LIGUE DES DROITS DE L'HOMME

Section de Nice

Observations sur le rapport de la délégation sénatoriale à la prospective

CRISES SANITAIRES ET OUTILS NUMERIQUES (juin 2021)

Rapport présenté par :

Véronique Guillotin : Vice-présidente de la délégation sénatoriale à la prospective - Docteur en médecine - Groupe rassemblement démocratique et social européen.

Christine Lavarde : Vice-présidente de la délégation sénatoriale à la prospective - Ingénieure du corps des Ponts - Groupe Les Républicains.

René-Paul Savary : Vice-président de la délégation sénatoriale à la prospective - Docteur en médecine - Groupe Les Républicains.

*

« quarantaine obligatoire pour les seules personnes positives strictement contrôlée grâce à des outils numériques (géolocalisation en temps réel avec alerte des autorités »

« dans les cas les plus extrêmes […] 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 »

« 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. 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 »

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.

Quatre citations extraites du rapport de 182 pages « Crises sanitaires et outils numériques » produit par la délégation sénatoriale à la prospective [ICI]. Nous avons tenté de comprendre les raisonnements qui conduisent la délégation sénatoriale à conclure son rapport par les propositions dignes d'une dictature policière. Prenant exemple sur certaines modalités de gestion de la pandémie observées dans les pays d'Asie Orientale, le rapport s'attache ensuite à démontrer que les concepts fondamentaux de proportionnalité et de nécessité dont la CNIL est la gardienne sont désormais caducs, au moins, dans leur forme actuelle.

La gestion de la pandémie dans les pays d'Asie Orientale

Le rapport débute et prend appui sur une étude de la situation sanitaire de divers pays asiatiques (Chine, Hong-Kong, Taïwan, Singapour, Corée du sud et Japon) réalisée (avril 2020) par l'Institut Montaigne, think tank néo-libéral **(1)**, étude intitulée « L'Asie orientale face à la pandémie » [ICI]. Les rédacteurs de l'étude se proposent de comprendre « comment le Japon, la Corée du Sud ou encore Taïwan sont-ils parvenus à éviter un confinement général de leurs populations ou celui de villes entières ? »

Le rapport du Sénat en tire la conclusion que si les pays asiatiques ont mieux géré la crise sanitaire que les pays occidentaux, c'est parce qu'ils ont massivement mis en œuvre des moyens numériques de contrôle de la population, à l'exception du Japon. Or, cette conclusion nous semble contestable.

Outre que les données statistiques publiées par certains des pays étudiés, dirigés par des dictatures ou des démocraties autoritaires, sont sujettes à caution, de très nombreux autres paramètres peuvent expliquer d'éventuels meilleurs résultats :

- Insularité ou quasi insularité (Taïwan, Corée du Sud, Japon, Singapour, Hong-Kong) qui permettent un contrôle très strict des frontières (comparativement à la France)
- Flux touristiques plus limités qu'en occident.

- Organisation sociale, encadrement des populations et disposition d'esprit des citoyens plus favorables à une discipline sanitaire stricte. Par exemple, le port du masque est habituel dans plusieurs de ces pays depuis des décennies ; en Chine, le quadrillage et le contrôle physique de la population se fait dans les grandes métropoles jusqu'au niveau du pâté d'immeubles, sans parler du contrôle absolu des médias.
- Meilleure organisation administrative et surtout, comme le note l'étude de l'institut Montaigne, très grande réactivité des administrations face au danger pandémique, comme par exemple la mise en place très rapide de tests généralisés ou de contrôles sanitaires draconiens aux frontières terrestres et maritimes et l'imposition de sévères mesures de quarantaine aux arrivants.

Le contrôle numérique intrusif des populations a pu jouer un rôle dans les éventuels meilleurs résultats obtenus par les pays d'Asie orientale ; mais laisser entendre - comme le suggère le rapport du Sénat - que ces contrôles intrusifs ont joué un rôle central dans la maîtrise de la pandémie ne relève pas d'une démarche scientifique, parce qu'il est impossible de quantifier la contribution de chacun des items au meilleur résultat qui aurait été obtenu par les pays asiatiques étudiés. **(2)**

La CNIL , la proportionnalité et la nécessité

Après avoir tenté de démontrer que les pays d'Asie orientale, en adoptant des procédures numériques extrêmement intrusives, avaient choisi la bonne procédure, le rapport tente de balayer les obstacles qui pourraient s'opposer en France à un développement du numérique intrusif.

Une des premières cibles est la CNIL, autorité administrative indépendante chargée dans notre pays de protéger les données personnelles en veillant, en particulier, au respect de la directive européenne transcrite en droit français sous le nom de règlement général de protection des données (RGPD) applicable en France à compter du 25 mai 2018. Le rapport affirme que la CNIL fait preuve d'« **un conservatisme juridique lourd de conséquences** » (page 92), suggérant ainsi que cette autorité administrative a été ou sera indirectement responsable du développement des pandémies en France. **(3)** C'est un parfait non-sens, puisque le rôle de la CNIL se limite à veiller à la bonne application de la loi voté par le parlement, donc, aussi, par ... le Sénat.

On sait que le RGPD pose des principes, traditionnels en droit public français, de proportionnalité et de nécessité.

Concernant la proportionnalité, le rapport critique les positions de la CNIL en ce qu'elles méconnaissent un nouveau concept juridique selon lequel ce sont les **« libertés numériques » qui devraient être subordonnées aux « libertés physiques »** (page 103). Par « libertés physiques » les auteurs entendent la liberté de rester en bonne santé. Les limitations aux libertés individuelles pour motifs de santé publique sont anciennes, nombreuses et légitimes : vaccinations obligatoires, hospitalisation d'office, loi Evin, etc. (voir, par exemple, [ICI].

Mais ce que propose le rapport est de nature totalement différente : ce ne sont pas des limitations d'aller et de venir ou des obligations plus ou moins contraignantes de faire ou de ne pas faire, mais une **intrusion massive dans la vie privée** des citoyens. Au demeurant, cette **opposition numérique/physique, qui est centrale dans le raisonnement développé par le rapport**, n'a pas

beaucoup de sens. En effet, il suffit de penser au cas du logiciel Israélien « Pégasus » utilisé par certaines dictatures pour espionner les opposants (« libertés numériques »), afin de pouvoir plus efficacement porter atteinte à leurs (« libertés physiques »).

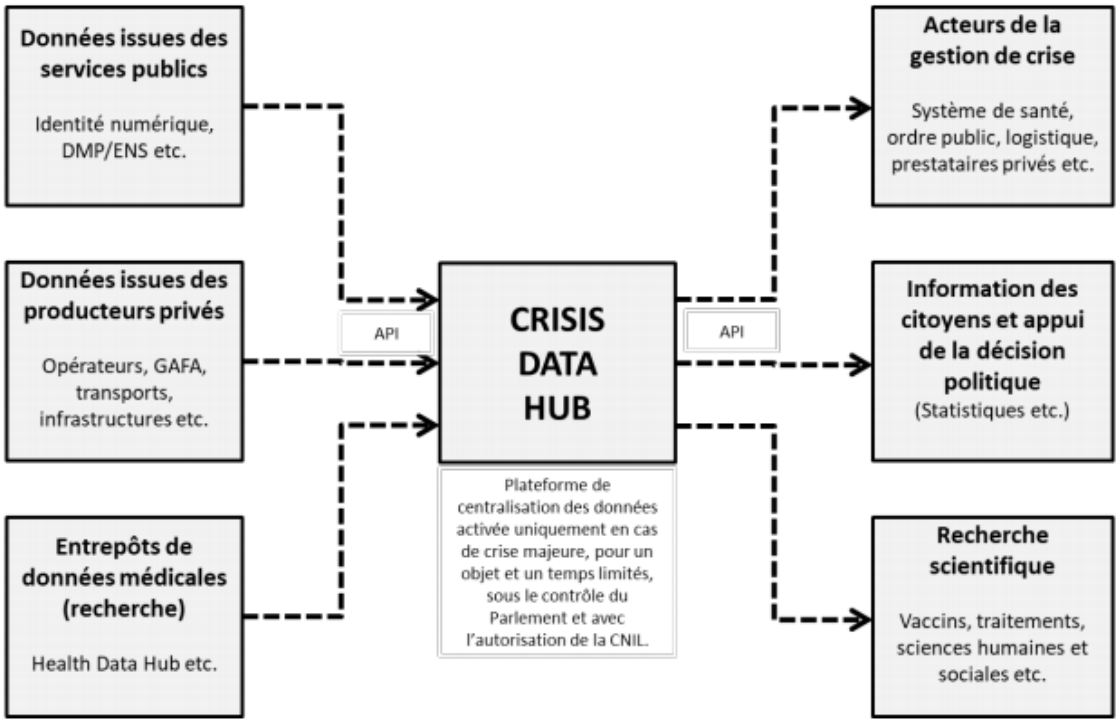
Ce concept central du rapport qui priorise les « libertés » physiques Vs les numériques est idéologiquement le pendant du concept conservateur qui voudrait privilégier ou même opposer sécurité et libertés [ICI]. François Sureau explique : « quand on écoute un homme politique parler, il faut toujours voir ce qu'il met en premier ; par exemple s'il vous dit la liberté c'est bien, mais la sécurité ça compte, vous pouvez être sûr que ce dont il parle, c'est de la sécurité » [ICI]. Ce discours est sous-tendu par la même idéologie qui fait dire à M. Ciotti qu'il faut chercher un « équilibre logique entre droits et devoirs pour les bénéficiaires des prestations sociales » (2011) ; à M. Sarkozy que « les droits sans les devoirs, ça n'existe pas » (2012) ou à M. Macron : « vous avez des devoirs avant d'avoir des droits » (2021). Au fond, ce qui est contesté, c'est l'existence des libertés fondamentales dont tout membre de l'espèce humaine est le dépositaire ; les conservateurs voudraient les contextualiser, voire le contractualiser ! Les libertés fondamentales ne sont pas négociables.

Concernant le principe de nécessité, le rapport observe que la CNIL n'a pas de compétence médicale et est donc amenée à prendre des décisions dont elle ne maîtrise pas tous les paramètres **(4)** et reproche aussi à la CNIL d'avoir interdit l'utilisation des caméras thermiques sur la voie publique au motif de l'imprécision des mesures et des cas asymptomatiques. Le rapport conclut cette séquence en élargissant le propos : « *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)* » (page 106). Le rapport prétend qu'il est possible de croiser les fichiers tout en protégeant les données personnelles, alors que de nombreux spécialistes expliquent que ce sont précisément les croisements de masses considérables de données (tel que les pratiquent les GAFAM) qui portent atteinte aux libertés individuelles.

Le crisis data hub

Le crisis data hub peut être défini comme étant une base de données alimentée par des croisements de fichiers, en particulier de fichiers de données personnelles (dont médicales), en principe utilisable uniquement en cas de crise, par exemple, pour contrôler un confinement ciblé.

Présentation simplifiée du *Crisis Data Hub*



Source : délégation sénatoriale à la prospective

Pour justifier une éventuelle intrusion massive dans les données personnelles des citoyens et en particulier les données personnelles de santé, le rapport développe une série d'arguments :

- On peut comprendre « la sensibilité française à toute **collecte et croisement de données** personnelles (allusion, sans doute, à l'utilisation du fichier des juifs sous l'occupation), mais à l'heure actuelle c'est « absurde » puisqu'on donne volontairement aux Gafam « d'avantage d'informations que l'Etat n'en aura jamais ». Cet argument rappelle celui utilisé pour justifier la reconnaissance faciale : « puisque vous mettez vos photos sur les réseaux sociaux, pourquoi la reconnaissance faciale vous poserait un problème ? ». Pour le dire autrement : puisque vous avez mis le petit doigt dans l'engrenage, vous n'avez aucune raison de refuser d'y passer tout le bras, voire plus. Sauf que, d'une part, **tous** les citoyens ne mettent pas leurs photos sur les réseaux sociaux et, d'autre part, pour le moment, les réseaux sociaux n'ont pas la capacité de nous contraindre physiquement : perquisitions, gardes à vue, prison, etc. (ça viendra peut-être …)

- « *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*** », mais c'est faux, répond le rapport, regardez le Japon, Israël ou l'Estonie **(5).** Israël ? un pays en guerre depuis 70 ans, grand pourvoyeur de logiciels espions à toutes les dictatures du monde (cf. affaire Pégasus et autres outils numériques d'espionnage) ; pour l'Estonie, cf. note n°2.

- *« 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. »* Certes, le croisement de données personnelles pourrait être utilisé à d'autres fins que des fins policières comme par exemple la recherche médicale ; en France, l'INSERM mène depuis plus de 20 ans des enquêtes épidémiologiques à grande échelle, sur la base du **volontariat**. En tout état de cause, ces techniques pourraient aussi être utilisées à des fins policières. Un récent projet de loi (juillet 2021) prévoit, que le fichier médical SI-DEP (Système d'Informations de DEPistage) puisse être consulté par des policiers : « On change complètement la finalité d'un fichier. On l'a créé pour qu'il soit médical et il devient finalement un fichier policier ». [ICI]

- *« il existe aujourd'hui des solutions techniques permettant de garantir un très haut niveau de **confidentialité** et de **sécurité** »* Discours habituel : « faites-nous confiance, tout est sous contrôle ». Or, très régulièrement, la presse se fait l'écho d'intrusions dans des systèmes informatiques parmi les plus protégés au monde comme par exemple le hack de la NSA [ICI]. D'ailleurs, les rédacteurs sont tellement conscients de la faiblesse de cet argument que l'adjectif sécurisé est cité, tel un mantra, 60 fois dans le rapport, pour tenter de bien ancrer l'idée dans la tête du lecteur. Fin août 2021, on apprend que « *Plus de 700 000 résultats de tests, et les données personnelles des patients, ont été durant des mois accessibles en quelques clics en raison de failles béantes sur le site de Francetest, un logiciel transférant les données des pharmaciens vers le fichier SI-DEP* » (Médiapart 31-8-231)

L'entêtement du rapport à présenter l'intrusion numérique comme l'axe central et incontournable de la politique publique en cas de nouvelle pandémie pose problème ; tout se passe comme si les rapporteurs avaient été hypnotisés par les marchands de solutionnisme techno. Cette option met de côté toute une série de progrès possibles dans le domaine de la médecine (tests plus faciles à pratiquer et plus efficaces, nouvelles molécules pour le traitement de la maladie, nouveaux vaccins plus efficaces, faciles à administrer et à diffuser, etc.) ou dans le domaine de l'organisation administrative de la lutte contre la pandémie et particulièrement en tirant les leçons de ce qui a très mal fonctionné lors de l'épisode que nous vivons actuellement et tout particulièrement l'absence de préparation à un tel événement, malgré l'alerte de l'épidémie H1N1 de 2009.

Le rapport insiste à plusieurs reprises sur le caractère limité dans l'espace et dans le temps des procédures ultra intrusives, comme par exemple p 126 : *« Le présent rapport propose donc de recourir bien plus fortement aux outils numériques dans le cadre de la gestion des crises sanitaires […] 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 »* ; toutefois, l'expérience vécue de ces vingt dernières années montre que les atteintes aux libertés individuelles et collectives présentées comme dirigées contre un unique ennemi (le terrorisme) et pour une durée très brève (état d'urgence) finit toujours, sous la pression policière, par être gravé définitivement dans le marbre de la loi qui s'applique en permanence **à tous et plus particulièrement aux opposants, aux journalistes, etc.** Il n'y a aucune raison de penser qu'il en irait autrement pour les dispositions si fortement intrusives proposées par la commission prospective du sénat.

*

(1) voir le comité directeur de l'Institut Montaigne [ICI]

(2) Pour parer à toute critique concernant la nature politique des pays étudiés, le rapport étudie aussi le cas d'une démocratie européenne : l'Estonie, pays doté d'une administration hyper informatisée, a fait l'objet en avril-mai 2007 d'une série de cyber attaques qui ont paralysé administrations et banques ; l'exemple de ce très petit pays, le plus septentrional des pays Baltes, avec **seulement 1,2 millions d'habitants,** peut-il vraiment servir de modèle pour un pays de près de 70 millions d'habitants ?

(3) cette attaque frontale contre les positions de la CNIL se combine de façon assez perverse avec l'assurance donnée que ce ne sont pas les statuts de la CNIL qui sont visés, pas plus que la réglementation européenne du RGPD (Règlement général de protection des données)

(4) comme les tribunaux administratifs, remarque le rapport

(5) Le Japon est cité comme une démocratie qui a utilisé des outils numériques intrusifs (page 101), mais page 22, le rapport indique : *« le Japon est, de loin, celui qui a le moins recouru à des mesures fortes, et a fortiori à des outils numériques […]Le Japon est aussi – faut-il y voir un hasard ? – celui de ces pays qui est le plus touché par l'épidémie »*