



HAL
open science

“ L'éthique : dernier rempart au traitement des données personnelles sensibles en temps de crise ”

Christina Koumpli Maître

► To cite this version:

Christina Koumpli Maître. “ L'éthique : dernier rempart au traitement des données personnelles sensibles en temps de crise ”. Jean-François Kerléo, Julien Padovani, Vanessa Barbé. L'éthique à l'épreuve de la crise, L'Épître, pp.217-234, 2021, L'Unité du Droit, 9791092684506. hal-04673902

HAL Id: hal-04673902

<https://hal.science/hal-04673902v1>

Submitted on 20 Aug 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright

L'éthique : dernier rempart au traitement des données personnelles sensibles en temps de crise

Christina Koumpli

Maître de conférences en droit public, Université d'Avignon, LBNC

*L'esclavage avilit l'homme jusqu'à s'en faire aimer ;
la vérité c'est que la liberté n'est précieuse qu'aux yeux
de ceux qui la possèdent effectivement.*
- Simon Weil, 1934 -

En matière de traitement de données personnelles sensibles, la France a de peu manqué d'être une exception et elle aurait pu en être fière. En effet, la création d'un nouveau type d'état d'urgence dit « sanitaire »¹ décidé par le Gouvernement, quelques jours après le début du premier confinement général de la population à partir du 17 mars 2020, avait laissé croire que ce dernier ne tomberait pas dans le piège liberticide de la mise en place d'une application utilisant les données personnelles pour lutter contre l'épidémie de Covid-19².

L'espoir né s'est cependant vite dissipé, non seulement parce que l'application « StopCovid » a bien été mise en œuvre à partir du 2 juillet 2020 (*via* une procédure contournant le contrôle du Conseil constitutionnel), mais surtout parce que bien avant cette date, deux autres fichiers bien plus attentatoires aux libertés individuelles ont été instaurés et ce avec l'aval du juge constitutionnel qui a réalisé un contrôle en apparence poussé mais en réalité limité³. Il s'agit des fichiers :

1. « SI-DEP » : service intégré de dépistage et de prévention qui permet le suivi des malades en centralisant les informations obtenues à travers les tests Covid-19 réalisés afin de les partager avec les acteurs sanitaires ;
2. « Contact Covid » : sous l'égide de l'Assurance maladie, ce dispositif, qui a obtenu l'aval du juge constitutionnel, permet de suivre les patients et d'identifier les cas contacts.

En outre, « considérant que la capacité à mobiliser les données de santé est un axe essentiel de la lutte contre l'épidémie de Covid-19 », un arrêté du 22 avril 2020 a autorisé le *Health Data Hub* et la Caisse nationale d'assurance maladie (Cnam) à collecter un large éventail de données « aux seules fins de faciliter l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le virus Covid-19 » ; une mesure qui porte *a priori* atteinte à la souveraineté numérique de la France⁴.

¹ RRAPI, P., « Le Préambule de la Constitution de 1946, fondement constitutionnel de l'état d'urgence », *Lettre Actualité Droits-Libertés du CREDOF*, 8 juin 2020, 9 p. Voir aussi les autres références doctrinales mentionnées par le Conseil constitutionnel dans la décision n° 2020-800 DC du 11 mai 2020.

² Il s'agit de ce qu'avait indiqué à l'AFP Cédric O., secrétaire d'État au Numérique, le 24 mars 2020. Voir : ROZENFELD, J., « L'urgence sanitaire : un test pour nos libertés », *Expertises des Systèmes d'Information*, n° 456, avril 2020, p. 123 ; CHEVALLIER, J., « Un nouvel outil numérique : StopCovid », *RFAP*, n° 174, 2020, p. 521.

³ WACHSMANN, P., « Les libertés et les mesures prises pour lutter contre la propagation du covid-19 », *La semaine juridique. Édition générale*, n° 20-21, 18 mai 2020, pp. 948-951.

⁴ CLUZEL-METAYER, L., « La datasurveillance de la Covid-19 », *RDSS*, 2020, pp. 918 et s.

Outre ces outils technologiques, mentionnons l'utilisation de drones par la Préfecture de Police de Paris afin de surveiller le respect des exigences de distanciation sociale par la population au nom de la lutte contre l'épidémie. Par une ordonnance de référé prise le 18 mai 2020⁵, le Conseil d'État a néanmoins fait cesser cet usage qui, selon ses propres termes, portait une atteinte « grave et manifestement illégale au droit au respect de la vie privée » au motif qu'il avait été employé en dehors du cadre prévu par la loi informatique et libertés (LIL) du 6 janvier 1978.

Ajoutons le développement rapide de caméras dites « intelligentes », tant dans l'espace public que dans les lieux ouverts au public (commerces, transports, lieux de travail), afin de permettre une prise de température automatique (caméras thermiques), détecter le port d'un masque et garantir le respect des mesures de distanciation sociale. Ainsi, de la même façon que nous avons appris à nous accommoder à l'exigence d'ouvrir notre sac à main depuis une vingtaine d'années avant d'entrer dans certains lieux en raison de la menace terroriste, il s'agit désormais de s'accommoder à la prise de sa température à chaque entrée dans une salle de sport, une boutique ou même à l'endroit où l'on travaille.

Ces quelques exemples nous permettent de constater que la solution technologique a été mobilisée à court (drones), moyen (application « StopCovid », fichiers « SI-DEP » et « ContactCovid ») et long terme (*Health Data Hub* et Cnam) au nom de la sécurité (sanitaire).

Or, une telle configuration pose plusieurs interrogations, notamment : *quid* dans une telle situation de la liberté sous-tendue par le concept de droit à la protection des données à caractère personnel ? ; *quid* de la protection particulière accordée à la catégorie des données sensibles dont relèvent les données de santé ? ; *quid*, plus précisément, de leur régime juridique qui, en principe, interdit leur traitement (article 9, RGPD) ?

Les colonnes des meilleures revues juridiques, comme des journaux à large diffusion, ont ainsi été remplies de contributions venant de la doctrine spécialisée en matière de libertés, et plus spécifiquement de protection des données personnelles, s'inquiétant de l'épreuve subie par ces dernières du fait de l'« urgence sanitaire »⁶.

La présente réflexion ne cherche pas à proposer une nouvelle contribution en ce sens mais plutôt à interroger la non-réaction du droit à l'égard de cette situation : pourquoi la résistance des boucliers juridiques protecteurs des données personnelles a-t-elle été aussi faible au moment où a été déclaré l'état d'urgence qui, justement, aurait dû présupposer une vigilance extrême des organes de contrôle à l'égard des restrictions apportées aux libertés individuelles ? Ce manque de réaction s'explique-t-il par le caractère provisoire du nouvel état d'urgence sécuritaire ou par la faiblesse intrinsèque de la protection juridique des données à caractère personnel ?

Notre démonstration consistera à observer que le droit étant perçu comme un ordre normatif beaucoup trop contraignant pour encadrer une activité en constante évolution tel que l'est le numérique, une activité caractérisée par un potentiel exponentiel autant en termes économiques

⁵ CE, ord., 18 mai 2020, *Association « La Quadrature du Net » et Ligue des Droits de l'Homme*, n° 440442 et n° 440445

⁶ À titre d'exemple, voir : METALLINOS, N., « Covid-19 : l'état d'urgence sanitaire à l'épreuve du droit de la protection des données à caractère personnel », *Communication Commerce Électronique*, n° 5, mai 2020, étude 9 ; WACHSMANN, P., « Les libertés et les mesures prises pour lutter contre la propagation du covid-19 », *op. cit.* ; CLUZEL-METAYER, L., « La dataturveillance de la Covid-19 », *op. cit.* ; MAXWELL, W., ZOLYNSKI, C., « Protection des données personnelles juillet 2019-mai 2020 », *Recueil Dalloz*, 2020, pp. 1262 et s. ; MATTATIA, F., « Suivi des populations pour lutter contre une épidémie et protection des données personnelles », *La Semaine juridique. Édition administrations et collectivités territoriales*, n° 18-19, 4 mai 2020, p. 2136 ; DESGENS-PASANAU, G., « Traçage des données mobiles : ne sacrifions pas la protection de nos données sur l'autel de la crise sanitaire », *La Semaine juridique. Édition générale*, n° 18, 4 mai 2020, p. 543.

que sécuritaires, il a été considéré comme préférable de conserver la forme juridique mais d'en atténuer la substance. Le droit est donc venu soutenir le solutionniste technologique de l'état d'urgence sanitaire, sauf rares exceptions qui sont intervenues *ex post*⁷ (I).

Ainsi, il convient de constater le début d'une ère dans laquelle la protection des données personnelles est entendue en tant qu'« alliée » de l'état d'urgence sanitaire (II). La protection des données personnelles repose désormais essentiellement sur l'éthique des responsables de leur traitement. Dès lors, le caractère raisonnable d'une mesure - élément du contrôle de proportionnalité - constitue la seule limite possible au traitement de données sensibles (en principe interdit). La « *privacy by ethics* » constituerait le nouveau élément central de la protection des données à caractère personnel⁸. Il suffit de lire le communiqué du Comité National Pilote d'Éthique du Numérique pour en prendre conscience⁹. Or, le traitement éthique des données personnelles est une notion très large et, en tout état de cause, difficilement appréciable. Il s'agira, à cet égard, de préciser certaines conséquences de ce changement de discours relatif à la protection des données à caractère personnel.

I. La fin de la « protection-limite »

Trois principaux arguments seront exposés à l'appui d'une démonstration de la fin de la conception envisageant la protection des données personnelles en tant que limite à l'état d'urgence : l'impossible concrétisation de l'interdiction de principe de traitement de données sensibles ; l'impossible contrainte du Gouvernement par l'avis de l'autorité administrative indépendante spécialisée en matière d'informatique et libertés (CNIL) ; l'impossibilité du juge constitutionnel de se prononcer clairement sur la mise en place d'une application de *contact-tracking*.

A. L'impossible interdiction du traitement de données sensibles

Il s'agit, en premier lieu, d'observer la manière dont la contrainte juridique s'est transformée en légitimité juridique. En particulier, on s'intéressera aux éléments susceptibles d'expliquer la facilité avec laquelle l'ordre juridique français a finalement accompagné tout ce qui était technologiquement possible au nom d'une lutte prétendue efficace contre le Covid-19.

La catégorisation des données à caractère personnel en tant que données sensibles ou non-sensibles s'accompagne de l'application d'un régime juridique *a priori* clair : le traitement des données sensibles est en principe *interdit* alors que celui des données non sensibles est en principe *permis sous certaines conditions*.

Or, les données de santé relevant de la catégorie des données sensibles, leur traitement est donc *en principe interdit*. Par ailleurs, leur traitement à grande échelle se voit appliquer un régime de protection plus forte qui, prévu par l'article 35 RGPD, exige une analyse d'impact préalable à la mise en place d'un tel traitement.

⁷ CE, ord., 26 juin 2020, *La Ligue des droits de l'Homme*, n° 441065. Voir le commentaire : DE MONTECLER, M.-C., « Quand l'usage des caméras thermiques est-il soumis au RGPD », *AJDA*, 1^{er} juillet 2020, p. 1319.

⁸ BOISSART, F., « Vers une "Privacy by Ethics" ? », *Dossiers d'actualité*, LexisNexis, 12/06/2020.

⁹ Communiqué du Comité National Pilote d'Éthique du Numérique (CNPEN), « Enjeux d'éthique du numérique du suivi épidémiologique en sortie de confinement », 29 avril 2020. On y lit, avec étonnement, l'insistance du Comité quant à « l'importance que représente la mise en place d'une application de suivi numérique de contacts ».

Toutefois, la règle connaît des exceptions qui sont bien plus nombreuses et bien plus concrètes que le principe ; surtout dans un contexte d'épidémie qui justifie plus facilement des dérogations.

Plus précisément, en dépit du principe d'interdiction du traitement des données de santé consacré à l'article 9§1 RGPD, une série d'exceptions a été prévue et pourrait être applicable à la situation sanitaire actuelle : : article 9 §§2a - consentement ; §2c - sauvegarde des intérêts vitaux de la personne ; §2g - motif d'intérêt public ; §2h - fins de médecine préventive ; §3 - traitement des professionnels de santé.

De plus, le RGPD laissant une marge de manœuvre importante aux législateurs nationaux en matière de données sensibles¹⁰, ces derniers ont adopté leurs propres règles qui sont venues légitimer les traitements de données de santé.

Ainsi, l'article 6-I de la LIL du 6 janvier 1978, dans sa rédaction issue de l'ordonnance n° 2018-1125 du 12 décembre 2018, réitère l'interdiction de principe de traitement de données concernant la santé mais son article 6-II mentionne que les exceptions à cette interdiction fixées par le RGPD s'appliquent également dans l'ordre juridique interne.

Il convient néanmoins de noter une différence notable entre le RGPD et la LIL quant à l'intérêt public justifiant le traitement de ce type de données.

L'article 9§2g RGPD prévoit que le motif d'intérêt public est une exception à l'interdiction de traitement et l'admet à la condition qu'il soit « proportionné à l'objectif poursuivi, respecte l'essence du droit à la protection des données et prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et intérêts de la personne concernée ». Par ailleurs, l'article 23 RGPD (limitations) prévoit dix bases juridiques autorisant les législateurs nationaux (et non le pouvoir réglementaire) à limiter la portée des obligations et droits prévus par le RGPD, à la condition que cette limitation « respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique ». Parmi ces dix fondements figurent la sécurité publique (article 23-1-c RGPD) ainsi que « la protection de la personne concernée ou des droits et libertés d'autrui » (article 23-1-i RGPD). Les dispositifs ainsi mis en place doivent, par conséquent, constituer des mesures nécessaires et proportionnées dans une société démocratique. Les responsables de traitements de données (publics ou privés) doivent respecter le cadre juridique prévu par le RGPD.

Or, l'article 6-III LIL ne dispose pas que les raisons d'intérêt public peuvent justifier une dérogation étant donné que d'après cette disposition, « ne sont pas soumis à l'interdiction prévue au I les traitements automatisés ou non, justifiés par l'intérêt public et autorisés suivant les modalités prévues aux I de l'article 31 et à l'article 32 » de la LIL.

En ce sens, si l'on admet que l'état d'urgence sanitaire justifie l'invocation de l'intérêt public en tant que fondement juridiquement valide du traitement de données de santé, il convient de

¹⁰ SENAT, Rapport d'information n°344 fait au nom de la commission des affaires européennes (1) sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à la protection des données personnelles (n° 296, 2017-2018), 8 mars 2018.

constater qu'il ne s'agit plus ici d'un traitement exceptionnel mais d'un traitement devenu « normal » dans un contexte sanitaire anormal.

La conséquence immédiate de cette situation se mesure d'abord en termes de contrôle de proportionnalité en supposant que celui-ci doit être plus approfondi lorsqu'on applique une dérogation (article 9§2g, RGPD) ou une limitation (article 23, RGPD) que lorsqu'on applique une norme dénuée de caractère dérogatoire (article 6-III, LIL).

B. La mise à l'écart de l'avis conforme de la CNIL

Sur la base d'une stricte lecture de la Constitution, le Conseil constitutionnel a validé, dans sa décision n° 2020-800 DC, la disparition de l'avis conforme de la CNIL ainsi que l'avait suggéré le Conseil d'État¹¹. La consultation obligatoire et contraignante de la CNIL avait à l'origine été voulue par le législateur agissant dans son rôle de garant de l'équilibre entre la protection de la santé et la limitation des libertés du fait du traitement de données à caractère personnel nécessaire en temps de crise sanitaire.

On aurait pu attendre du législateur de 2020 qu'il concilie l'obligation de confier au pouvoir exécutif des pouvoirs justifiables par l'urgence avec l'obligation de veiller au respect des libertés individuelles. L'avis conforme n'était pas obligatoire mais n'était pas interdit, ni par le texte constitutionnel ni par l'urgence. Il aurait assuré un équilibre institutionnel, fragilisé par la prorogation de l'état d'urgence sanitaire, et surtout manifesté - à tout le moins en apparence - une préoccupation pour les libertés individuelles tant éprouvées par la crise.

Le législateur a bien décidé de proroger l'état d'urgence en subordonnant à l'avis conforme de la CNIL le pouvoir réglementaire détenu par le Premier ministre. Cependant, le Conseil constitutionnel n'a pas validé cette position qui aurait lié le Premier ministre. En effet, celui-ci n'aurait pu se soustraire d'un tel avis qu'en s'abstenant d'édicter l'acte réglementaire en question mettant en place un traitement de données personnelles.

En outre, il convient de relever que les réserves émises par la CNIL n'ont pas d'incidence sur la légalité externe de l'acte réglementaire en question autorisant un traitement de données¹² lorsqu'il s'agit d'un avis public simple de la CNIL mais qu'elles ont des effets en cas d'avis conforme.

À l'instar du juge constitutionnel, la haute juridiction administrative a aussi réduit à néant le rôle de la CNIL dans le contexte d'urgence sanitaire.

En effet, dans un avis sur un projet de loi prorogeant l'état d'urgence sanitaire¹³, le Conseil d'État a admis que la consultation de la CNIL est requise à l'égard de tout projet de loi déterminant les caractéristiques essentielles ou les conditions de création ou de mise en œuvre d'un traitement ou d'une catégorie de traitements de données à caractère personnel. En revanche,

¹¹ CE, avis sur un projet de loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, 4 mai 2020, cons. 17-18.

¹² CE, 24 août 2011, *HSBC Private Bank (Suisse)*, n° 336382, Lebon T. 939.

¹³ CE, avis sur un projet de loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, n° 4000104, séance du vendredi 1^{er} mai 2020, NOR : PRMX2010645L/Verte-1, p. 7.

une telle consultation n'est pas requise pour des projets d'actes réglementaires adoptés par décret en Conseil d'État qui instituent des traitements de données personnelles.

Précisément, selon le Conseil d'État, le projet de loi en question :

« se borne à autoriser le pouvoir réglementaire à créer un ou plusieurs systèmes d'information aux fins précédemment mentionnées, sans en définir l'architecture générale, et à ne prévoir que certaines de ses modalités de mise en œuvre. En particulier, le projet renvoie à un décret en Conseil d'État la détermination des données qui seront accessibles aux personnes et organismes qu'il énumère ainsi que les services et personnels qui se verront reconnaître un tel accès. Le Conseil d'État estime, en conséquence, que ces dispositions ne déterminent pas dans leurs caractéristiques essentielles, les conditions de création ou de mise en œuvre d'un traitement ou d'une catégorie de traitements de données à caractère personnel, de sorte que la consultation préalable de la CNIL n'est requise ni sur le fondement de l'article 36.4 du RGPD ni sur celle de la loi du 6 janvier 1978 »¹⁴.

Ainsi, la haute juridiction administrative n'a pas même discuté la qualification de l'avis - en tant qu'avis simple ou avis conforme - et a d'emblée rejeté la consultation de la CNIL dans le cadre de l'état d'urgence au motif que le législateur s'est borné à habiliter le pouvoir réglementaire pour mettre en place le traitement des données. Son argumentation a donc essentiellement consisté à considérer que les paramètres du traitement envisagé n'étant pas élaborés par le législateur mais par le pouvoir réglementaire à travers un décret en Conseil d'État, la consultation obligatoire de la CNIL n'était pas indispensable étant donné que celle-ci ne l'est que dans les cas de traitements prévus par des projets de loi. De plus, le juge administratif s'est estimé suffisamment compétent pour apprécier la conformité du traitement au RGPD et à la LIL malgré sa technicité. Ce faisant, il a écarté la CNIL du paysage institutionnel consultatif en matière de traitement de données personnelles en se substituant à elle.

Or, s'agissant de l'avis public (simple), ce raisonnement est contraire tant au RGPD qu'à la LIL. En outre, le caractère erroné de l'avis du Conseil d'État peut également être avancé en ce qui concerne l'avis conforme en tenant compte de la sensibilité tant du traitement que du contexte dans lequel il est mis en place.

Concernant l'avis simple, rappelons que la position du Conseil d'État est contraire à la LIL puisque cette dernière prévoit, dans son article 8-2°-a, l'obligation de la CNIL de donner son avis (sans que cela lui soit demandé) s'agissant des traitements relatifs à la sécurité publique (art. 31, LIL) et de ceux mis en œuvre pour le compte de l'État (art. 32, LIL). De plus, l'article 8-4°-a de la LIL pose l'obligation des pouvoirs publics de consulter la CNIL sur « tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données » lorsque des technologies nouvelles sont développées afin d'apprécier les conséquences qui en résultent sur l'exercice des droits et libertés. Le législateur n'a donc fait aucune distinction entre un traitement prévu par un projet de loi et celui prévu par un décret s'agissant de l'exigence de consultation de la CNIL.

Quant au RGPD, il prévoit, dans son article 36§4, que « *les États membres consultent* l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être

¹⁴ *Ibidem*

adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».

En ce qui concerne l'avis conforme, il convient de se référer à l'histoire de la protection des données personnelles en France pour comprendre son intérêt en temps de crise sanitaire.

Afin d'autoriser des traitements portant sur des informations particulièrement sensibles, la loi de 1978 exigeait un avis conforme de la CNIL, lui accordant ainsi un véritable pouvoir de codécision que l'on peut envisager comme un partage du pouvoir réglementaire entre le Gouvernement et cette dernière ; ce à l'égard de deux types d'actes :

1. L'acte réglementaire autorisant des personnes morales gérant un service public à procéder au traitement de données relatives à des condamnations, infractions et mesures de sûreté (art. 30 al. 1, LIL 1978) ;
2. Les décrets en Conseil d'État autorisant, pour des motifs d'intérêt public, le traitement de données sensibles (art. 31, al. 3, LIL 1978) dont relèvent les données de santé.

Dans ces deux configurations, le pouvoir réglementaire ne pouvait passer outre l'avis de la CNIL. L'acte juridique définitif adopté à la suite d'un avis conforme était donc « l'œuvre de plusieurs agents publics »¹⁵.

Cette condition était une limitation préalable réelle au pouvoir réglementaire démontrant l'engagement du législateur de 1978 de faire de la CNIL un coauteur fonctionnel de la décision de l'autorité réglementaire ; une solution qui ne surprend guère dans un domaine aussi technique que l'informatique¹⁶.

Cependant, la loi du 6 août 2004 transposant la Directive 95/46/CE a transformé l'avis conforme de la CNIL en avis simple de telle sorte qu'un avis négatif de sa part ne peut désormais plus faire obstacle à la volonté du pouvoir réglementaire.

Ainsi, au moment de la prorogation de l'état d'urgence sanitaire en raison du Covid-19, la consultation de la CNIL était obligatoire selon l'article 8 LIL contrairement à ce qu'a affirmé le Conseil d'État. Sa qualification d'avis conforme aurait pu aussi être justifiée par la nature des données traitées et l'architecture générale du traitement envisagé ; elle aurait pu surtout être justifiée par sa mise en place dans une situation exceptionnelle qui requiert de veiller à la protection de la santé autant qu'aux garanties des libertés individuelles mises en péril par le « *solutionnisme technologique* ». Qui mieux que la CNIL, grâce à sa compétence technique, aurait pu apprécier le caractère intrusif du traitement au regard de tous ses aspects techniques, surtout dans le cadre d'un état d'urgence ?

Certes, la position du Conseil d'État peut se comprendre par le fait qu'il ne souhaitait pas se retrouver lié à l'avis de la CNIL, d'autant plus qu'il est récemment apparu comme un réel protecteur des données personnelles. Pour autant, le constat que le Conseil d'État ne souhaite pas se retrouver lié à l'avis de la CNIL n'empêche pas le législateur de le vouloir.

¹⁵ JEZE, G., *Les principes généraux du droit administratif*, Marcel Giard, Tome III, 1925, p. 278. Voir aussi : LAFERRIERE, E., *Traité de la juridiction administrative et des recours contentieux*, tome II, 1888, p. 505.

¹⁶ Notons également que le Conseil d'État avait déjà pu sanctionner pour vice d'incompétence l'omission d'avis conforme durant la procédure d'élaboration d'actes nécessitant une telle formalité. Voir : CE, 7 janvier 1955, *Sieur Ged*.

L'affaire a finalement dû être tranchée par le Conseil constitutionnel dont l'argumentation a été succincte. Précisément, l'inconstitutionnalité de l'avis conforme a été prononcée dans le considérant 77 de la décision n° 2020-800 DC dans les termes suivants :

« ... en vertu de l'article 21 de la Constitution et sous réserve de son article 13, le Premier ministre exerce le pouvoir réglementaire à l'échelon national. Ces dispositions n'autorisent pas le législateur à subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire ».

Pour le Conseil constitutionnel, le législateur aurait donc méconnu ses pouvoirs en prévoyant une contrainte (à travers l'avis conforme) du pouvoir réglementaire du Premier ministre. Si ce considérant est la continuité logique de la jurisprudence antérieure du Conseil constitutionnel, comme l'explique le commentaire officiel de la décision, on ne peut manquer de relever que l'argumentation ici retenue est quelque peu surprenante.

L'échelon national auquel s'exerce le pouvoir qui mettra en place un traitement de données de santé aurait justement pu justifier le constat d'une atteinte très considérable. Cette atteinte aurait pu être rééquilibrée par la garantie de l'avis conforme de l'autorité indépendante spécialement créée pour se prononcer sur les traitements automatisés des données sensibles, la CNIL.

Or, d'après le Conseil constitutionnel :

« 77. (...) Ces dispositions n'autorisent pas le législateur à subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire. Dès lors, le mot "conforme" figurant à la première phrase du paragraphe V de l'article 11 est contraire à la Constitution ».

La garantie d'un avis conforme de la CNIL liant le pouvoir réglementaire pour la création d'un traitement de données personnelles de santé dans le cadre de l'état d'urgence sanitaire a donc été considérée comme contraire à la Constitution. Il lui a été préféré un avis public simple.

C. L'ambiguïté du considérant 65 de la décision n° 2020-800 DC

Appréciant la conformité à la Constitution du dispositif créant un système d'informations destiné à lutter contre la propagation de l'épidémie de Covid-19, le juge constitutionnel a pu considérer :

« 65. Enfin, le dispositif proposé exclut expressément le développement ou le déploiement d'une application informatique à destination du public et disponible sur équipement mobile permettant d'informer les personnes du fait qu'elles ont été à proximité de personnes diagnostiquées positives au covid-19 »^{17 18}.

Comment doit-on comprendre ce considérant 65 de la décision n° 2020-800 DC¹⁹ ?

¹⁷ Cons. const., décision n° 2020-800 DC du 11 mai 2020, *Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions*.

¹⁸ Notons que cette exclusion de principe reprise par le juge constitutionnel a été introduite par un amendement parlementaire. Voir : http://www.senat.fr/encommission/2019-2020/414/Amdt_COM-119.html.

¹⁹ Curieusement la doctrine n'a pas commenté le considérant 65 de la décision. Voir, par exemple : VERPEAUX, M., « Le Conseil constitutionnel sauve l'essentiel », *AJDA*, 2020, pp. 1242 et s.

En soi, il s'agit d'un paragraphe qui n'est ni décisif ni même indispensable à la construction du raisonnement du juge constitutionnel. Il ne s'agit pas, non plus, d'une réserve d'interprétation puisque ce considérant ne relève pas des réserves énumérées par le juge lui-même (cons. 78)²⁰.

Néanmoins, il convient d'observer que l'engagement du législateur d'exclure des « finalités du dispositif le développement ou le déploiement d'une application informatique à destination du public et disponible sur équipement mobile permettant d'informer les personnes du fait qu'elles ont été à proximité de personnes diagnostiquées positives au covid-19 » (art. 11-II, dernier alinéa) fait office de « garantie légale » conduisant à la décision conforme (sauf exceptions) du Conseil constitutionnel. On pourrait alors supposer *a contrario* que si un tel dispositif de *contact-tracking* avait été prévu par le législateur de façon autonome ou en tant que finalité du dispositif créé, la décision du Conseil constitutionnel aurait été différente.

Plusieurs éléments pointent en ce sens : le commentaire officiel de la décision du Conseil constitutionnel rappelle l'hostilité des députés et de la société civile à propos d'une telle application au moment de la décision. En effet, dans son commentaire, le Conseil a rappelé les craintes exprimées au cours des travaux parlementaires, traduites expressément par le législateur dans l'article 11-II dernier alinéa, ce qui a semblé rassurer le juge constitutionnel²¹. Pour autant, ce dernier n'a pas fait siens les termes utilisés par le Conseil d'État²², laissant ainsi planer un doute.

On sait, par ailleurs, que le dispositif « StopCovid » n'a pas été mentionné par la loi prorogeant l'état d'urgence, non seulement parce que l'application n'était pas prête au 11 mai 2020 (jour de la levée du premier confinement) mais également parce que son admissibilité au sein même de la majorité n'était pas garantie²³.

Alors qu'il n'avait donc pas à juger de cette application, le Conseil constitutionnel a toutefois choisi de faire apparaître dans son considérant 65 cet engagement du législateur en guise de condition de la constitutionnalité du nouvel état d'urgence.

On peut ainsi regretter que le juge constitutionnel ait sous-estimé, voire dissimulé - dans un moment aussi délicat pour les libertés -, l'imminence du danger de laisser le Gouvernement mettre en place, par voie réglementaire, une application de *contact-tracking* utilisant des données personnelles sensibles. Le Conseil constitutionnel savait effectivement très bien, dès le 11 mai 2020, que le Gouvernement allait mettre en œuvre, quelques semaines plus tard, « StopCovid » sans être obligé de passer par le Parlement.

²⁰ Article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire.

²¹ « Le Conseil a alors constaté que les quatre finalités assignées au traitement étaient bien conformes à cet objectif et que le législateur avait expressément exclu que le dispositif proposé serve au développement ou au déploiement d'une application fonctionnant à partir des téléphones portables comme celle que le Gouvernement envisageait par ailleurs de mettre en place sous le nom de "StopCovid". Cette exclusion rendait compte de certaines craintes qui s'étaient exprimées au cours des travaux parlementaires (paragr. 64 et 65) » (Conseil constitutionnel, commentaire officiel, décision n° 2020-800 DC, p. 20).

²² « Il ressort de l'étude d'impact ainsi que des précisions apportées par le Gouvernement que le dispositif envisagé, qui reposera sur un premier traitement ayant pour objet d'identifier les personnes infectées et sur un second traitement destiné à identifier, par des enquêtes sanitaires nécessitant des moyens humains importants, les cas-contacts et à assurer la surveillance épidémiologique, est totalement distinct du projet "StopCovid", dont l'objectif est de permettre d'identifier les personnes en contact avec une personne infectée par une application téléchargée sur les téléphones portables des intéressés » (CE, avis sur un projet de loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, 1^{er} mai 2020, NOR : PRMX2010645L, p. 6).

²³ Pour une analyse détaillée d'une collaboratrice parlementaire, voir : VIGUEUR, S., « StopCovid et "tracking" : la délicate question d'un vote au Parlement », *Le Monde*, 21 avril 2020.

En effet, à la suite des indications de la CNIL (qui avait expliqué dans son avis²⁴ relatif à « StopCovid » qu'en termes de fondement juridique le Gouvernement pouvait se baser autant sur le consentement des utilisateurs que sur l'intérêt légitime de l'État dans le cadre de la lutte contre l'épidémie)²⁵, l'application a été légalement mise en place le 29 mai 2020 par le décret n° 2020-650²⁶.

Nous voyons ainsi qu'en temps de crise sanitaire, la protection des données personnelles ne constitue plus une limite au traitement de ces dernières alors même que c'est justement dans un tel contexte que l'atteinte aux libertés mériterait d'être le plus scrupuleusement appréciée.

II. L'ère de la « protection-alliée »

Le paysage juridique de la situation d'urgence sanitaire devient encore plus intéressant à analyser si l'on tient compte du fait que la protection des données à caractère personnel non seulement ne constitue plus un obstacle au traitement de données personnelles sensibles mais devient un gage d'efficacité de l'action du Gouvernement.

Le changement de discours - devenu possible ces dernières années avec l'application de la Directive 95/46 et officiel après l'adoption du RGPD - a été discret jusqu'à l'arrivée du Covid-19. Puis, l'état d'urgence sanitaire est devenu le laboratoire d'expériences normatives concrètes du RGPD faisant de l'application de ses normes la condition de la réussite de la lutte contre l'épidémie (A). Or, on peut se demander quelle effectivité en termes de protection des données personnelles peut être attribuée à cette nouvelle approche qui repose essentiellement sur une responsabilisation éthique *ex ante* (B).

A. Un changement de discours

Depuis l'adoption du RGPD, au risque de laisser les gouvernements agir hors des clous de la législation relative à la protection des données à caractère personnel, les autorités chargées de cette protection dans les États membres se sont précipitées pour rassurer les responsables politiques sur le fait que le cadre protecteur des données personnelles ne constituait pas une contrainte.

En France²⁷, nous avons pu ainsi entendre la présidente de la CNIL expliquer devant la Commission des lois de l'Assemblée Nationale que :

²⁴ CNIL, délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid », pp. 5-6.

²⁵ Voir en ce sens l'amendement n° 414 présenté au Sénat le 4 mai 2020 introduisant cette exclusion (équivoque) dans l'article 11 de la loi prorogeant l'état d'urgence.

²⁶ Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid ».

²⁷ « 2. L'EDPB souligne que le cadre juridique en matière de protection des données a été conçu de façon à être souple et que, dès lors, il peut constituer un outil de réaction efficace pour, à la fois, endiguer la pandémie et sauvegarder les droits de l'homme et les libertés fondamentales. 3. L'EDPB est fermement convaincu que, lorsque le traitement de données à caractère personnel est nécessaire pour gérer la pandémie de COVID-19, la protection des données est indispensable pour instaurer la confiance, créer les conditions d'acceptabilité sociale à l'égard de toute solution et garantir ainsi l'efficacité des mesures prises. Le virus ne connaissant pas de frontières, l'élaboration d'une approche européenne commune en réaction à la crise actuelle, ou à tout le moins la mise en place d'un cadre interopérable, semble préférable » (European Data Protection Board, *Lignes directrices*

« les textes qui protègent les données personnelles ne s'opposent pas à la mise en œuvre de solutions de suivi numérique, individualisé ou non, pour la protection de la santé publique »²⁸.

Ainsi, la CNIL n'est plus l'autorité de 1978 que le législateur a voulu indépendante afin de protéger les citoyens contre les abus venant - justement - de l'État. Elle est devenue, en 2020, une sorte de commission consultative du Gouvernement spécialisée en matière de légalité des traitements de données personnelles ; autrement dit, une agence gouvernementale d'accompagnement des politiques publiques, voire une complice du Gouvernement, mais certainement pas une entité capable de se prononcer avec autorité et de manière indépendante.

En ce sens, la présidente de la CNIL a précisé :

« ... mettre en avant un cadre respectueux de la vie privée et des données personnelles est tout à fait nécessaire pour, tout à la fois, asseoir la confiance, créer les conditions d'une acceptabilité sociale de toute technique potentiellement intrusive et garantir la sécurité. J'y insiste : il n'y a pas à se demander s'il faut s'affranchir du cadre, ou prendre des libertés avec celui-ci, parce que le cadre juridique que l'Europe et la France se sont donné comporte en lui-même, en son propre sein, les solutions permettant de répondre à la situation »²⁹.

Dès lors, on ne peut que constater la confirmation de notre hypothèse selon laquelle on assisterait à la fin de la « protection-limite » des données personnelles à l'égard de l'exercice d'autres droits ou prérogatives. Le RGPD et la LIL contiennent des « solutions de mise en conformité » de tout type de traitement de données personnelles, même sensibles, que ce soit en raison de leur nature (données de santé, art. 9, RGPD) ou des modalités de leur traitement (*contact-tracking*) (art. 35, RGPD).

Dorénavant, le cadre protecteur des données personnelles se réduit donc à la mise en place, en amont des traitements, à des principes éthiques dont la transgression ne peut être juridiquement empêchée par aucun organe. Dans une telle configuration, la fonction de garantie des libertés individuelles des normes juridiques semble réduite à néant.

B. Ses conséquences

Quelles sont les conséquences de cette nouvelle normativité ? Faire appel à un dénominateur idéologique commun, en l'occurrence le respect du cadre protecteur des données personnelles, devient un « tour de prestidigitation » qui vise à faire disparaître ce qui gêne. La protection des données personnelles est devenue l'une des composantes du « discours d'accompagnement » de l'état d'urgence sanitaire aux fins de le justifier (a). Mais à quel prix en termes de libertés individuelles ? (b)

a. L'« habillage juridique sur mesure » de l'application « StopCovid » par la CNIL

4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19, adoptées le 21 avril 2020, p. 4).

²⁸ Audition à la Commission des lois de l'Assemblée Nationale, Propos liminaires de Madame Marie-Laure Denis, présidente de la CNIL, mercredi 8 avril 2020, p. 4.

²⁹ *Ibidem*

La délibération de la CNIL à propos du projet d'application « StopCovid » peut être vue comme un avis confortant le Gouvernement dans sa position plutôt que comme un avis analysant la légalité du traitement de données personnelles envisagé.

Certes, au moment de sa délibération, la CNIL n'était pas à même de connaître le paramétrage exact de l'application en question puisque le Gouvernement ne lui avait pas transmis de détails à ce sujet (comme cela s'est aussi passé avec le Conseil constitutionnel).

Si l'on partage entièrement toutes les considérations de la délibération mettant en lumière la difficulté de la CNIL de se prononcer sur une application théorique, il convient d'observer que la procédure de demande d'avis s'est transformée en un « habillage juridique sur mesure » de l'application envisagée.

En effet, étant donné qu'au moment de la demande d'avis, le projet n'avait pas été formulé de manière détaillée par le Gouvernement, la CNIL n'a pu qu'exprimer des réticences et quelques solutions pour permettre le respect des libertés individuelles. *In fine* et à défaut de pouvoir véritablement donner son avis, la CNIL s'est donc retrouvée dans l'obligation de répondre au Gouvernement en lui communiquant des consignes visant à permettre une mise en œuvre de l'application « la plus légale possible ».

Dès lors, la délibération ressemble plus à une réponse à l'interrogation « comment le gouvernement doit-il procéder pour agir en conformité avec la LIL et le RGPD ? » qu'à un véritable avis se prononçant sur la question de savoir si un tel projet de traitement est conforme ou non à la législation nationale ?

Un avis négatif de la CNIL était impossible tant en raison de l'état non abouti du projet soumis que de l'affaiblissement de son rôle d'autorité dont les opinions sont respectées par le Gouvernement. Finalement, négatif ou positif, l'avis de la CNIL n'engageait en rien ce dernier (ce que le Conseil d'État et le Conseil constitutionnel ont confirmé).

Il s'agit donc d'un avis de « responsabilisation » du Gouvernement dont le seul engagement est désormais moins de nature juridique que de caractère éthique.

b. Un contrôle de proportionnalité insidieux

Il ne serait pas exagéré d'affirmer que la proportionnalité a « porté sur ses épaules » tout l'état d'urgence. Cependant, il ne s'agira ici que de faire quelques brèves observations à propos de son application en matière de traitement des données personnelles en temps de crise.

Le contrôle de proportionnalité n'est qu'une illusion de garantie d'un État de droit en l'absence de paramètres bien déterminés pour le réaliser³⁰. Mal exécuté, il peut effectivement se transformer en une justification de l'arbitraire³¹.

Dans le cas des traitements mis en place pour lutter contre l'épidémie, avant même de se prononcer sur les trois étapes classiques du test de proportionnalité (adéquation, nécessité,

³⁰ Par exemple : légalité de la finalité du traitement, légalité du moyen, adéquation, nécessité, proportionnalité *stricto sensu*, non violation de l'essence du droit fondamental.

³¹ Tel un « caméléon juridique ». Voir : MUZNY, P., « Proportionnalité (principe de- et contrôle de-) », in *Dictionnaire des Droits de l'Homme*, Paris, PUF, 2008, pp. 810-814 ; KOUMPLI, C., « Un essai sur la clarification de l'inférence : État de droit - principe de proportionnalité », *VIII^e Congrès mondial de l'Association Internationale de Droit Constitutionnel*, 2010, Mexico, (hal-02971400).

proportionnalité *stricto sensu* entre l'atteinte aux libertés et la finalité de la mesure envisagée), il est primordial d'examiner séparément et objectivement la conformité au droit de la finalité de la norme instaurant le traitement en question ainsi que du moyen choisi pour l'atteindre.

La légalité de la finalité de lutte contre une épidémie est difficilement discutable au regard de la préoccupante situation sanitaire qu'elle engendre³².

En revanche, la légalité du moyen (par exemple l'application « StopCovid »), c'est-à-dire sa conformité avec le droit positif en vigueur (sans se préoccuper pour l'instant du caractère adéquat, nécessaire, proportionné de la relation moyen-finalité), n'est pas évidente à admettre ; ni en termes de légalité formelle (adoption par décret) ni en termes de légalité substantielle (conformité aux droits et libertés individuelles).

Or, poser la question de la légalité au sens large (y compris de la constitutionnalité et de la conventionnalité) du moyen est une étape essentielle conditionnant la poursuite du test de proportionnalité en permettant une vigilance plus forte en cas de dérogation. Conscient de cette situation, le gouvernement a réussi à satisfaire les exigences de forme en faisant voter le projet de décret « StopCovid » par le Parlement alors qu'il n'en était pas obligé. Mais qu'en est-il du fond ? Un dispositif de *contact-tracking* de données de santé est-il juridiquement respectueux des libertés individuelles ?

En ce qui concerne les fichiers « SIDEP » et « ContactCovid », le Conseil constitutionnel a évoqué la nécessité d'« une particulière vigilance » (cons. 61, déc. n° 2020-800DC) envers le traitement de données personnelles de nature médicale mais n'a pas osé approfondir son avertissement et a directement basculé vers un contrôle du rapport moyen-finalité. Cependant, ce dernier s'est avéré être un test en apparence poussé mais en réalité d'une extrême superficialité aboutissant à la reconnaissance de la constitutionnalité des nouveaux fichiers créés. En outre, comme il a été évoqué préalablement, le juge constitutionnel n'a de fait pas procédé à un contrôle de la conformité de l'application « StopCovid » au regard des libertés individuelles.

Par ailleurs, même si elle a émis différentes réserves, la CNIL a tacitement reconnu son « admissibilité » à la condition d'accompagner le traitement de données induit par cette application de certaines garanties en raison de la situation d'urgence dans laquelle elle est mis en œuvre. Or, il nous semble que c'est justement en raison de cette situation d'urgence que l'admissibilité d'un tel dispositif mériterait une considération moins arrangeante ; ce d'autant plus qu'il n'y avait pas d'enjeu majeur à le faire, l'avis de la CNIL ne liant pas le Gouvernement.

Par ailleurs, s'agissant de la question de l'adéquation entre le moyen et la finalité, on peut regretter que la CNIL n'ait pas insisté sur le fait qu'une application de *contact-tracking* ne constitue pas un moyen techniquement pertinent pour réaliser la finalité poursuivie, à savoir lutter contre une épidémie, compte tenu notamment du caractère volontaire de son téléchargement qui compromet d'emblée son efficacité³³. La mise en place d'un moyen *en principe* interdit a ainsi été avalisée et c'est finalement la CNCDH et non la CNIL qui a insisté sur les effets incertains d'une lutte contre une épidémie par le biais d'une application³⁴.

³² (Il n'est pas inopportun non plus de rappeler que les Pays-Bas et de pays scandinaves ont opté pour une lutte contre l'épidémie sans restriction de libertés). Mais cela est un autre débat...

³³ En ce sens, voir : CNCDH, avis sur le suivi numérique des personnes (A-2020-2), 28 avril 2020, p. 9.

³⁴ *Ididem*

Était-il vraiment *nécessaire* de mettre en œuvre une application de traçage de contacts pour lutter contre une épidémie ? Étant donné le caractère intrusif d'un tel traitement de données, pourquoi la CNIL n'a-t-elle pas posé de réserve claire et stricte ? Au contraire, elle a recommandé que l'impact du dispositif sur la stratégie globale soit régulièrement étudié afin que son efficacité au fil du temps puisse être évaluée³⁵. En d'autres termes, la CNIL a admis qu'un dispositif en principe préjudiciable aux libertés individuelles et *a priori* faiblement efficace puisse perdurer à la condition de l'évaluer fréquemment.

Reste la question de la proportionnalité au sens strict à laquelle il est habituellement recouru pour justifier une mesure attentatoire. Rappelons que la proportionnalité *stricto sensu* correspond à l'étape du « *reasonableness* »³⁶, pour reprendre le terme anglais, c'est-à-dire à un questionnement sur le caractère raisonnable, opportun, voire éthiquement acceptable d'une mesure. Cependant, en France, nous savons bien que les juges préfèrent sanctionner l'auteur d'un acte ayant « touché aux limites des limites », c'est-à-dire au « manifestement disproportionné ». En son absence, le moyen est généralement considéré comme valide.

Le recours au contrôle de proportionnalité alors qu'il est *a priori* défaillant dans ce cas pose la question de la « prise au piège » de l'État de droit au nom de la lutte contre le Covid-19.

c. Résultats de la protection-alliée

Face à des garanties affaiblies faute de pouvoir de contrainte effectif afin d'assurer la protection des citoyens, celle-ci repose dorénavant davantage sur l'éthique des responsables politiques représentée par l'idée abstraite et générale de respect des droits de l'homme³⁷ qui devient ainsi le dernier rempart de protection des données personnelles en amont de la mise en place d'un traitement. Or, quelle est la résistance de cette forteresse ? Quel résultat a produit la « protection-alliée » dans le cas particulier de l'épidémie de Covid-19 ?

- *La pérennisation de la « logique d'autruche » du juge constitutionnel.* En d'autres termes, à partir du moment où la « protection » a perdu son sens de limite, la perception dont se fait le juge constitutionnel de la protection des données personnelles le conduit de façon circulaire au même raisonnement : tant qu'il existe des garanties suffisantes, l'atteinte à la protection des données personnelles est admissible. Ce discours jurisprudentiel répandu ne traite cependant pas le problème de fond qui, finalement, n'est abordé par personne alors qu'il y aura toujours et de plus en plus de garanties techniques puisque la protection des données est devenue un objet de commercialisation. Cette question de fond est la suivante : à partir de quelles caractéristiques considère-t-on qu'un traitement de données personnelles porte atteinte à l'essence du droit fondamental à la protection des données à caractère personnel ? Les circonstances exceptionnelles que nous vivons, alors qu'elles auraient pu être le moment idéal pour poser des principes clairs en la matière, ont finalement constitué une occasion ratée.

³⁵ CNIL, délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid », p. 9.

³⁶ PHILIPPE, X., « Le contrôle de proportionnalité exercé par les juridictions étrangères : l'exemple du Conseil constitutionnel », *Les Petites Affiches*, n° 46, numéro spécial, 5 mars 2009, p. 16. Voir aussi : XYNOPOULOS, G., *Le contrôle de proportionnalité dans le contentieux de la constitutionnalité et de la légalité (Étude comparative France, Angleterre, Allemagne)*, Paris, LGDJ, 1995, p. 188-189 ; KOUMPLI, C., « Un essai sur la clarification de l'inférence : État de droit - principe de proportionnalité », *op. cit.*, p. 20.

³⁷ Voir : « L'éthique doit avoir sa place dans les situations d'urgence », *AJDA*, 2020, p. 1320.

- *La mise en place d'une application mobile défaillante.* Si la CNIL n'était pas intervenue *ex post*, il n'aurait pas été connu que le Ministère de la Santé et des Solidarités avait enfreint une longue liste de dispositions légales de protection des données à caractère personnel (manquements aux principes de licéité, de loyauté et de transparence, à l'obligation d'informer les personnes concernées, à l'obligation relative à l'encadrement de la sous-traitance, à l'obligation de réaliser une AIPD complète³⁸, aux règles relatives aux cookies et autres traceurs). La mise en demeure du ministère de la Santé et des Solidarités prononcée par la CNIL, le 15 juillet 2020³⁹, est revenue en grande partie sur les points qu'elle avait auparavant relevé dans son avis⁴⁰. On ne peut que se féliciter de cette décision de clôture et de la nouvelle version de l'application qu'elle a engendré⁴¹. Pour autant, il convient de songer aux milliers de traitements réalisés hors des clous de la législation depuis le RGPD et qui n'ont pas eu l'honneur de bénéficier de l'attention particulière de la CNIL.
- *L'emploi illégal de drones.* Inutile d'insister sur le mépris du ministère de l'Intérieur à l'égard de ses obligations issues de la législation de protection des données personnelles⁴². Le relever constitue un lieu commun. S'agissant de la mise en place de drones, le Conseil d'État est venu sanctionner *ex post* le dépassement de la limite des limites⁴³. Il n'est donc intervenu qu'*a posteriori* d'une atteinte grave aux libertés. Alors que cette décision a fait naître l'espoir d'un juge soucieux de l'équilibre « liberté-sécurité, cet espoir risque de s'évanouir puisque l'article 22 de la proposition de loi sécurité globale sur l'encadrement des « caméras aéroportées » permettra de donner un cadre légal à la mise en place de la surveillance par drones de la population.
- *Une mithridatisation des citoyens quant à la perte de libertés.* Une protection des données personnelles ajustables aux besoins et aux circonstances a surtout permis à l'État d'expérimenter une mesure comportant un risque considérable d'accoutumance à des pratiques en principe contraires à l'État de droit. Or, il est bien connu que les pouvoirs publics ont pu, dans le passé, étendre le champ et les modalités d'utilisation de techniques attentatoires aux libertés, toujours adoptées au début pour une période courte, et que le risque d'un « effet cliquet »⁴⁴ a été décrié par un grand nombre d'organismes sensibles à la cause des libertés. En dépit de cela, « StopCovid » continue de fonctionner alors que son inefficacité est patente et son coût exorbitant⁴⁵.

³⁸ Ce qui, en soi, n'a que très peu de valeur aux yeux du juge administratif à l'opposé de l'approche du législateur européen. Voir à propos de CE, 2^e et 7^e ch. réunies, 6 novembre 2019, n° 434376, mentionné aux tables du recueil Lebon : DEBET, A., « La non-réalisation d'une analyse d'impact relative à la protection des données ne rend pas l'acte définissant les caractéristiques d'un traitement soumis au RGPD ? illégal », *Communication Commerce Électronique*, n° 4, avril 2020, comm. 37.

³⁹ CNIL, décision n° MED-2020-015 du 15 juillet 2020.

⁴⁰ CNIL, délibération n° 2020-046 du 24 avril 2020.

⁴¹ CNIL, décision n° 2020-015 du 3 septembre 2020 - Clôture de la décision n° 2020-015 du 15 juillet 2020 mettant en demeure le ministère des Solidarités et de la Santé.

⁴² AUDIT, P.-E., « Le Conseil d'État et la légalité de l'utilisation des drones : quelle place pour la vie privée ? », *Recueil Dalloz*, 2020, pp. 1336 et s. ; ERSTEIN L., « Covid : finalement pas si drone », *La Semaine Juridique. Édition Générale*, n° 22, 1^{er} juin 2020, p. 668.

⁴³ PFERSMANN, O., in FAVOREU L. (dir.), *Droit des libertés fondamentales*, Paris, Dalloz, coll. « Précis. Droit public », 4^e éd., 2007, pp. 100-101.

⁴⁴ CNCDDH, avis sur le suivi numérique des personnes, 28 avril 2020, p. 11.

⁴⁵ Assemblée Nationale, *Rapport d'information déposé en application de l'article 145 du Règlement par la mission d'information relative à l'impact, la gestion et les conséquences dans toutes ses dimensions de l'épidémie de Coronavirus-*

En tout état de cause, l'état d'urgence aura été une occasion pour les pouvoirs publics de mettre en œuvre des partenariats entre le public et le privé qui, à défaut d'être efficaces, ont à tout le moins permis à l'État, d'envisager de nouvelles perspectives en termes de dispositifs numériques, indépendamment du fait qu'elles ne sont pas neutres pour les libertés individuelles⁴⁶.

Or, à l'aube de pages noires pour l'économie mondiale qui ne feront qu'exacerber un populisme montant, *quid* du chemin, déjà esquissé, que prendra la « *datasurveillance* » au regard de l'État de droit ?

Covid-19, n° 1399, p. 129 (v. « Le Journal du Dimanche, « EXCLUSIF. Covid-19 : voici le rapport de la commission d'enquête sur la gestion gouvernementale » du 2 décembre 2020 et ZDNet, « StopCovid : 5 mois d'activité et 6,5 millions d'euros dépensés » du 4 décembre 2020.

⁴⁶ CHEVALLIER, J., « Un nouvel outil numérique : StopCovid », *op. cit.*, pp. 519-540.