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

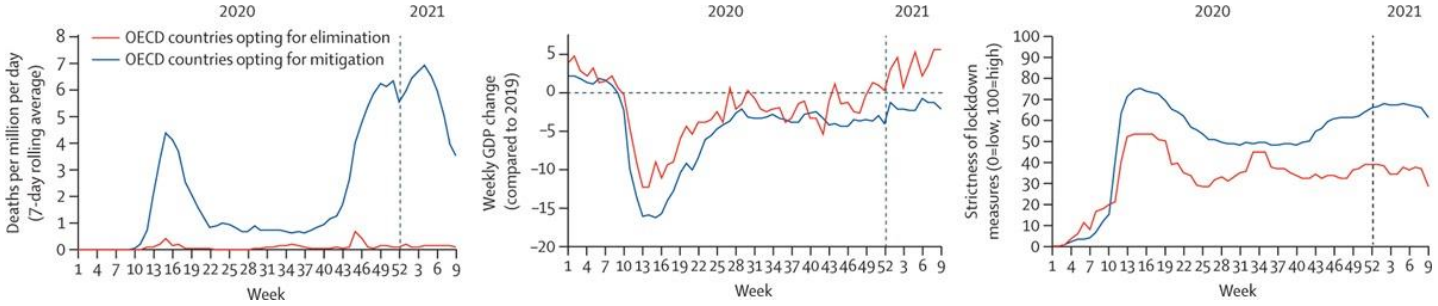
Source : Johns Hopkins University (5 mai 2021)

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**.

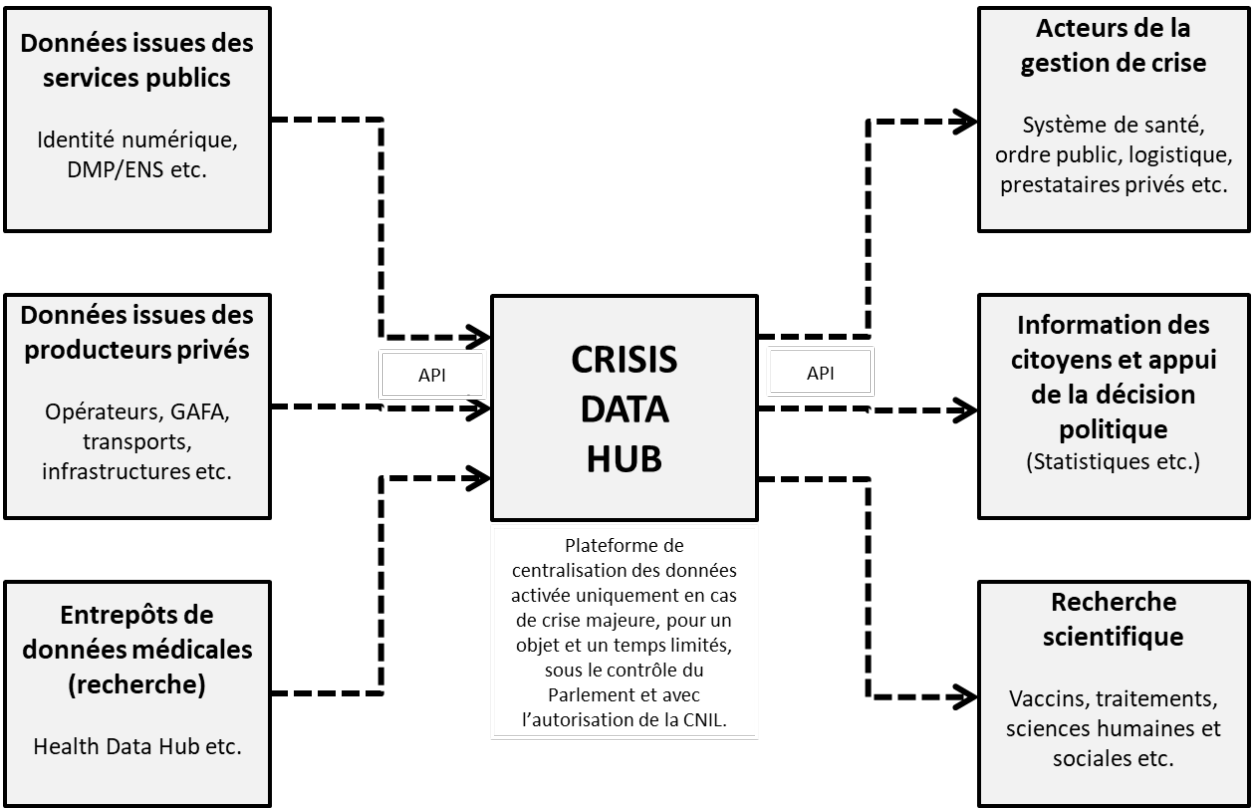
Le rapport ne propose *en aucun cas* de collecter ces données, mais **seulement de nous mettre en capacité technique et juridique de le faire rapidement, si jamais les circonstances devaient l'exiger**, pour ainsi dire en appuyant sur un bouton.

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