démocratie » pleure ses morts, il y a sans doute d'autres questions à se poser.

Enfin, cette conception repose sur une confusion entre les fins (protéger la vie privée) et les moyens (interdire les croisements de fichiers). Dans les années 1970, il n'était pas absurde de raisonner ainsi : c'était encore la meilleure garantie possible, à une époque où on était bien loin, par ailleurs, d'imaginer les bénéfices immenses qu'apporterait la révolution numérique. Mais aujourd'hui, les choses sont différentes : il existe bien d'autres façons de garantir la confidentialité des données sans pour autant s'interdire de les utiliser, comme par exemple la *blockchain* ou l'*open source*, qui sont au cœur des applications de *contact tracing*. En somme, tout se passe comme si nous avions une préférence pour l'inefficacité.

Revenons aux outils permettant de lutter contre l'épidémie. Tout le monde est d'accord sur un point : il s'agit d'une affaire de proportionnalité. Mais est-elle vraiment bien comprise ? Quand on impose des restrictions à un individu pendant une crise sanitaire, ce n'est pas seulement pour le protéger lui, c'est pour protéger toute la société. De plus, les atteintes portées

aux libertés « numériques » par certains outils de lutte contre la pandémie doivent être comparées aux atteintes portées aux libertés « physiques », qui sont bien plus lourdes, durent bien plus longtemps et s'appliquent à tous de manière aveugle. Elles sont aussi bien plus difficiles à faire respecter et *in fine* moins efficaces.

C'est dans cet esprit que nous avons mené nos travaux. Plutôt que de formuler 50 ou 60 propositions, nous avons choisi d'en retenir une seule, pragmatique, qui permette de répondre efficacement aux futures crises sanitaires – et qui ne fasse que cela. Elle est complémentaire des chantiers plus généraux, de plus longue haleine, qu'il faut continuer à mener avec détermination, en gagnant la confiance des citoyens : le numérique en santé, l'identité numérique, l'État-plateforme.

Résumons le problème : si nous voulons sauver des vies humaines et éviter de mettre la vie économique et sociale sous cloche à chaque nouvelle crise, il faudra inévitablement s'appuyer sur des croisements de données massifs et dérogatoires. Sauf que les données en question sont soit des données personnelles qu'il est inconcevable d'exploiter en temps « normal » (par exemple des données médicales croisées avec des données de géolocalisation), soit des données produites par des entreprises privées (opérateurs télécom, entreprises technologiques, entreprises de transport, établissements financiers, etc.) qui n'ont aucune raison ni obligation de les fournir par ailleurs, ni même de s'y préparer.

Notre proposition consiste donc non pas à collecter ces données, mais à nous mettre en capacité de le faire, en appuyant sur un bouton, si jamais les circonstances devaient l'exiger. Concrètement, cela passe par la mise en place d'une plateforme sécurisée spécifique, qui ne serait activée qu'en temps de crise, et qui permettrait de centraliser les données utiles avant de les redistribuer aux acteurs concernés selon leurs missions : établissements de santé, sécurité civile voire forces de l'ordre, collectivités locales, transports publics, prestataires privés, etc.

Nous appelons cela le « *Crisis Data Hub* », sur le modèle du *Health Data Hub*. La différence est que le *Health Data Hub* ne centralise que des données médicales et pseudonymisées mais qu'il le fait massivement et en permanence, tandis que le *Crisis Data Hub* collecterait des données plus diverses et nominatives, mais sur un champ plus restreint et surtout pendant une période limitée. Une autre image est celle du « poste de contrôle » ou de « gestion de crise », celui qu'on voit dans les films avec tous ces écrans allumés, mais qui n'existe pas dans la réalité – ou en tout cas pas dans le domaine sanitaire, sinon nous n'en serions pas là. En somme, le *Crisis Data Hub* est à la gestion numérique de la crise ce que l'Établissement de préparation et de réponse aux urgences sanitaires (EPRUS) aurait dû être à la gestion logistique de la crise, si cet établissement public créé au lendemain de l'épidémie de H1N1 n'avait pas été dissous en 2016.

Sur le plan technique, la mise en place de cette plateforme implique d'investir dans une solution d'hébergement sécurisée, un *cloud* souverain qui pourrait instantanément monter en capacité. Sur le plan juridique, notre proposition se traduirait par une obligation légale, pour certaines entreprises et administrations, de maintenir des bases de données dont le contenu et le format seraient fixés à l'avance, et de se tenir prêtes à les « brancher » à la plateforme en cas de nécessité, c'est-à-dire sur réquisition au titre de l'état d'urgence sanitaire. En temps « normal », aucune donnée ne serait bien sûr transmise, mais le système serait prêt, grâce à un travail continu de maintenance et d'amélioration.

Pour fixer la liste des acteurs concernés, nous pourrions nous inspirer de celle des 250 « opérateurs d'importance vitale » (OIV), soumis à des obligations particulières et accompagnés par l'Agence nationale de cybersécurité (ANSSI).

Nous sommes conscients de toutes les craintes et interrogations qu'une telle proposition soulève. Mais une fois de plus : rien n'est pire que l'improvisation, qui est à la fois inefficace et potentiellement bien plus attentatoire aux libertés individuelles. Se préparer en amont à collecter des données ne veut pas dire qu'on va forcément le faire, ni, le cas échéant, que toutes les possibilités seront utilisées. Nous proposons bien un dispositif de riposte graduée.

Par contre, se préparer en amont permet de créer les conditions de la confiance, en prenant le temps d'expliquer le dispositif aux citoyens, et en le soumettant au Parlement. D'ailleurs, en cas de crise, l'activation de tout ou partie du dispositif pourrait prendre une forme solennelle, par l'adoption d'un article dédié dans la loi instituant l'état d'urgence, qui marquerait clairement le soutien – ou le refus – de ces mesures.

Très bien, dira-t-on, mais comment peut-on avoir la garantie que les données ne seront pas utilisées de manière abusive ? C'est le dernier grand avantage de notre proposition : le *Crisis Data Hub* peut être développé en *open source*. Faisons confiance à la société civile pour examiner chaque ligne de code dans les moindres détails, chaque champ, chaque base de données, pour être bien sûrs que ce dispositif ne fait rien d'autre que tenir sa promesse : sauver des vies, sans condamner le pays.

M. Mathieu Darnaud, président. – Merci pour la richesse de vos travaux et la clarté de votre propos, quand bien même il pourrait susciter des critiques. Faute de nous inciter à l'allégresse ou l'insouciance, votre rapport nous éclaire sur ce que pourrait être un système efficace et efficient de prévention des crises sanitaires. Avant de passer la parole à mes collègues, j'aimerais vous demander si vous pensez que, dans la période que nous venons de vivre, marquée par l'échec assez cinglant des applications comme *StopCovid* puis *TousAntiCovid*, montrant que nous n'avons pas été en mesure d'utiliser le numérique pour lutter efficacement contre la crise sanitaire, les

mesures que vous proposez, notamment la mise en place d'un *cloud* souverain qui collecterait les données de santé, auraient pu rassurer nos concitoyens, inquiets de possibles entraves aux libertés publiques ?

M. Alain Richard. – Je suis favorable à la proposition des rapporteurs. Toutefois, j'ai participé aux travaux de rédaction de la loi de 1978 qui a créé la CNIL et j'ai retrouvé ce texte quand je suis entré au Parlement. On craignait alors les effets sur les libertés publiques des croisements de fichiers. Cette crainte reste encore forte en France, même si celle-ci est largement alimentée par l'incompréhension et l'ignorance. Le Sénat a toujours marqué son attachement à une protection forte des libertés individuelles. Les propositions des rapporteurs contrastent avec les positions traditionnelles du Sénat. Je suggère donc que le rapport prenne en compte cette difficulté en apportant des arguments solides. La délégation à la prospective ne doit pas être en position de vulnérabilité sur ce sujet. Nous pouvons aussi partager certaines positions avec le Gouvernement sur la question. Les rapporteurs ont effectué un très bon travail, avec des éléments de réflexion particulièrement justifiés mais il faudra convaincre.

M. Jean-Raymond Hugonet. – Merci aux rapporteurs pour leur travail très intéressant. Je m'associe aux propos d'Alain Richard. Il me semble qu'un élément manque à l'analyse, qui ne doit rien à l'intelligence artificielle ou à la vaccination, mais relève plutôt d'un problème philosophique. Par rapport à la mortalité enregistrée dans les autres pays européens, la France n'a pas à rougir dans la crise actuelle. Souvenons-nous aussi que le cancer fait 150 000 morts par an en France, comme les maladies cardiovasculaires. La gestion de la crise sanitaire actuelle pose la question très profonde du rapport entre efficacité et liberté. En France, nous sommes attachés à la liberté. Mais depuis plus d'un an, nous vivons cette liberté selon un mode dégradé. Le Président de la République a parlé à tort de guerre. Nous ne sommes pas en guerre, mais nous ne connaissons pas la même situation qu'avant. Faut-il pour autant se résoudre à ce que, selon votre formule abrupte mais juste, « *les dictatures sauvent des vies et les démocraties comptent leurs morts* » ? Le peuple français, pourtant de tradition révolutionnaire, a accepté les restrictions imposées par une législation d'urgence. Dans un tel contexte, devrions-nous rester arc-boutés sur les principes édictés par la CNIL ? Cela a peu de sens. Il y a certainement une voie médiane entre la dictature qui sauverait des vies, mais dans laquelle aucun d'entre nous ne veut vivre et les positions caricaturales de la CNIL. Avant de rendre publiques vos propositions, nous devons faire preuve de prudence dans les formulations sans oublier d'élargir la réflexion à sa dimension philosophique.

M. Bernard Fialaire. – Je m'associe aux félicitations adressées aux rapporteurs. J'ai quelques interrogations. Des études ont-elles été menées sur le comportement de la presse et des médias dans les différents pays lors de la crise sanitaire ? Les médias servent-ils à apporter de l'information ou à insister sur les mauvaises nouvelles et les craintes qui apportent plus

d'audience et donc plus de recettes ? Par ailleurs, on dit souvent qu'il n'y a rien de pire que l'improvisation. C'est inexact. Il faut de la réactivité face à l'imprévu. On a rarement le bon outil à l'avance. Or, avec le principe de précaution, nous risquons fort de ne plus disposer de suffisamment de réactivité. Pendant longtemps, notre pays a été à la pointe du « système D », avec de petits moyens mais une grande efficacité. Je ne suis pas sûr que ce soit encore notre culture. Enfin, la réflexion sur la réponse à la crise sanitaire s'inscrit pleinement dans le débat entre sécurité et liberté. Appliqué aux EHPAD, ce débat est redoutable. Aurait-on envie de vivre dans un univers ultra-sécurisé, avec des caméras partout, des portes qui s'ouvrent automatiquement, en restant passifs ? On en arrive à attacher les gens au nom de la sécurité pour ne pas qu'ils tombent et ne puissent plus demain se déplacer. En conséquence, on leur ôte la possibilité de se déplacer. Quel paradoxe ! Ce débat entre liberté et sécurité doit avoir lieu mais la liberté, c'est aussi la responsabilité pour soi et pour les autres. L'épidémie pose ces questions avec beaucoup d'acuité. Enfin, une difficulté que nous rencontrons dans la crise tient à ce que certains acteurs ont déjà préparé des solutions numériques : les GAFAM ont pris de l'avance et sont prêts à profiter de l'opportunité offerte par cette crise pour renforcer leurs positions.

M. Éric Bocquet. – Le rapport s'appuie sur les précédents rapports de 2012 et 2015. Quels en étaient les préconisations et celles-ci ont-elles été suivies d'effets ? Le rapport pose plus globalement la question de l'emprise du numérique sur nos sociétés contemporaines. Facebook a chamboulé l'histoire. Il y a 2,8 milliards d'utilisateurs dans le monde, soit un tiers de l'humanité. Jamais une entreprise n'avait disposé d'un tel pouvoir, qui touche au politique. On a ainsi pu mettre en avant le rôle du numérique dans l'élection de Donald Trump aux États-Unis en 2016. Je suis réservé sur les propositions formulées par les rapporteurs. On vit clairement dans une société très différente de celle d'il y a 15 ou 20 ans. On parle de garanties démocratiques, mais quelles sont-elles, même dans un système en *open source* ? Qu'entend-on exactement à travers la notion de *cloud* souverain ? Qui sera le vrai souverain sur le stockage de données des uns et des autres ?

M. Mathieu Darnaud, président. – Avant de laisser répondre les rapporteurs, j'indique partager les précautions demandées par Alain Richard et Jean-Raymond Hugonet. Ce rapport comporte une analyse claire et sans ambiguïté et fait des propositions concrètes en prenant à bras le corps la question de la souveraineté numérique, menacée par les GAFAM et les BATX (Baidu, Alibaba, Tencent, Xiaomi, autrement dit les GAFAM chinois). Il est nécessaire que vos propositions soient amenées avec une argumentation solide, s'appuyant sur la richesse de vos travaux, pour ne pas venir heurter les consciences. Je pense aussi que l'anticipation et la préparation, d'une part, et la réactivité, d'autre part, ne sont pas incompatibles. Mais la précipitation, la hâte à mettre en place de nouveaux outils dans la crise peuvent amener de l'inquiétude et de la défiance, surtout si l'urgence a conduit à certains manquements, on l'a vu depuis un an.

Mme Christine Lavarde, rapporteur. – Initialement, nous voulions simplement actualiser les rapports de 2012 et 2015. Mais en lisant les préconisations de ces rapports, on s'est vite rendu compte que le monde avait changé en peu de temps. Par exemple, le rapport de Fabienne Keller recommandait, pour se prémunir de futures pandémies, d'utiliser plus massivement le levier de l'aide publique au développement en direction de l'Afrique afin de l'aider à structurer son système de santé. Or, aujourd'hui, l'Afrique est relativement épargnée par la Covid-19. Il a fallu s'intéresser au numérique, qui caractérise désormais fortement nos sociétés. Ceux qui sont à côté du numérique ont un univers des possibles restreint. Nous ne sommes pas étonnés des réactions à nos propositions, qui heurtent par rapport aux principes et actions actuelles de la CNIL. L'idée n'est pas de remettre en cause la politique de protection des données « en temps de paix ». Mais nous estimons qu'en situation exceptionnelle, il faut adapter nos cadres de régulation pour fournir une réponse appropriée. On a du se confiner pendant des semaines et notre économie a été bloquée. Pourquoi ne pourrions-nous pas adapter nos règles de protection des données, pour un temps limité et pour des raisons précises, liées à la situation sanitaire que nous vivons ? Nous devons avoir aussi en tête les problématiques de souveraineté numérique et prévoir la sécurité des outils que nous mettons en place.

Mme Véronique Guillotin, rapporteure. – Nous attendions des réactions à nos propositions « décoiffantes ». Le sujet du numérique, des données et de la protection des libertés est dans l'actualité et suscite logiquement de nombreux débats. On peut se demander si nos libertés n'ont pas été mises exagérément entre parenthèses durant la crise sanitaire, alors que le numérique aurait permis d'alléger les contraintes si nous avions anticipé le recueil de données. Dans le débat sur l'acceptation du recueil de données, nous faisons face à une véritable question philosophique, qui s'est posée au moment de la mise en place de l'application *StopCovid*, avec des interrogations sur le meilleur modèle, centralisé ou décentralisé. Or, nous donnons tous les jours des données aux géants du numérique, à travers notre usage habituel des outils à notre disposition, comme notre *smartphone*. Nous sommes constamment pistés. D'autres pays que le nôtre sont plus pragmatiques. L'Estonie a par exemple mis en place un identifiant unique pour tous les services à ses citoyens, lui permettant d'être davantage préparée en cas de crise. Les propositions techniques ne sont pas irréalistes. Mais nous devons surmonter les blocages philosophiques. Nous devons aussi faire preuve de pédagogie dans l'explication des propositions de notre rapport. Il faut créer une « boîte à outils » permettant de régler le niveau du risque et le niveau de collecte de données. Si demain nous avons un risque chimique ou nucléaire à gérer sur une zone géographique déterminée, par exemple autour d'une centrale, comment expliquer que nous n'aurions pas le droit d'envoyer des SMS à l'ensemble des personnes concernées dans la zone considérée, seul moyen de prévenir les intéressés en temps réel ?

M. René-Paul Savary, rapporteur. – Aucun collègue n'a exprimé une totale opposition à nos propositions. Beaucoup d'interlocuteurs estiment que la CNIL est aujourd'hui sur des positions archaïques. Critiquer la CNIL revient à s'attaquer à un monument. Or, nous restons attachés à la protection de nos données, mais nous devons organiser leur utilisation. Et aujourd'hui, nous donnons largement nos données personnelles aux GAFAM. Certes, nous redoutons de fournir nos données à un État qui deviendrait totalitaire, mais cela ne doit pas nous paralyser. Je souligne que si la crise sanitaire a été administrée, je ne considère pas qu'elle a été bien gérée. Pourquoi ne pourrions-nous pas construire un EPRUS numérique ? Il faut certes prendre des précautions dans la collecte et le traitement des données personnelles mais en préservant des capacités de réaction. Si une solution numérique permet de cibler les réponses et d'éviter de prendre des mesures générales de confinement, c'est un progrès.

Quand j'étais président de conseil général, je voulais faire des économies d'énergie. Je ne voulais pas laisser penser aux agents que je savais mieux qu'eux ce qu'il fallait faire et leur ai demandé de formuler des propositions. Spontanément, ils ont recommandé d'éteindre les lumières dans les bureaux vides. Il faut en toute chose avoir la même approche : ne pas être trop directif et demander les suggestions à la base. Plus de contraintes numériques peut aider à avoir plus de libertés physiques, donc permettons-nous d'avoir le choix. Nous n'avons pas étudié le rôle des médias dans les différents pays. L'improvisation n'est pas toujours mauvaise mais pas toujours bonne non plus. C'est pourquoi, il faut avoir prévu à l'avance des outils pour gérer les crises.

Disposer d'un *cloud* souverain est évidemment la solution que nous préférons, mais certains de nos voisins européens ont choisi d'aller vers des dispositifs adossés aux GAFAM, qui s'avèrent finalement assez sécurisés. Nous craignons tous que les outils numériques soient aux mains du pouvoir, mais nous pouvons prendre des mesures législatives protectrices. Si nous ne faisons rien, ce sont les GAFAM qui imposeront leurs solutions. Certaines de nos propositions sont parfaitement acceptables : un identifiant numérique paraît de bon sens au 21e siècle. Même la CNIL a fait évoluer sa position sur le sujet, du moins dans le domaine de la santé. L'espace numérique de santé est aussi une avancée. On a 10 millions de personnes qui disposent désormais d'un dossier médical partagé (DMP). Il convient d'avancer. Nous aurions pu vivre avec moins de contraintes si cela avait été mis en place plus tôt. Enfin, un *Crisis Data Hub* serait à mon sens utile, car il permettrait d'adapter le degré plus ou moins intrusif d'utilisation des données personnelles en fonction de la gravité de la crise.

M. Jean-Raymond Hugonet. – Merci aux collègues de ne pas avoir fait un rapport à l'eau tiède. Mais certains sujets n'ont pas été abordés. Celui de la fuite des grandes villes nous interroge. Les terrains se vendent aujourd'hui au fin fond de l'Essonne à des urbains qui cherchent un cadre de

vie plus agréable. La territorialisation de la réponse sanitaire à la crise est une nécessité. On ne peut pas comprendre des règles de confinement là où il n'y a pas de cas de Covid-19. Allons aussi dans le sens de l'expérimentation territoriale, y compris dans l'utilisation des données de santé. Essayons aussi de répondre au mal principal de notre pays : l'incroyable archaïsme de notre administration. Dans la crise, on a constaté que les préfets nous convoquaient à des réunions alors qu'ils n'avaient aucun pouvoir sur la gestion de crise sanitaire.

M. Mathieu Darnaud, président. – Souvent, on reproche aux politiques de manquer d'anticipation. Votre rapport, bien au contraire, anticipe et propose des outils. Je suggère que l'on s'accorde encore un délai pour parfaire la présentation du rapport, sur un sujet sensible et d'actualité qui nécessite d'être traité de manière précise et approfondie. Nous solliciterons un débat en séance publique pour en débattre avec le Gouvernement et nos collègues.

II. RÉUNION DU JEUDI 3 JUIN 2021

M. Mathieu Darnaud, président. – Véronique Guillotin, Christine Lavarde et René-Paul Savary nous ont présenté, le 6 mai dernier, leur rapport consacré aux outils numériques dans la prévention et la gestion des pandémies. Cette séance a été l'occasion d'un débat intense car le rapport de nos collègues est à la fois riche, très dense et percutant, voire provocateur. En revenant sur la gestion de la pandémie au cours de la dernière année ainsi que sur l'expérience des autres pays, notamment asiatiques, ce rapport nous met face à nos contradictions. Il tente de résoudre une équation difficile qui comporte trois éléments : la gestion optimale d'une pandémie, les immenses possibilités des outils numériques et la préservation de nos libertés.

Ce rapport a une vraie vision prospective. Il se termine par une proposition choc pour la gestion des futures pandémies, en tirant les leçons de l'expérience acquise ces derniers mois.

Pour donner à tous le temps de la réflexion sur l'analyse et la proposition de nos rapporteurs, nous avions décidé d'un commun accord de reporter de quelques semaines l'examen définitif du rapport afin de laisser à tous la possibilité de s'en saisir et à nos rapporteurs le temps de bien ciseler leur propos. Le document qui vous a été envoyé en amont de cette réunion vous a permis d'en prendre connaissance en détail. Je propose à nos rapporteurs de vous le présenter.

M. René-Paul Savary, rapporteur. – Il y a un mois, nous avions présenté devant vous les premiers résultats de nos travaux sur le recours aux outils numériques dans la gestion des crises sanitaires. Nous proposions, en un mot, de recourir bien plus fortement aux outils numériques, en assumant si nécessaire des mesures plus intrusives, mais aussi plus ciblées et limitées dans le temps. Avec, pour contrepartie, une liberté retrouvée plus vite dans le « monde réel ».

Nous avons fait le choix d'une proposition volontairement provocatrice, mais aussi d'un dispositif qui se prête à l'expérimentation, et qui puisse être utile lors de crises autres que sanitaires. Notre proposition suscite des craintes et des interrogations légitimes, et nos échanges de la dernière fois l'ont bien montré. Le projet de rapport que nous vous avons adressé mardi ne revient pas sur le fond de notre pensée, mais il tient compte de vos remarques et permettra, nous l'espérons, de répondre à vos questions.

Reste que, sur le fond, nous n'avons pas le choix. Depuis un an et demi, les Français sont soumis à des restrictions inédites et généralisées de leurs libertés, qui n'ont pas pour autant permis d'éviter un trop lourd bilan sanitaire (100 000 morts), qui ont causé la plus grande récession économique jamais connue en temps de paix, et dont on commence à peine à mesurer les conséquences psychologiques. Surtout, si la vaccination permet aujourd'hui

d'espérer un retour à la normale, la pandémie de Covid-19 n'est ni la dernière, ni sans doute la plus grave à laquelle nous aurons à faire face à l'avenir. Nous ne pouvons pas nous permettre de revivre cela à chaque fois.

Dès le début de la crise, certains pays ont fait le choix de s'appuyer sur des outils numériques, y compris pour contrôler le respect des restrictions à un niveau individuel, en croisant des données médicales avec une multitude d'autres informations, notamment de géolocalisation. C'est notamment le cas des pays d'Asie orientale, dont l'exemple, à défaut d'être transposable, est instructif.

En Chine, toutes les données disponibles sont exploitées pour identifier les cas positifs, y compris la vidéosurveillance, et chacun peut enquêter directement sur trois individus. Avec son « code couleur de santé » disponible sur les incontournables applications *WeChat* et *AliPay*, la Chine est aussi le premier pays à s'être doté d'un pass sanitaire. Quant au *contact tracing* numérique, c'est Singapour qui l'a inventé, dans une version autrement plus contraignante que *TousAntiCovid*. En Corée du Sud, le *contact tracing*, obligatoire et intrusif, exploite aussi bien les factures téléphoniques que les relevés bancaires, et les autorités n'hésitent pas à interroger les employeurs. Les quarantaines individuelles, indemnisées par l'État, sont strictement surveillées, *via* une application de géolocalisation. Il en va de même à Taïwan. À Hong Kong, les personnes en quarantaine doivent même porter un bracelet électronique, et peuvent recevoir un appel vidéo surprise des forces de l'ordre, quand ce n'est pas un contrôle à domicile.

Il n'y a malheureusement pas de mystère : plus les outils sont intrusifs, plus ils sont efficaces. Ces pays ont la plus faible mortalité du monde : avec 12 décès seulement début mai, Taïwan compte 3,5 morts par million d'habitants, au 3e rang mondial, suivi de peu par la Chine (6e rang) puis Singapour (10e rang, avec 31 décès). La France, elle, figure au 136e rang mondial sur 155 (compte tenu des *ex-aequo*), avec 1 633 morts par million d'habitants, non loin des États-Unis (142e) et du Brésil (146e), qui ont notoirement refusé tout dispositif intrusif.

On peut douter des chiffres officiels de la Chine, mais pas de ceux de Taïwan, de Singapour ou de la Corée du Sud. Or, même en tenant compte de tous les autres facteurs possibles – démographie, insularité, urbanisation, génétique… –, il est impossible d'expliquer de tels résultats sans reconnaître le rôle majeur joué par les outils numériques.

Le modèle asiatique, dira-t-on, n'est pas transposable à la France. Peut-être ! Mais les pays asiatiques ne sont pas les seuls. Depuis notre dernière réunion, une étude remarquée, publiée dans *The Lancet* et portant sur l'ensemble des pays de l'OCDE, a comparé l'efficacité de la stratégie dite « zéro Covid », qui vise à éliminer le virus le plus vite possible au moyen de mesures plus fortes, avec l'efficacité de la stratégie d'atténuation, celle des

pays qui, comme la France, choisissent plutôt de « vivre avec ». Sur les 37 pays de l'OCDE, seuls 5 ont opté pour la stratégie « zéro Covid » – dont l'Australie, la Nouvelle-Zélande et l'Islande –, et tous se sont appuyés sur des outils numériques.

Les résultats sont sans appel : dans les pays qui ont choisi la stratégie « zéro Covid », le nombre de morts par million d'habitants a été 25 fois inférieur à celui des autres pays. Au prix d'une récession économique plus forte ? Pas du tout : l'évolution du PIB y a été systématiquement plus favorable, avec une moindre chute et une reprise plus forte. Et les libertés publiques, dans tout cela ? C'est sans doute le plus intéressant : les restrictions n'ont en réalité été plus fortes que pendant les trois premières semaines de la pandémie, avant d'être allégées, pendant que les pays plus « permissifs » se retrouvaient contraints de maintenir sur la durée des mesures plus attentatoires aux libertés.

Il est vrai, toutefois, qu'on observe ces dernières semaines un regain de l'épidémie dans les pays asiatiques, même si celui-ci demeure léger et sans commune mesure avec ce que nous connaissons en Europe. C'est en quelque sorte l'envers de la médaille : parce que leur stratégie initiale a très bien fonctionné, ces pays ont négligé la vaccination, ce qui les a rendus vulnérables aux cas importés des pays plus « permissifs ». Mais ne nous y trompons pas : ce rebond plaide pour davantage de numérique, plutôt que pour moins de numérique, car face à une situation qui se dégrade brutalement, il donne les moyens de réagir sans revenir à des restrictions généralisées.

La France elle-même a fait beaucoup de chemin depuis un an et demi, à l'époque où ce qui allait devenir notre pass sanitaire était vu comme une atteinte inacceptable à notre vie privée. Aujourd'hui, nous le prenons pour ce qu'il est : un moyen de retrouver nos libertés, en attendant la vaccination de la majorité de la population.

La prochaine fois, surtout face à une crise plus grave, nous devrons être capables d'aller plus loin et de réagir plus vite.

Toutefois, et j'insiste sur ce point, nous ne préconisons aucun dispositif numérique en particulier dans ce rapport. Nous disons, précisément, qu'il est impossible de savoir à l'avance de quoi les prochaines crises seront faites, et quels seront les meilleurs moyens d'y répondre. C'est pourquoi, plutôt que de proposer tel ou tel outil, nous défendons le principe d'une « boîte à outils », à laquelle il serait possible de recourir de façon graduée en fonction des circonstances, à condition toutefois de s'y être préparés.

D'ailleurs, l'avantage d'une « boîte à outils », c'est qu'elle se prête fort bien à l'expérimentation, notamment au niveau local. Certaines collectivités – je pense par exemple à la région Grand Est – sont très avancées en matière de numérique, et le déploiement de la fibre permet d'envisager des applications innovantes, notamment pour porter assistance aux personnes vulnérables. Pourquoi ne pas leur permettre d'essayer ?

En effet, tout est affaire de proportionnalité. Face à une crise « modérée », qui appelle surtout des mesures de « freinage » pour éviter la surcharge des hôpitaux, nous pourrions nous limiter à quelques outils d'information et de coordination bien pensés. Ce serait déjà un progrès. Face à une menace un peu plus grave, on pourrait imaginer l'envoi automatique d'un SMS à tout individu qui s'éloignerait de son domicile pendant le couvre-feu, à simple titre de rappel et sans aucune remontée d'information.

Dans les cas les plus extrêmes, des mesures plus fortes ou coercitives pourraient s'avérer indispensables : ainsi, toute violation de quarantaine pourrait conduire à une information en temps réel des forces de l'ordre, à une désactivation du titre de transport ou des moyens de paiement du contrevenant, ou encore à une amende prélevée automatiquement sur son compte bancaire, comme le font des radars routiers.

N'écartons pas trop vite de tels scénarios. Le taux de létalité de la Covid-19 est autour de 1 %. Que se passerait-il si demain nous étions frappés par une maladie plus virulente, ou qui touche en priorité les jeunes adultes, comme ce fut le cas avec la grippe espagnole, avec ses 100 millions de morts (5 % de l'humanité) pour un taux de létalité de 3 % ? La médecine a progressé, mais trouver un vaccin n'est jamais garanti, et notre époque a aussi ses propres vulnérabilités : la mondialisation, le risque de bioterrorisme, etc.

La proportionnalité, ce n'est pas seulement adapter les outils à la gravité de la menace. C'est aussi comparer les atteintes portées aux libertés « numériques » à celles portées aux libertés « physiques ». Or celles-ci ont été bien plus lourdes, ont duré bien plus longtemps, et se sont appliquées à tous de façon aveugle. Il faut se poser la question honnêtement : qu'est-ce-qui est le pire, du point de vue de ma liberté, entre le croisement de deux informations que l'administration possède déjà sur moi, et une interdiction de sortir de mon domicile pendant plusieurs mois ?

Le deuxième point fondamental sur lequel je souhaiterais insister, c'est que plus les technologies sont intrusives, plus elles peuvent être ciblées, individualisées et limitées dans le temps. Imaginons, par exemple, que seules les personnes diagnostiquées positives soient soumises à des restrictions, sous la forme d'une quarantaine obligatoire et effectivement contrôlée par géolocalisation. C'est effectivement intrusif. Mais si une telle mesure était décidée aujourd'hui, elle concernerait seulement 85 000 personnes, soit moins de 0,1 % de la population française, tandis que les 99,9 % restants ne

seraient soumis à aucune mesure particulière : les déplacements seraient libres, les magasins resteraient ouverts, les écoles et les musées aussi. Et nous en aurions fini avec l'épidémie en quelques semaines.

À la place, nous avons préféré mettre en place des restrictions généralisées mais impossibles à contrôler, en interdisant à 67 millions de Français de sortir de chez eux pendant plusieurs mois sauf motif impérieux, en mettant toute la société sous cloche, sans pour autant réussir à éliminer le virus. Bref, nous sommes restés « libres et égaux », mais confinés.

J'espère avoir bien exposé les raisons qui nous ont guidés dans nos travaux. Nous ne proposons pas de limiter les libertés, nous cherchons un moyen de les retrouver. Le numérique peut nous y aider, à condition de nous y préparer – car, si nous ne le faisons pas, d'autres le feront pour nous, et il sera trop tard, alors, pour défendre nos valeurs démocratiques.

Mme Véronique Guillotin, rapporteure. **–** Depuis le mois dernier, les choses ont beaucoup changé en France, et dans le bon sens. D'abord, l'épidémie recule, grâce à la vaccination notamment. Ensuite, nous nous sommes dotés d'un outil numérique qui permettra, espérons-le, de réussir le déconfinement : le pass sanitaire, et bientôt son équivalent pour les voyages internationaux, le passeport sanitaire, auxquels on peut ajouter les « carnets de rappel numériques », nouvelle fonctionnalité de *TousAntiCovid*.

Il n'empêche, par rapport aux pays asiatiques, et par rapport aux possibilités des technologies actuelles, sans même parler de celles de demain, le moins qu'on puisse dire est que la France ne s'est pas donné tous les moyens de réussir.

Que s'est-il passé exactement ? Permettez-moi de revenir un instant sur les raisons de ce retard français, qui sont de deux types : d'une part, des raisons immédiates, d'ordre technique et matériel, qui nous ont conduits à improviser, avec tout ce que cela implique ; d'autre part, des raisons plus profondes, d'ordre politique et idéologique, sur lesquelles je reviendrai.

Faute d'avoir mené en amont les efforts de modernisation de nos systèmes d'information, nous avons dû nous appuyer sur des fichiers *ad hoc*, créés pour la circonstance : les fichiers SI-DEP et *Contact-Covid*, dans le cadre de la stratégie « tester, alerter, protéger », puis le fichier *Vaccin Covid*, pour le suivi de la campagne de vaccination.

Commençons par l'aspect positif : dans ces circonstances difficiles, la France a su faire preuve d'une grande réactivité, grâce à un mélange de volonté politique, de gouvernance forte et de financements à la hauteur. Le fichier SI-DEP, en particulier, a été développé en moins d'un mois, alors qu'un projet identique porté par Santé Publique France était bloqué depuis 8 ans… Bien sûr, les débuts ont été un peu chaotiques, avec des remontées concurrentes voire contradictoires, et un vrai problème du côté des EHPAD, dont le retard en matière d'informatisation est alarmant. Mais la France est loin d'être le seul pays dans ce cas !

Sauf que – voilà l'aspect négatif – tout cela ne suffit pas. Avec des fichiers *ad hoc*, on peut faire des statistiques pour voir l'étendue des dégâts, on peut décider de confiner telle région ou de vacciner telle classe d'âge, mais pour briser les chaînes de contamination et sauver des vies, c'est autre chose… En effet, ces fichiers ne sont pas interconnectés – ni avec le reste du système de santé, ni même entre eux !

Résultat : impossible de savoir, par exemple, si les « cas contacts » d'une personne ont été effectivement contaminés, ou s'ils sont vaccinés. Impossible, aussi, de savoir s'ils courent un risque particulier (maladie, comorbidité, etc.), faute de pouvoir accéder à leur dossier médical. Nous avons mobilisé des milliers d'agents au sein des « brigades de traçage » pour passer des appels téléphoniques et effectuer des visites à domicile, mais la réalité, comme nous le disions déjà la dernière fois, c'est qu'au lieu de briser les chaînes de contamination, ils jouaient aux devinettes avec le premier maillon.

Impossible, aussi, de faire circuler correctement l'information. Je pense notamment aux collectivités locales, dont la tâche aurait été grandement facilitée si elles avaient pu identifier les personnes vulnérables, pour la distribution de masques par exemple.

Parfois, des acteurs privés, au sein de la société civile notamment, ont pris le relai au pied levé. On peut évidemment se féliciter de ce dynamisme, mais tout de même : est-il normal qu'un informaticien de 24 ans, Guillaume Rozier, fasse mieux que Santé Publique France avec son *CovidTracker*, et mieux que l'Assurance maladie avec *ViteMaDose* ?

Tout se serait passé bien différemment si nous avions – comme l'Estonie dont nous analysons la stratégie dans le rapport – disposé d'un système de santé organisé autour d'une « plateforme », où chaque usager dispose d'un identifiant unique, et où tous les services sont connectés entre eux. Nous aurions pu avoir une stratégie de détection plus efficace, en ayant au même endroit non seulement les données de SI-DEP, *Contact-COVID* et *Vaccin Covid*, mais aussi tout l'historique médical du patient, avec ses facteurs de risque et ses comorbidités, grâce au dossier médical partagé (DMP). Nous aurions aussi disposé d'une messagerie sécurisée, d'une application de prise de rendez-vous pour les tests et les vaccins, d'un outil de e-prescription, et de tout un catalogue d'applications tierces, utilisant notamment les données des objets connectés.

Mais rien de tout cela n'était prêt lorsque la crise est arrivée, même si un tournant majeur a eu lieu en 2019, avec la reprise en main du chantier du numérique en santé. Il faudra toutefois des années pour rattraper le retard accumulé.

Un mot également sur le *Health Data Hub*, créé en 2019 : il ne s'agit pas cette fois d'un outil destiné aux patients, mais d'un « entrepôt » de données médicales agrégées et pseudonymisées, une sorte de guichet unique

pour la recherche médicale, qui pourrait bien faire de la France le *leader* mondial en matière d'intelligence artificielle appliquée à la santé. Son intérêt dans le cadre d'une crise comme celle du Covid-19 est évident, et quelques projets de recherche en ont d'ailleurs bénéficié. Mais le *Health Data Hub* n'en est qu'à ses balbutiements, et à vrai dire, on en a surtout parlé jusqu'à maintenant en raison de l'opposition de la CNIL, qui conteste l'hébergement des données sur les serveurs de Microsoft.

Ceci m'amène à la deuxième grande raison du retard de la France, sans doute beaucoup plus fondamentale que les aspects techniques qui n'en sont que la conséquence : sa profonde défiance à l'égard du numérique dès lors que cela implique l'État ou des pouvoirs publics.

On l'a vu avec *TousAntiCovid*, qui constitue un cas d'école des contradictions françaises à l'égard du numérique : nous avons voulu une application « souveraine » et totalement anonyme, allant même jusqu'à développer notre propre protocole, dit « centralisé », quand la quasi-totalité des pays du monde choisissaient la solution « décentralisée » développée par Apple et Google. En réalité, *TousAntiCovid* n'est pas particulièrement plus sécurisé, et même les ingénieurs qui l'ont conçu se sont montrés prudents sur le sujet. Par contre, nous l'avons payé cher sur le plan de l'efficacité : l'application française ne fonctionne pas sur les *iPhones*, qui bloquent le *Bluetooth*, et n'est pas interopérable avec celles des autres pays, alors même qu'une pandémie requiert, par définition, une réponse coordonnée – comme les élus des zones frontalières ont pu le constater très directement.

Comme si cela ne suffisait pas, l'application est peu utilisée : seulement 1,7 million de téléchargements un mois après son lancement, soit 2 % de la population française, quand les Allemands en étaient à 6 millions en moins de deux jours. Une partie du retard a été rattrapé, mais c'est d'abord grâce à ses nouvelles fonctionnalités, qui n'ont rien à voir avec le *contact tracing*. D'ailleurs, pour que celui-ci soit efficace, il faut que les gens jouent le jeu. Or seules 4,5 % des personnes testées positives se sont effectivement signalées dans *TousAntiCovid*… Dans ces conditions, faut-il s'étonner que l'application n'ait pas permis d'envoyer plus de 200 000 notifications, soit 1 % de la population, quand les Britanniques en sont déjà à 8 % ?

Mais au fond, le problème dépasse largement la France : toutes ces applications ont un point commun, leur inefficacité, qui s'explique par le choix des pays occidentaux de s'en tenir à des dispositifs strictement volontaires et strictement anonymes. Comme le disait René-Paul Savary, il n'y a pas de mystère. Par contre – et je passe maintenant la parole à Christine Lavarde –, il y a peut-être une solution.

Mme Christine Lavarde, rapporteur. – Lors de notre dernière réunion, les remarques que nous avions formulées au sujet du rôle de la Commission nationale de l'informatique et des libertés (CNIL) avaient paru sévères à certains d'entre vous. Nous en avons tenu compte dans le rapport, sans pour autant revenir sur le fond de notre propos.

Soyons clairs : nous accordons la plus grande importance à la protection de la vie privée et des données personnelles, mais nous pensons aussi qu'en cas de crise, leur protection ne doit pas avoir pour conséquence de restreindre durablement nos autres libertés. Nous ne remettons nullement en cause le cadre créé par le règlement général sur la protection des données (RGPD), qui est le plus protecteur au monde, et qui prévoit en même temps tous les éléments de flexibilité nécessaires pour faire face à une crise majeure. Ce que nous regrettons – et nous ne sommes pas les seuls, car le sujet est constamment revenu au fil de nos auditions –, c'est plutôt l'interprétation qu'en fait parfois la CNIL, bien plus conservatrice que chez nos voisins européens.

De fait, il existe en France un véritable tabou dès lors qu'il s'agit de collecte de données personnelles et de croisements de fichiers par « l'État », au sens large, que l'on retrouve dans la doctrine de la CNIL.

Tout à l'heure, Véronique Guillotin évoquait l'absence d'interconnexion entre les fichiers SI-DEP, Contact-COVID et Vaccin Covid : l'obstacle n'est pas technique, il est purement juridique, au nom de la « vie privée », alors que cela ne pose aucun problème chez la plupart de nos voisins européens. À vrai dire, dans plusieurs pays, la question ne se pose même pas, puisque chaque citoyen dispose d'un numéro d'identification unique, qui relie toutes ses données et lui permet d'accéder à l'ensemble des services publics, de façon simple et sécurisée. En Estonie, en Allemagne, en Belgique, l'identité numérique est obligatoire : faut-il en conclure qu'il s'agit de dictatures ?

Le paradoxe, c'est que tout citoyen français dispose bien d'un numéro unique et fiable, le numéro de Sécurité sociale (NIR), mais la CNIL s'est toujours opposée à son utilisation au-delà de la sphère de la protection sociale. Par conséquent, toutes les autres administrations attribuent des identifiants sectoriels spécifiques : numéro fiscal, identifiant national de l'élève ou de l'étudiant (ils sont différents), etc. Même dans le domaine de la santé, nous sommes tous associés à une multitude d'identifiants « locaux », à l'hôpital, chez le généraliste, chez le dentiste, au laboratoire, etc., sources de multiples erreurs et de démarches administratives au détriment du « temps médical ». En temps de crise, alors que les hôpitaux sont surchargés, les conséquences peuvent être dramatiques.

Ce n'est qu'en 2019 que la loi Santé a cassé cette doctrine dite de « cantonnement », ouvrant la voie à l'utilisation du NIR comme identifiant unique pour toutes les données de santé, notamment pour le DMP. Mais les choses prendront encore du temps, et la CNIL s'oppose toujours à l'identité numérique d'une manière générale.

Pour revenir à la crise sanitaire, les raisonnements de la CNIL sont parfois à la limite de l'absurde. On peut citer l'exemple des caméras utilisées pour mesurer le port du masque, un temps envisagées par la RATP : la CNIL s'y était opposée, au motif qu'il s'agirait d'un traitement de données biométriques, donc comportant par définition un risque d'identification. Alors même que les caméras en question ne conservaient aucune image et ne transmettaient que des statistiques agrégées de taux de port du masque… S'agissant des caméras thermiques, largement utilisées ailleurs pour détecter le Covid-19, la CNIL s'y est opposée au motif que la fièvre n'est pas un symptôme systématique : par peur de ne pas détecter tout le monde, nous nous sommes donc privés de la possibilité de détecter au moins certains cas, ce qui aurait déjà représenté une victoire contre la maladie.

Les nouvelles technologies comportent des risques, c'est vrai, et lors de notre précédente réunion, plusieurs d'entre vous ont à juste titre évoqué le cas des GAFA. Mais justement, ne nous trompons pas de *Big Brother* : à chaque instant de notre vie, nous livrons aux géants du numérique bien plus de données que l'État n'en aura jamais, à des fins purement commerciales et sans aucune des garanties qu'offre le contrôle démocratique. Par contre, quand il s'agit d'intérêt général, de protection de la santé publique, et plus largement d'amélioration du service public, le moindre croisement de fichiers suscite des polémiques infinies. Faut-il s'étonner, ensuite, que Google et Facebook en sachent davantage sur l'épidémie de Covid-19 en France que le ministère de la Santé ou l'Assurance maladie ? Et qu'ils proposent des outils plus efficaces, que nous pourrions bien, demain, nous retrouver contraints d'accepter ?

Cette sensibilité française à la collecte des données par l'administration est ancienne et profonde. Dans l'imaginaire collectif, elle est associée à l'idée d'un « État policier » et d'un « fichage » de la population, et c'est cette même idée qu'on retrouve dans l'opposition à chaque nouveau projet, du fichier SAFARI en 1974 à *TousAntiCovid*.

Mais à l'heure de la révolution numérique, du *big data* et de l'intelligence artificielle (IA), on ne peut plus raisonnablement soutenir que le seul intérêt des croisements de fichiers est l'instauration d'un État totalitaire ! Dans les années 1970, il n'était pas absurde de raisonner ainsi : c'était encore la meilleure garantie possible, à une époque où on était bien loin, par ailleurs, d'imaginer les possibilités immenses du numérique. Mais aujourd'hui, les choses sont différentes : il existe bien d'autres façons de garantir la confidentialité des données sans pour autant s'interdire de les utiliser, comme par exemple la *blockchain* ou l'*open source*. En somme, tout se passe comme si nous avions une préférence pour l'inefficacité.

Nous avons donc mené nos travaux en nous posant la question suivante : comment répondre à une crise avec toute l'efficacité du numérique, sans rien céder sur nos valeurs démocratiques ?

Vous avez pu voir, dans le projet de rapport, que nous avons choisi de ne retenir qu'une seule grande proposition, plutôt que de multiplier les recommandations. C'est une proposition pragmatique, qui permettrait de répondre efficacement aux situations de crise – et qui ne ferait que cela.

C'est un fait : si nous voulons sauver des vies humaines et éviter de mettre la vie économique et sociale sous cloche à chaque nouvelle menace, il faudra inévitablement s'appuyer sur des croisements de données massifs et dérogatoires. Sauf que les données en question sont soit des données personnelles qu'il est inconcevable d'exploiter en temps « normal » (par exemple des données médicales croisées avec des données de géolocalisation), soit des données produites par des entreprises privées (opérateurs télécom, entreprises technologiques, entreprises de transport, etc.) qui n'ont aucune raison ni obligation de les fournir par ailleurs, ni même de s'y préparer.

René-Paul Savary a déjà insisté sur ce point : nous ne proposons en aucun cas de collecter ces données. Par contre, nous proposons de nous mettre en capacité de le faire rapidement, si jamais les circonstances devaient l'exiger, pour ainsi dire en appuyant sur un bouton.

Concrètement, cela passe par la mise en place d'une plateforme sécurisée spécifique, qui ne serait activée qu'en temps de crise, et qui permettrait de centraliser les données utiles avant de les redistribuer aux acteurs qui en ont besoin pour remplir leurs missions : établissements de santé, sécurité civile, forces de l'ordre, collectivités locales, transports publics, prestataires, etc.

Nous appelons cela le *Crisis Data Hub* (CDH), sur le modèle du *Health Data Hub* évoqué par Véronique Guillotin. La différence est que le *Health Data Hub* ne centralise que des données médicales et pseudonymisées mais qu'il le fait massivement et en permanence, tandis que le *Crisis Data Hub* collecterait des données plus diverses et nominatives, mais sur un champ bien plus restreint, pendant une période très limitée, et avec un objectif déterminé : sauver des vies, tout en préservant la société et l'économie.

Sur le plan juridique, notre proposition se traduirait par une obligation légale, pour certaines entreprises et administrations, de maintenir des bases de données dont le contenu et le format seraient fixés à l'avance, et de se tenir prêtes à les « brancher » à la plateforme en cas de nécessité. La liste de ces acteurs pourrait s'inspirer de celle des 250 opérateurs d'importance vitale (OIV), soumis à des obligations particulières et accompagnés par l'Agence nationale de cybersécurité (ANSSI). En temps « normal », aucune donnée ne serait bien sûr transmise, mais le système serait toujours prêt, grâce à un travail continu de maintenance et d'amélioration – soit tout ce qui nous a manqué ces derniers mois.

Enfin, cette préparation en amont est la meilleure des garanties que nous puissions apporter aux droits et libertés des citoyens. Elle permettrait au débat démocratique de se ternir sereinement, en prenant le temps de la réflexion et de la pédagogie, plutôt que de réagir « à chaud » et au cas par cas sur chaque mesure. Pour cela, nous pourrions réfléchir sur la base de différents « scénarios », et nous poser la question des mesures efficaces et acceptables en fonction de la gravité de la menace.

En particulier, cette méthode permettrait à la CNIL d'établir une doctrine préalable d'autorisation de chaque dispositif. Le juge pourrait se prononcer en amont plutôt que dans l'urgence. On pourrait aussi imaginer une procédure de « rescrit » spécifique, que pourraient par exemple solliciter les associations de défense des libertés publiques.

Nous proposons même d'aller encore plus loin : tous les dispositifs seraient développés en *open source*, de sorte que chacun pourra vérifier qu'ils ne font rien d'autre que ce qu'ils sont censés faire – et on peut faire confiance à la société civile pour examiner chaque ligne de code dans les moindres détails. Quant aux données agrégées (chiffres de l'épidémie, respect des restrictions, etc.), elles seraient publiées en *open data*. Disons-le clairement : aucun pays, face à la crise de la Covid-19, n'a fait preuve d'un tel niveau de transparence. Mais nous pensons que c'est la condition *sine qua non* de la confiance des citoyens, sans laquelle rien ne pourra être fait.

Voilà tout ce que le *Crisis Data Hub* permettrait de faire en amont. Que se passe-t-il ensuite, sur le moment, en cas de crise ? Déjà, nous serions prêts. Rien ne pourrait se faire sans un soutien de l'opinion, c'est-à-dire sans un consensus démocratique, mais il est aussi nécessaire que le Gouvernement puisse réagir et surtout s'adapter rapidement.

Le *Crisis Data Hub* rendrait possible un nouvel équilibre. D'une part, son activation, acte politique fort, devrait revêtir un caractère solennel, par exemple par un article spécifique dans la loi proclamant l'état d'urgence sanitaire, qui permettrait d'obtenir une majorité claire et de fixer des limites, par exemple de durée. Au sein de celles-ci, l'exécutif disposerait ensuite d'une plus grande marge de manœuvre. D'autre part, et en contrepartie de cette flexibilité, la mise en œuvre des différents dispositifs pourrait faire l'objet d'une procédure de contrôle spécifique, en continu, impliquant le Parlement, la CNIL ou encore la société civile.

L'outil que nous proposons serait utile au-delà des seules crises sanitaires, par exemple en cas de catastrophes naturelles ou industrielles, ou encore en cas d'attaques terroristes ou bioterroristes. Imaginons par exemple la fuite d'un réacteur nucléaire : alors que moins de la moitié des foyers vivant à proximité d'une centrale nucléaire ont effectivement retiré leurs pastilles d'iode en pharmacie, le numérique permettrait de savoir immédiatement qui se trouve dans la zone, et à qui fournir en priorité les pastilles. Autre exemple, la chute de débris spatiaux. Cela peut sembler très

théorique, mais leur nombre augmente de façon exponentielle – on l'a vu avec la chute récente de débris des lanceurs spatiaux chinois de la *Longue Marche* (*Tiangong*). Aujourd'hui, nous sommes capables de modéliser avec précision le point d'impact de ces débris – mais nous ne le savons qu'au dernier moment : seul le numérique permet alors de prévenir la population. Dernier exemple : aux États-Unis, la population est prévenue par des messages individuels à l'approche d'un ouragan.

Mais au fond, le propre d'une crise, c'est d'être imprévisible. Nous préférons donc envisager le maximum, en espérant avoir à utiliser le minimum. Car le plus dangereux pour nos libertés, ce n'est pas l'imagination, c'est l'improvisation.

M. Mathieu Darnaud, président. – Merci à nos rapporteurs pour ce travail et pour la prise en compte de nos échanges antérieurs. Vous avez nuancé certains arguments sur l'équilibre entre l'efficience de la solution que vous proposez et le respect des libertés auxquelles nos concitoyens sont très attachés. Comme vous le dites, les pays asiatiques ont un degré d'acceptation des restrictions des libertés publiques bien plus fort que nous. Merci encore une fois pour le temps consacré à ce travail et pour l'exhaustivité du rapport que vous nous présentez.

M. René-Paul Savary, rapporteur. – Je voudrais ajouter un mot : attention à ne pas tomber dans la naïveté, surtout nous législateurs. Le *Health Data Hub* qui regroupe des données à but de recherche est certes pseudonymisé, comme nous le pensons tous, mais, avec des données de santé un peu spécifiques, il n'est pas difficile de retrouver l'identité d'une personne. Ce que nous proposons est simple en réalité : bien sûr, on croise un certain nombre de données mais il s'agit de rapprocher des fichiers qui étaient nécessaires à la gestion de la pandémie. Si nous avions mis en parallèle les trois fichiers SI-DEP, *Contact-COVID* et *Vaccin Covid*, cela aurait été plus simple. Je rappelle aussi qu'on accepte souvent de donner beaucoup d'informations aux brigades de traçage qui appellent à domicile, bien plus que n'en contiennent ces fichiers.

M. Bernard Fialaire. – Je vous rejoins sur le besoin de simplifier tous ces numéros qui existent en matière de santé, mais en veillant à l'utilisation qui peut en être faite. C'est d'ailleurs un sujet plus global pour l'organisation de la société française. Aujourd'hui, il est obligatoire de prendre une assurance complémentaire pour sa santé. Mais, dans quelques années, quel usage sera fait des données de santé ainsi récupérées par les mutuelles ?

La comparaison avec les pays asiatiques a ses limites. Il y a aussi des problèmes de différences de mentalités. Il ne faut pas oublier que certains virus ont une contagiosité qui préexiste à un état positif. Ce qui importe, c'est la pédagogie, la responsabilité, le civisme. Le civisme est peut-être plus important encore dans les périodes de crise que l'outil le plus performant que l'on peut avoir mis en place.

Il nous faudra un peu plus de recul pour analyser cette crise. Certains, par exemple, pensent que dans cinq ans, on pourra étudier l'évolution de la démographie en Chine et en tirer les conséquences sur le nombre de morts qui auront été liés à la pandémie. Il est essentiel de ne pas donner l'illusion qu'un outil performant permettra à tous de se comporter de n'importe quelle façon, le civisme et la responsabilité sont plus importants.

Mme Cécile Cukierman. – Je voudrais d'abord saluer le travail fait par les rapporteurs. On ne peut jamais tout anticiper mais travailler en amont, loin de l'urgence, est utile. La question principale est celle du point d'équilibre de l'acceptabilité sociale du dispositif, qui justifie le rôle du Parlement dans la mise en œuvre du dispositif. Pour une crise pandémique, un vote du Parlement peut s'organiser. Ce serait plus compliqué pour la gestion de crises urgentes, comme la fuite d'un réacteur nucléaire. Comment dans ce cas déclencher le dispositif ? Par qui serait prise la décision ? Si on légifère sur la proposition des rapporteurs, il faudra réfléchir entre les mains de qui, y compris à l'avenir, on pourrait remettre un tel pouvoir ? Bien sûr, on peut avoir besoin de réactivité mais jusqu'où faut-il aller ?

Sur les critiques faites sur les chiffres annoncés par certains pays, je voudrais rappeler que, dans notre pays aussi, il a été difficile d'obtenir les données, en particulier lors de la première vague.

M. Julien Bargeton. – Félicitations aux rapporteurs. Je partage leur orientation, courageuse qui prend clairement partie en faveur de l'utilisation des outils numériques pour gérer et anticiper une crise sanitaire. Ils évoquent le croisement des fichiers et, comme eux, je pense que nous baissons la garde devant nos propres outils. Il y a eu des débats dans l'hémicycle sur ce sujet, notamment sur le rôle de la CNIL. Il y en aura encore. Je partage le constat général et le rôle indispensable des applications numériques. Il faut lever les réticences car il y a un blocage culturel dans notre pays, souvent par peur ou méconnaissance. Il y a des outils numériques qui permettent à la fois le respect des libertés publiques et d'apporter un gain en efficacité.

L'important est d'avoir une vision proactive de l'utilisation du numérique, ce que fait le rapport et que j'approuve, nonobstant les remarques que j'aurais sur ce qui est dit, ici ou là, de la gestion de la crise par le gouvernement.

Sur les chiffres, je partage ce qui est dit par les rapporteurs. Certes, il y a le cas de la Chine mais il y a aussi le Brésil, l'Iran, l'Inde, la Russie. Pourquoi l'Organisation mondiale de la santé (OMS) prend-elle pour argent comptant les chiffres donnés par les pays ? Dans les pays développés aussi, on constate des difficultés, comme a pu en témoigner la polémique au début de l'épidémie dans la comparaison des chiffres de décès entre l'Allemagne et la France. Il faudrait qu'il y ait un partage de méthodologie générale sur les paramètres des données, qu'il y ait un travail de standardisation, pour permettre les comparaisons et un meilleur suivi des épidémies.

J'ai une dernière nuance sur ce qui est dit sur le sujet des *start-ups* et de l'innovation. L'administration de demain embarque les citoyens, les experts, les entreprises, pour les mettre en réseau. Si les personnes privées font mieux que l'administration ce n'est pas un problème en soi. *Doctolib*, *CovidTracker*, *ViteMaDose* sont des réussites liées à l'engagement de personnes privées, d'ailleurs récompensées. L'innovation vient en effet souvent du privé. Le vrai sujet est comment l'administration peut l'accueillir et la diffuser au service de la population. Apprenons à nous appuyer sur ces compétences pour les mettre au service de l'intérêt général. C'est une chance d'avoir une licorne comme *Doctolib* qui a permis la prise de rendez-vous pour la vaccination. On peut regretter que l'administration n'ait pas été en mesure de mettre en place un tel système mais on peut se féliciter que des initiatives privées l'aient permis.

M. Patrick Chaize. – J'adresse également mes félicitations aux rapporteurs pour leurs conclusions pertinentes et pragmatiques.

Je voudrais insister sur un point particulier, celui de l'identité numérique. Il faut que l'on ait cette identité numérique qui doit être fiable, garantie, et surtout être une vraie identité numérique comme dans d'autres pays. C'est un choix politique qui n'a pas été fait, je le regrette, comme d'ailleurs pour un sujet similaire, celui de la carte d'identité électronique. Les choix prévus ne sont pas satisfaisants. Or, il existe des entreprises performantes qui peuvent apporter des technologies puissantes et innovantes, mais on reste sur des décisions timides voire dépassées. Il faudrait insister collectivement auprès du Gouvernement pour que l'on ne se trompe pas dans les choix.

Un autre point sur lequel je voudrais insister est le problème de la liberté qui a bien sûr un caractère très subjectif. Dans une situation de crise, il faut accepter que nos libertés soient un peu écornées, à condition que la décision soit encadrée dans un moment particulier par la loi et donc un vote du Parlement.

Mon dernier point est un fait d'actualité qui doit cependant être constant dans nos préoccupations, celui de la sécurité. Hier encore, il y a eu un problème technique avec les numéros d'urgence. Il est impératif que dans tout ce qui est mis en place, on ait une validation de l'ANSSI et des services compétents pour encadrer les choix technologiques. Il faut se prémunir contre une situation d'attaque ou même une difficulté technique, comme celle vécue lors de l'incendie d'OVH. Nous avons l'obligation de mettre en place des systèmes robustes.

M. Éric Bocquet. – Je voudrais à mon tour saluer la qualité du travail. C'est un rapport dense et riche dans lequel les réserves de la première présentation ont été intégrées.

Aujourd'hui, le débat n'est pas entre les pro et les anti numérique. Le numérique est là. En moins d'une génération, il s'est imposé dans des proportions que personne n'imaginait. Facebook c'est 2,8 milliards d'utilisateurs, 40 % de l'humanité. Il est donc normal d'y réfléchir et c'est le rôle de la délégation.

Le risque provisoire sur l'utilisation de données n'existe pas, les données sont de toute façon transmises. Il y a donc besoin de précaution, de transparence, de régulation et de contrôle par la puissance publique.

Une petite remarque enfin, de pure forme, sur l'abondance de termes anglais dans le rapport. On arrive à une situation un peu curieuse, par exemple lorsqu'on évoque le *contact tracing* à la française. Il me semble important de veiller à utiliser les équivalents français, lorsqu'ils existent, dans les rapports parlementaires.

M. Jean-Raymond Hugonet. – Merci à nos rapporteurs pour la « sénatorisation » de la première version du rapport et la prise en compte des remarques que nous avions collectivement exprimées.

Indépendamment des aspects techniques et technologiques qui sont importants, le sujet de fond est la difficulté de concilier notre sacro-sainte liberté à la française et ce que j'appelle notre survie collective. Notre collectivité nous protège car derrière nos libertés individuelles, nous voulons la sécurité et le risque zéro. L'avantage du rapport est qu'il traite de cette survie collective. Le point crucial néanmoins est : qui déclenche les opérations ? Les parlementaires ne doivent pas perdre le contrôle car alors, oui, on pourrait craindre pour les libertés individuelles. La question est donc plus philosophique et politique que technologique. Nous devons conserver par tous les moyens le contrôle du déclenchement du recours à des outils jugés nécessaires pour notre survie collective.

Je ferais un parallèle avec la fraude sociale qui coûte plusieurs milliards à notre pays qui est exsangue : au nom du respect des libertés individuelles, on voudrait parfois s'interdire de préserver la survie de notre système social.

M. René-Paul Savary, rapporteur. – Certes, on ne peut pas tout maîtriser dans les contaminations, mais si des applications performantes existent, on peut réduire plus vite la chaîne des contaminations.

Le privé a bien sûr tout son rôle à jouer. Il est également important de veiller à la sécurité des outils. Le contrôle parlementaire est essentiel. C'est le Parlement qui décide du déclenchement et de la gradation des opérations.

Mme Christine Lavarde, rapporteure. – Dans notre dispositif, il est important de distinguer ce qui relève de l'activation ponctuelle par le Gouvernement lorsque le risque est urgent (fuite radioactive, chute d'un débris spatial) de ce qui relève du temps long, comme une crise sanitaire, où le Parlement doit être le décideur dans le respect des règles démocratiques.

Par ailleurs, il est important de dissocier le rôle de la CNIL, pour l'autorisation de transmettre les données, et celui du contrôle de la sécurité des dispositifs, domaine de l'ANSSI.

Le nom que nous avons donné à notre dispositif – *Crisis Data Hub* – se calque sur celui du *Health Data Hub*.

Mme Véronique Guillotin, rapporteure. – Le sujet du rapport était l'utilisation des outils numériques mais bien évidemment aussi, en matière de pandémie, les aspects éducatif et de prévention sont essentiels.

M. Mathieu Darnaud, président. – Mes chers collègues, autorisez-vous la publication de ce rapport ? Je ne vois pas d'objection, c'est une belle unanimité. Nous nous attacherons à le faire vivre jusqu'à la séance publique. Je vous remercie.

La délégation à la prospective autorise la publication du rapport d'information sous le titre « Crises sanitaires et outils numériques : répondre avec efficacité pour retrouver nos libertés ».

LISTE DES PERSONNES ENTENDUES

I. AUDITIONS DEVANT LA DÉLÉGATION À LA PROSPECTIVE

- **28 janvier 2021 : audition publique de M. Olivier Babeau**, professeur à l'université de Bordeaux, président de l'Institut Sapiens, sur les nouvelles technologies et la crise de la Covid-19
  - Compte-rendu : http://www.senat.fr/compte-rendu-commissions/20210125/pro_2021_01_28.html
  - Vidéo : http://www.senat.fr/compte-rendu-commissions/20210125/pro_2021_01_28.html

- **11 février 2021 : audition publique de Mme Séverine Arsène**, chercheuse associée au Médialab de Sciences Po et enseignante à l'Université chinoise de Hong Kong, sur le crédit social en Chine
  - Compte-rendu : http://www.senat.fr/compte-rendu-commissions/20210208/pro_2021_02_11.html
  - Vidéo : http://videos.senat.fr/video.2105624_60231a5b42006.audition-de-mme-severine-arsene-chercheuse-associee-au-medialab-de-sciences-po-et-enseignante-a-lu

- **18 mars 2021 : audition de M. Gilles Babinet**, co-président du Conseil national du numérique
  - Compte-rendu : http://www.senat.fr/compte-rendu-commissions/20210315/pro_2021_03_18.html
  - Vidéo : http://videos.senat.fr/video.2173364_60513ee15c749.audition-de-m-gilles-babinet-vice-president-du-conseil-national-du-numerique-digital-champion-de-

II. AUDITIONS DEVANT LES RAPPORTEURS

- Gilles Babinet, co-président du Conseil national du numérique, *digital champion* de la France à la Commission européenne
- Nadi Bou Hanna, directeur de la Direction interministérielle du numérique (DINUM)
- Antoine Buéno, essayiste et écrivain, auteur de *Futur* (Flammarion, 2020)
- Bertrand Pailhès, directeur des technologies et de l'innovation, à la Commission nationale de l'informatique et des libertés (CNIL)
- Emile Gabrié, conseiller auprès de la présidente et du secrétaire général de la CNIL
- Laure Millet, responsable du Programme santé à l'Institut Montaigne
- François Godement, conseiller pour l'Asie à l'Institut Montaigne
- Éric Bothorel, député, rapporteur de la mission confiée par le Premier ministre sur la politique publique de la donnée, des algorithmes et des codes sources
- Delphine Chaumel, inspectrice à l'Inspection générale des Affaires sociales (IGAS), membre de la mission Bothorel
- Frédéric Léger, *Director APCS Product & Services*, Association du transport aérien international (IATA)
- Robert Chad, *Area Manager France, Belgium, Netherlands & Southern Europe*, IATA
- Naly Rafalimanana, *Manager Policy & Campaigns – France, Belgium & The Netherland*s, IATA
- Vittoria Colizza, directrice de recherches à l'Institut national de la santé et de la recherche médicale (Inserm), spécialiste de la modélisation des maladies infectieuses
- Stéphanie Combes, directrice du *Health Data Hub* (HDH)
- Claire Chalvidant, directrice des relations institutionnelles du groupe Orange
- Laurentino Lavezzi, directeur des affaires publiques du groupe Orange
- Cyrille Isaac-Sibille, député, rapporteur de la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale sur le dossier médical partagé et les données de santé

- Veronika Levendof, responsable de la mission relations avec le parlement et veille législative, Caisse nationale de l'Assurance maladie (CNAM)
- Annika Dinis, directrice opérationnelle du numérique et de l'innovation santé, CNAM
- Rémi Pecault-Charby, médecin conseil responsable des missions nationales, cabinet du Médecin Conseil national, CNAM
- Emmanuel Gomez, directeur des services de la maîtrise d'ouvrage informatique, CNAM
- Claude Jissot, directeur de la stratégie, des études et des statistiques, CNAM
- Côme Berbain, directeur de l'innovation, Groupe RATP
- Julien Laurent, directeur des relations institutionnelles, Groupe RATP
- Dr. Stéphane Schück, président et directeur scientifique, Kap Code
- Baudouin Baudru, chef de la représentation en France de la Commission européenne
- Laura Létourneau, déléguée ministérielle au numérique en santé, Délégation ministérielle au numérique en santé (DNS)
- Olivier Tesquet, journaliste et écrivain, auteur de *État d'urgence technologique* (Premier Parallèle, 2021)

L'ESSENTIEL SUR…

Délégation à la PROSPECTIVE

SÉNAT

…le rapport d'information

CRISES SANITAIRES & OUTILS NUMÉRIQUES :

RÉPONDRE AVEC EFFICACITÉ POUR RETROUVER NOS LIBERTÉS

Depuis près d'un an et demi, les Français sont soumis à **des restrictions inédites et généralisées de leurs libertés**, qui n'ont pas pour autant permis d'éviter un lourd bilan sanitaire (**plus de 100 000 morts**), qui ont causé la plus grande récession économique jamais connue en temps de paix, et dont on commence à peine à mesurer les conséquences psychologiques. **Surtout, si la vaccination permet aujourd'hui d'espérer un retour à la normale, la pandémie de Covid-19 n'est ni la dernière, ni sans doute la plus grave** des crises auxquelles nous aurons à faire face dans les années à venir.

Nous ne pouvons pas nous permettre mettre sous cloche la vie sociale et économique du pays tout entier à chaque nouvelle crise. C'est pourquoi le présent rapport propose **de recourir bien plus fortement aux outils numériques, en assumant si nécessaire des mesures plus intrusives, mais aussi plus ciblées et limitées dans le temps. Avec, pour contrepartie, une liberté retrouvée plus vite dans le « monde réel ».**

1. LE NUMÉRIQUE, UN PUISSANT ANTIVIRUS

Dès le début de la crise, **certains pays, en Asie notamment, ont choisi de recourir à des outils numériques intrusifs** :

- **Exploitation de toutes les données disponibles** : géolocalisation, vidéosurveillance, historique médical, données bancaires, voyages, réponses des voisins et employeurs etc.
- **Quarantaines obligatoires contrôlées grâce au numérique** : *tracking* par GPS (Taïwan, Corée du Sud etc.) voire bracelet électronique (Hong Kong), visites des forces de l'ordre ou appels vidéo inopinés etc. Fortes sanctions, mais aussi indemnisation des jours perdus (Corée du Sud).
- **Mise en place précoce et obligatoire du *contact tracing* numérique** (Singapour avec *TraceTogether*) **ou encore du pass sanitaire** (Chine, avec le « code couleur de santé », disponible sur *Alipay* et *WeChat*).
- **Une priorité accordée à la santé publique sur la vie privée** : en Chine, chacun peut enquêter directement sur trois individus de son choix ; en Corée, l'identité et la géolocalisation des personnes infectées était initialement publique etc.

Rang (sur 155)		*Nombre de morts par million d'habitants*
3	Taïwan	3,5
6	Chine	3,5
7	Nouvelle-Zélande	5
10	Singapour	5,5
37	Hong Kong	28
41	Corée du Sud	36
…		
136	France	1 573
142	États-Unis	1 765
144	Royaume-Uni	1 922
146	Brésil	2 009
155	Hongrie	2 857

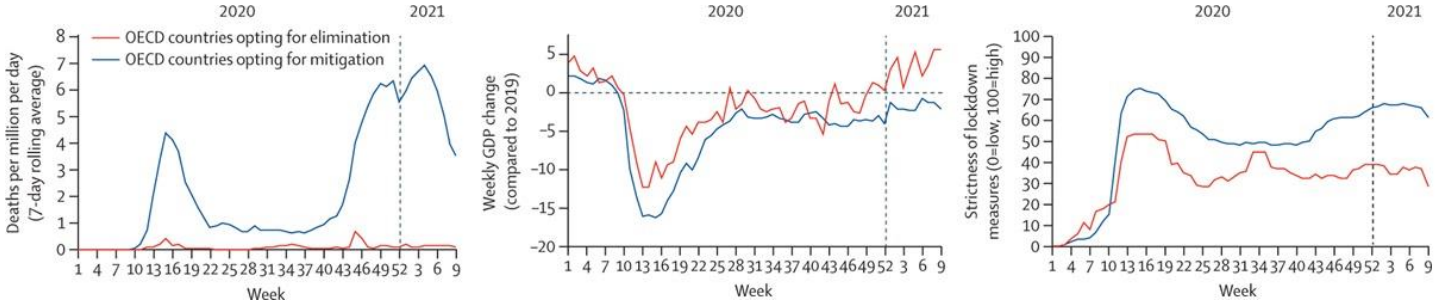
Source : Johns Hopkins University (5 mai 2021)

Ces pays ont la plus faible mortalité du monde : même en tenant compte des autres facteurs (insularité, démographie, urbanisation, génétique etc.) et des évolutions récentes, il est impossible d'expliquer de tels résultats sans reconnaître **le rôle majeur joué par les outils numériques. Il n'y a pas de mystère : plus ils sont intrusifs, plus ils sont efficaces**.

Le modèle asiatique n'est, certes, pas transposable tel quel à la France ni aux pays occidentaux – encore qu'il faille se garder de toute caricature en la matière.

Mais les pays asiatiques ne sont pas les seuls : le numérique joue – et jouera de plus en plus – **un rôle important dans les stratégies visant à l'élimination rapide du virus, dites « zéro Covid »**, par opposition aux stratégies dites d'atténuation, celles des pays qui, comme la France, choisissent plutôt choisi de « vivre avec » le virus. Au sein de l'OCDE, **seuls 5 pays sur 37 ont opté pour une stratégie « Zéro Covid »**, dont l'Australie, l'Islande et la Nouvelle-Zélande, avec des résultats sans appel : **25 fois moins de morts par million d'habitants**, une chute systématiquement moindre et une reprise systématiquement plus rapide de l'activité économique, et surtout **des restrictions aux libertés qui n'ont été plus fortes que pendant les trois premières semaines**.

Comparaison des stratégies d'élimination (en rouge) et d'atténuation (en bleu) au sein des pays de l'OCDE



Nombre de morts par jour **Variation hebdomadaire du PIB** **Restrictions des libertés**

Source : Miquel Oliu-Barton, Bary S. R. Pradelski, Philippe Aghion, Patrick Artus, Ilona Kickbusch, Jeffrey V. Lazarus et al., SARS-CoV-2 elimination, not mitigation, creates best outcomes for health, the economy, and civil liberties*, The Lancet, 28 avril 2021*

2. LA FRANCE, ENTRE IMPRÉPARATION ET CONTRADICTIONS

La France elle-même a fait beaucoup de chemin depuis un an et demi, à l'époque où ce qui allait devenir notre pass sanitaire était vu comme une atteinte inacceptable à notre vie privée. Toutefois, par rapport aux pays asiatiques, et par rapport aux possibilités des technologies actuelles, sans même parler de celles de demain, **le moins qu'on puisse dire est que la France ne s'est pas donné tous les moyens de répondre à la crise** – et qu'elle prend le risque de ne pas pouvoir répondre aux prochaines.

Ce retard a **deux types de raisons** : des raisons **immédiates et techniques** d'une part (A), et des raisons plus profondes, **d'ordre politique et idéologique**, d'autre part (B).

A. LA GRANDE IMPRÉPARATION NUMÉRIQUE DE L'ADMINISTRATION

Lorsque la crise est arrivée, **des fichiers *ad hoc* ont été mis en place dans l'urgence** : les fichiers **SI-DEP** (tests) et **Contact-Covid** (enquêtes sanitaires) dans le cadre de la stratégie « *tester, alerter, protéger* », puis le fichier **Vaccin-Covid** (vaccination).

Certes, la France a fait preuve de réactivité, grâce à un mélange de volonté politique, de gouvernance forte et de financements à la hauteur. Le fichier SI-DEP, en particulier, a été développé en moins d'un mois, alors qu'un projet identique porté par Santé Publique France était bloqué depuis 8 ans… Bien sûr, **les débuts ont été un peu chaotiques**, avec des remontées concurrentes voire contradictoires, et des difficultés dues au retard informatique des EHPAD. Mais la France est loin d'être le seul pays dans ce cas.

Mais tout cela ne suffit pas. Avec des fichiers *ad hoc*, on peut faire des statistiques pour voir l'étendue des dégâts, on peut décider de confiner telle région ou de vacciner telle classe d'âge, mais on ne peut pas directement briser les chaînes de contamination ni sauver des vies. **En effet, ces fichiers ne sont pas interconnectés – ni avec le reste du système de santé, ni même entre eux !**

- **Impossible, par conséquent, de savoir** si les « cas contacts » d'une personne ont été effectivement contaminés, ou s'ils sont vaccinés, ou encore s'ils courent un risque particulier (maladie, comorbidité etc.), faute de pouvoir accéder à leur dossier médical.

- **Les « brigades de traçage » ont mobilisé des milliers d'agents** pour passer des appels et effectuer des visites à domicile. Mais en réalité, loin de briser les chaînes de contamination, ils étaient condamnés à jouer aux devinettes avec le premier maillon.

- **Impossible aussi de faire circuler correctement l'information**. Par exemple, la tâche des collectivités locales aurait été grandement facilitée si celles-ci avaient pu identifier les personnes vulnérables (pour la distribution de masques etc.).

- **Heureusement, des entreprises privées ont parfois pris le relai**, par exemple *Doctolib* pour la campagne de vaccination. La société civile a également fait preuve d'un dynamisme qu'il faut saluer – mais tout de même, est-il rassurant qu'un informaticien de 24 ans, Guillaume Rozier, fasse mieux que Santé Publique France avec *CovidTracker*, et mieux que l'Assurance maladie avec *ViteMaDose* ?

Tout cela se serait passé différemment si nous avions disposé d'un système de santé organisé autour d'une « plateforme », où chaque usager dispose d'un identifiant unique, et où tous les services sont connectés entre eux. C'est par exemple le cas de **l'Estonie**, qui a ainsi bénéficié d'un atout précieux dès les premiers jours de la crise.

C'est précisément **l'objectif poursuivi par le grand chantier du numérique en santé**, mais celui-ci se heurte depuis des décennies à l'éclatement des acteurs et au poids de l'histoire. **Un tournant majeur a eu lieu en 2019** avec sa reprise en main, il faudra encore des années pour rattraper le retard accumulé.

- **Avec l'espace numérique de santé (ENS), la stratégie « tester, alerter, protéger » aurait été autrement plus efficace**, puisqu'il aurait été possible d'avoir au même endroit non seulement les données de SI-DEP, Contact-Covid et Vaccin-Covid, mais aussi tout l'historique médical du patient, avec ses facteurs de risque et comorbidités, grâce au **dossier médical partagé (DMP)** – un chantier lancé en 2004.

- Outre le DMP, chacun aurait aussi disposé d'une **messagerie sécurisée**, d'une application de **prise de rendez-vous** pour les tests et les vaccins, d'un outil de **e-prescription**, et d'un **catalogue d'applications tierces**, utilisant notamment des objets connectés.

- **L'identifiant national de santé (INS)** aurait aussi été un atout précieux. Aujourd'hui, nous sommes tous associés à **une multitude d'identifiants « locaux »**, à l'hôpital, chez le généraliste, chez le dentiste, au laboratoire etc., sources de multiples erreurs et de démarches administratives au détriment du « temps médical ». En temps de crise, alors que les hôpitaux sont surchargés, les conséquences peuvent être dramatiques.

Le *Health Data Hub*

Créée en 2019, la plateforme des données de santé (PDS) est **un entrepôt de données médicales agrégées et pseudonymisées**, **qui offre un guichet unique pour la recherche médicale**. Avec le HDH, la France pourrait devenir le leader mondial en matière d'IA appliquée à la santé.

Son intérêt dans le cadre d'une crise comme celle du Covid-19 est évident, et quelques projets de recherche en ont d'ailleurs bénéficié. **Mais le HDH n'en est qu'à ses balbutiements**, et à vrai dire, c'est surtout l'opposition de la CNIL à l'hébergement du HDH (quoique temporaire et partiel) par Microsoft qui a jusqu'à maintenant retenu le plus d'attention.

- **Chacun dispose pourtant d'un numéro unique et fiable, le numéro de Sécurité sociale (NIR)**, **mais la CNIL s'est toujours opposée** à son utilisation dans le domaine de la santé, au nom de la protection de la vie privée. Ce n'est qu'en 2019 que la **loi Santé** a permis d'utiliser le NIR comme base de l'INS, mais les choses prennent du temps et son utilisation, en théorie obligatoire depuis le 1er janvier, est encore loin d'être généralisée.

B. LE PRIX DE NOS TABOUS ET DE NOS CONTRADICTIONS

Il existe en France un tabou autour de la collecte de données personnelles et de croisements de fichiers par « l'État » (au sens large). C'est la deuxième grande raison du retard numérique de la France dans la crise sanitaire, bien plus fondamentale en fait que les aspects techniques qui n'en sont que la conséquence.

Ce tabou est au cœur de la doctrine de la CNIL, nettement plus conservatrice que ses homologues européennes en matière de croisements de fichiers par les pouvoirs publics, alors même que **tous sont soumis au RGPD** – le texte le plus protecteur au monde pour la vie privée, que les rapporteurs ne remettent nullement en cause.

Ainsi, c'est bien un obstacle juridique, et non technique, qui explique **l'absence d'interconnexion** entre les fichiers SI-DEP, Contact-Covid et Vaccin-Covid. C'est ce même obstacle qui explique le retard pris par le DMP, par l'INS, et par **le chantier de l'identité numérique en général**.

- De fait, la doctrine de « cantonnement » de la CNIL oblige chaque administration, au nom de la protection de la vie privée, à attribuer des **identifiants sectoriels spécifiques** : numéro de Sécurité sociale, numéro fiscal, numéro d'élève ou encore d'étudiant etc.

- **Pourtant, dans de nombreux pays, la question ne se pose même pas** : chaque citoyen dispose d'un numéro d'identification unique, qui relie toutes ses données et qui lui permet d'accéder à l'ensemble des services publics, de façon simple et sécurisée. **En Estonie, en Allemagne ou encore en Belgique, l'identité numérique est obligatoire**.

Lors de la crise sanitaire, **la doctrine de la CNIL en matière de captation d'images** a également rendu impossibles certains outils pourtant largement employés ailleurs :

- **Interdiction pour la RATP d'utiliser des caméras de détection du port du masque** en raison du risque d'identification… alors mêmes que ces caméras ne conservaient aucune image et ne transmettaient que des statistiques agrégées toutes les 15 minutes.

- **Refus de l'usage de caméras thermiques** au motif que la fièvre n'est pas un symptôme *systématique* du Covid-19 : il serait donc préférable de ne détecter personne plutôt que de ne pas détecter tout le monde…

- **Interdiction d'utiliser des drones pour contrôler le respect du confinement** (et pour tout le reste), car les images de la caméra sont visibles en direct par le pilote, *avant* le floutage automatique des visages. Ne serait-ce que pour des raisons de sûreté aérienne, il apparaît toutefois difficile de faire autrement.

TousAntiCovid, cas d'école des contradictions françaises

<u>L'objectif</u>

- 2 priorités très politiques : une appli de *contact tracing* **totalement anonyme** mais aussi « **souveraine** ».

- Développement par l'Inria d'un **protocole spécifique « centralisé »**, alors que la quasi-totalité des autres pays choisissaient le protocole « décentralisé » d'Apple et Google.

- ***StopCovid*** est lancé le 2 juin 2020, après d'intenses polémiques. L'application devient ***TousAntiCovid*** le 22 octobre suivant.

<u>Le résultat</u>

- En réalité, **le protocole « centralisé » n'est pas plus sécurisé ni plus anonyme** que le « décentralisé ».

- Par contre, du fait de ce choix, *TousAntiCovid* **ne fonctionne pas sur les *iPhones*, et n'est pas interopérable** avec les applications des autres pays.

- **Une faible adoption** : 1,7 million de téléchargements (2 % de la population) un mois après son lancement, quand l'Allemagne en était à 6 millions en moins de deux jours. Le rattrapage partiel (22 % de la population à ce jour) n'est pas lié au *contact tracing* mais aux **nouvelles fonctionnalités** (infos, attestation, certificat…).

- **Une utilité limitée** : seules 4,5 % des personnes testées positives jouent le jeu et se déclarent dans l'application. **Seuls 1 % des utilisateurs ont donc pu être prévenus** qu'ils étaient cas contact, contre 8 % au Royaume-Uni. Aucune étude d'impact n'a été réalisée.

La sensibilité française sur le sujet est ancienne et profonde, et elle n'est pas dénuée de toute justification historique. Dans l'imaginaire collectif, la collecte des données est **associée à l'idée d'un État policier et d'un « fichage » de la population**, et c'est cette même idée qu'on retrouve à chaque fois que les gouvernements successifs souhaitent avancer sur le sujet, du fichier *SAFARI* en 1974 à *TousAntiCovid*.

Mais cette sensibilité est aussi devenue coûteuse, et ceci d'autant plus qu'elle repose sur un grand nombre de fantasmes et d'incompréhensions, qu'il faut avoir le courage d'affronter. En effet :

- **À l'heure de la révolution numérique, du *big data* et de l'IA en santé**, on ne peut plus raisonnablement soutenir que le seul intérêt des croisements de fichiers soit l'instauration d'un État totalitaire.

- **Le « blocage » français repose sur une confusion entre les *fins*** (protéger la vie privée) **et les *moyens*** (interdire les croisements de fichiers). Dans les années 1970, il n'était pas absurde de lier les deux : c'était encore la meilleure garantie possible, à une époque où on était bien loin, par ailleurs, d'imaginer les possibilités immenses du numérique. Aujourd'hui, les choses sont différentes : **il existe bien d'autres façons de garantir à la fois la confidentialité des données et leur sécurité, sans pour autant s'interdire de les utiliser**, comme par exemple la *blockchain* ou l'*open source*. En somme, tout se passe comme si nous conservions **une préférence pour l'inefficacité**.

- **Ne nous trompons pas de *Big Brother*** : à chaque instant de notre vie, nous livrons aux **GAFA** bien plus de données que l'État n'en aura jamais, à des fins commerciales et sans aucune des garanties qu'offre le contrôle démocratique. Mais quand il s'agit d'intérêt général, de protection de la santé publique, et plus largement d'amélioration du service public, le moindre croisement de fichier suscite des polémiques infinies. **Faut-il s'étonner, ensuite, que Google et Facebook en sachent davantage sur l'épidémie de Covid-19** en France que le ministère de la Santé ou l'Assurance maladie ?

- **Si nous ne nous préparons pas, d'autres le feront à notre place**. Ce n'est certainement pas en laissant les régimes les plus autoritaires prendre une avance décisive en ce domaine, ou en abandonnant aux GAFA le soin de lutter contre les épidémies (et quoi d'autre demain ?), que nous défendrons au mieux nos « valeurs démocratiques ».

Comment, dès lors, répondre à une crise avec toute l'efficacité du numérique, sans rien céder sur nos valeurs démocratiques ?

3. LE *CRISIS DATA HUB*, BOÎTE À OUTILS POUR UNE RÉPONSE GRADUÉE

A. LE NUMÉRIQUE, UN ALLIÉ DE NOS LIBERTÉS FACE AUX CRISES

Le rapport défend une position claire : **à l'avenir, nous devrons recourir bien plus fortement aux outils numériques, en assumant si nécessaire des mesures plus intrusives, mais aussi plus ciblées et limitées dans le temps**. Avec, pour contrepartie, une liberté retrouvée plus vite dans le « monde réel ».

Toutefois, le rapport ne préconise aucun outil numérique en particulier. Il estime, précisément, qu'il est impossible de savoir à l'avance de quoi les prochaines crises seront faites, et quels seront les meilleurs moyens d'y répondre. C'est pourquoi, plutôt que de proposer tel ou tel outil, il défend **le principe d'une « boîte à outils » numérique**, à laquelle il serait possible de **recourir de façon graduée** en fonction des circonstances, à condition toutefois de s'y être préparés. En tout état de cause, **rien n'est pire que l'improvisation**, qui souvent se révèle à la fois moins efficace et bien plus attentatoire aux libertés publiques.

Deux principes fondamentaux sous-tendent le rapport : la **proportionnalité** des mesures, et leur **individualisation**.

Premier principe fondamental : la <u>proportionnalité</u> des mesures.

- Les perspectives ouvertes par le recours au numérique dans la gestion des crises soulève **d'importantes interrogations quant à la protection des droits et libertés**.
- **Toutefois, raisonner en termes absolus n'a strictement aucun sens** : des atteintes considérées comme inacceptables face à une menace modérée ne le seront pas forcément face à une crise plus grave.
- **Même si ce n'est ni le plus probable, ni le plus plaisant, il est de notre responsabilité d'imaginer le pire**. Le taux de létalité du Covid-19 est autour de 1 %. Que se passerait-il si demain nous étions frappés par une maladie plus virulente, ou qui touche en priorité les jeunes adultes, comme ce fut le cas avec la grippe espagnole, avec ses 100 millions de morts (5 % de l'humanité) pour un taux de létalité de 3 % ? La médecine a progressé, mais trouver un vaccin n'est jamais garanti, et notre époque a aussi ses propres vulnérabilités : la mondialisation, le risque de bioterrorisme etc.

<u>Quelques exemples</u>

Face à une crise « modérée », qui appelle surtout des mesures de « freinage » pour éviter la surcharge des hôpitaux, de simples outils d'information et de coordination bien pensés pourraient suffire.

Face à une menace un peu plus grave, on pourrait imaginer l'envoi automatique d'un SMS à tout individu qui s'éloignerait de son domicile pendant le couvre-feu, à simple titre de rappel et sans aucune remontée d'information.

Dans les cas les plus extrêmes, des mesures plus fortes pourraient s'avérer indispensables : ainsi, toute violation de quarantaine pourrait conduire à une information en temps réel des forces de l'ordre, à une désactivation du titre de transport, ou encore à une amende prélevée automatiquement sur son compte bancaire – comme le font, du reste, les radars routiers.

La proportionnalité, c'est aussi comparer les atteintes portées aux libertés « numériques » à celles portées aux libertés « physiques ». **Or celles-ci ont été bien plus lourdes, ont duré bien plus longtemps**, et se sont appliquées à tous de façon aveugle. Il faut se poser la question honnêtement : le risque qu'un individu soit reconnu par le croisement de deux informations que l'administration possède déjà sur lui vaut-il vraiment une interdiction de sortir de son domicile pendant plusieurs mois ?

Deuxième principe fondamental : <u>l'individualisation</u> des mesures.

- Plus les technologies sont intrusives, plus elles peuvent être **individualisées, ciblées, et limitées dans le temps.** Des mesures fortes concernant peu de monde pourraient permettre d'en finir rapidement avec une épidémie, pour le bénéfice de tous.
- **À la place, nous avons préféré mettre en place des restrictions généralisées mais impossibles à contrôler**, en interdisant à 67 millions de Français de sortir de chez eux pendant plusieurs mois sauf motif impérieux, en mettant toute la société sous cloche, sans pour autant réussir à éliminer le virus. Nous sommes restés « libres et égaux », mais confinés.

<u>Exemple</u>

<u>Mesure</u> : une quarantaine obligatoire *pour les seules personnes positives*, strictement contrôlée grâce à des outils numériques (géolocalisation en temps réel avec alerte des autorités et/ou sanction automatique si infraction).

<u>Ciblage</u> : 0,1 % de la population (65 000 personnes), correspondant au taux d'incidence constaté fin mai 2021. **Aucune restriction ne serait imposée aux 99,9 % du reste de la population**, et l'épidémie serait arrêtée rapidement.

B. QU'EST-CE-QUE LE *CRISIS DATA HUB* ?

Le *Crisis Data Hub* (CDH) est une plateforme sécurisée de collecte et d'échange de données dont l'unique fonction est de répondre aux situations de crise (sanitaire ou autre), lorsque des croisements de données massifs et dérogatoires deviennent indispensables, pour sauver des vies sans condamner le pays.

Les données en question sont **soit des données personnelles qu'il est inconcevable d'exploiter en temps « normal »** (par exemple des données médicales croisées avec des données de géolocalisation), **soit des données produites par des acteurs privés** (opérateurs télécom, entreprises technologiques, entreprises de transport, établissements financiers etc.) **qui n'ont aucune raison ni obligation de les fournir par ailleurs, ni même de s'y préparer**.

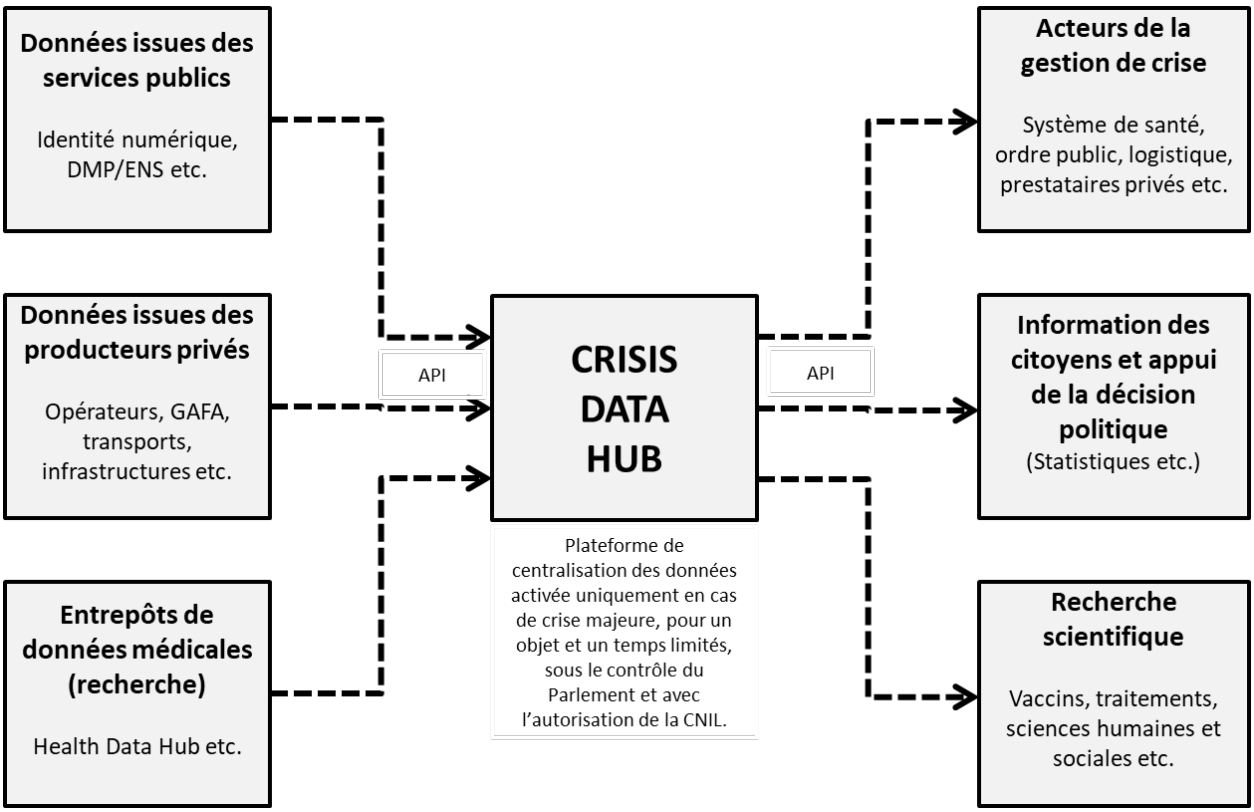
Le rapport ne propose *en aucun cas* de collecter ces données, mais **seulement de nous mettre en capacité technique et juridique de le faire rapidement, si jamais les circonstances devaient l'exiger**, pour ainsi dire en appuyant sur un bouton.

Concrètement, le *Crisis Data Hub* c'est donc :

- **Sur le plan technique, une plateforme *cloud* sécurisée** qui ne serait activée qu'en temps de crise, et qui permettrait, *via* **une série d'API**, de centraliser les données utiles et de les redistribuer aux acteurs qui en ont besoin : établissements de santé, sécurité civile, forces de l'ordre, collectivités, transports, prestataires etc.
- **En temps « normal », aucune donnée ne serait bien sûr transmise**, mais le système serait prêt, grâce à un travail continu de maintenance et d'amélioration.
- **Sur le plan juridique, une obligation légale, pour certaines entreprises et administrations**, de maintenir des bases de données dont le contenu et le format seraient fixés à l'avance, et de se tenir prêtes à les « brancher » à la plateforme en cas de nécessité.
- La liste des acteurs concernés pourrait s'inspirer de **la liste des 250 opérateurs d'importance vitale (OIV)**, soumis à des obligations particulières et accompagnés par l'agence nationale de cybersécurité (ANSSI).

Loin d'être une menace pour les libertés individuelles et la démocratie, cette préparation *en amont* est la meilleure des garanties que l'on puisse y apporter – bien meilleure, en tout cas, que l'improvisation.

- **Elle permettrait au débat démocratique de se ternir sereinement**, **en prenant le temps de la réflexion et de la pédagogie**, plutôt que de réagir « à chaud » et au cas par cas sur chaque mesure, avec les inévitables polémiques et contradictions.
- **La CNIL pourrait établir une doctrine préalable d'autorisation** de chaque dispositif en fonction de « scénarios ». Le **juge** pourrait se prononcer sans la pression de l'urgence. Une procédure de **rescrit** spécifique pourrait être créée.
- **Les outils du CDH seraient développés en *open source*** : chacun pourra vérifier qu'ils ne font rien d'autre que ce qu'ils sont censés faire. Les données agrégées seraient publiées en *open data*. **Aucun pays, face à la crise du Covid-19, n'a fait preuve d'une telle transparence**.
- **En cas de crise, l'« activation » du CDH revêtirait une forme solennelle**, par exemple *via* un article spécifique de la loi proclamant l'état d'urgence, qui permettrait de dégager **une majorité politique claire**, de **fixer les limites** (de durée notamment) et, au sein de celles-ci, de **laisser au Gouvernement la marge de manœuvre nécessaire.**
- En contrepartie, la mise en œuvre des différents dispositifs ferait l'objet d'une **procédure de contrôle spécifique, en continu, impliquant le Parlement, la CNIL ou encore la société civile**, afin non seulement de créer les conditions de la confiance des citoyens, mais aussi de son maintien dans la durée.



Pourquoi « *Crisis Data Hub* » ?

Le nom est inspiré du *Health Data Hub*. La différence est que le HDH ne centralise que des données médicales et pseudonymisées mais qu'il le fait massivement et en permanence, tandis que le CDH collecterait des données plus variées et nominatives, mais sur un champ bien plus restreint et surtout pendant une période très limitée.

- **De multiples cas d'usage** : épidémie, catastrophe naturelle (inondation, tremblement de terre etc.) ou technologique (accident industriel ou nucléaire, chute de débris spatiaux etc.) et risques NRBC (*nucléaires, radiologiques, biologiques, chimiques*) en général. Ils peuvent résulter d'un accident mais aussi d'une attaque (conventionnelle ou terroriste, en particulier bioterroriste).

- **Une expérimentation possible** : c'est l'avantage d'un dispositif conçu comme une « boîte à outils ». Pourquoi pas au niveau des **collectivités locales**, qui portent assistance aux personnes vulnérables pendant les crises ?

Rapporteurs

Véronique Guillotin
(Meurthe-et-Moselle, RDSE)

Christine Lavarde
(Hauts-de-Seine, LR)

René-Paul Savary
(Marne, LR)

Délégation à la prospective
http://www.senat.fr/commission/prospective/index.html