Traçage, fichage, profilage

Degrave, Elise

Published in:
Le droit public belge face à la crise du COVID-19

Publication date:
2022

Document Version
le PDF de l'éditeur

TRAÇAGE, FICHAGE, PROFILAGE : LA VIE PRIVÉE TOUCHÉE PAR LE COVID

Élise Degrave

Professeure à la Faculté de droit de l'Université de Namur
Directrice de recherches au CRIDS
Codirectrice de la chaire Egov

Introduction

L'apparition du virus a propulsé la gestion des données par l'État sur le devant de la scène juridique et médiatique. Longtemps resté dans l'ombre[1], ce sujet a gagné en lumière et en ampleur à l'occasion de la mise en place, par le Gouvernement, de plusieurs outils visant à collecter, enregistrer et réutiliser ultérieurement les données des citoyens, dont les données de santé relatives au Covid.

Ainsi, au début de la pandémie, le Gouvernement met en place le *traçage des contacts* des citoyens : traçage manuel (par des agents des *call centers*) et traçage numérique (par une application pour smartphone appelée « Coronalert »). Il s'agit d'identifier les personnes en contact avec un individu contaminé, afin de les prévenir d'un possible risque de contamination et de les inviter à s'isoler, dans l'idée de couper les chaînes de transmission du virus.

Plusieurs données (le numéro de Registre national, l'identité, l'adresse, la date de l'apparition des symptômes, la date et le résultat du test, la collectivité de la personne, le scan des poumons le cas

1. Deux chercheurs n'ayant pas peur de la complexité et l'obscurité (ou ne les percevant pas d'emblée…) y ont tout de même consacré leur thèse de doctorat il y a plusieurs années déjà. Voy. D. De Bot, *E-government in het federale België : een juridische analyse van authentieke registers, de bestuurlijke verplichting tot onrechtstreekse verkrijking, dienstenintegratoren en machtingigingscomités als de 4 sleutelconcepten van interbestuurlijk gegevensverkeer*, Bruxelles, Politeia, 2015 ; E. Degrave, *L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle*, coll. Crids, Bruxelles, Larcier, 2014.

échéant, etc.[2]) à propos de plusieurs types de personnes (personnes à qui un test est prescrit, personnes testées, personnes pour lesquelles le médecin a une présomption sérieuse d'infection, personnes de contact de ces personnes, médecins) sont enregistrées dans cinq bases de données détenues par l'institut public Sciensano.

Le *fichage des personnes vaccinées* démarre avec la campagne de vaccination. Chaque personne vaccinée est enregistrée dans une base de données appelée « Vaccinet ». On y enregistre plusieurs données (données d'identité de la personne vaccinée et de la personne qui a administré le vaccin, date et lieu de l'administration du vaccin, effets indésirables éventuels, etc.[3]), pendant « 30 ans au minimum » à compter de la vaccination[4].

Le *profilage* est mis en place avant les départs en vacances, fin juin 2020, et consiste à rassembler dans une grande base de données appelée « *datawarehouse* », détenue par l'Office national de sécurité sociale (O.N.S.S.), de nombreuses informations relatives aux travailleurs salariés et indépendants (données de santé relatives au Covid, données de contact, d'identification, de travail, etc.) pour « soutenir le traçage et l'examen des clusters et des collectivités ». Ces données peuvent être combinées, croisées et soumises à du *datamining*, c'est-à-dire du profilage, comme nous l'expliquerons dans cette étude.

Ces outils présentent plusieurs points communs.

Ils génèrent la collecte d'une multitude de données à caractère personnel des citoyens et leur enregistrement dans des bases de données détenues par l'État.

De plus, leur utilisation est balisée par les décisions d'un organe appelé « Comité de sécurité de l'information », compétent, par exemple, pour décider de la réutilisation de certaines de ces données et des personnes qui pourront y avoir accès.

Enfin, aucun de ces outils n'a été créé par une loi. Il n'y a donc pas eu de débat démocratique sur leur nécessité et leur proportionnalité, notamment. Ils sont institués, initialement, par une norme du Gouvernement

2. Art. 6 à 9 de l'accord de coopération du 25 août 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact (qui a reçu notamment l'assentiment de la loi du 9 octobre 2020, voy. *infra*). Ci-après, « accord de coopération "Traçage" ».
3. Art. 2, § 2 de l'accord de coopération du 12 mars 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre le Covid-19. Ci-après « accord de coopération "Vaccination" ».
4. Art. 6, § 2 de l'accord de coopération « Vaccination ».

(arrêté royal de pouvoirs spéciaux et, depuis la fin de la période de pouvoirs spéciaux, par arrêté royal ou ministériel) auquel succède, en principe[5], un accord de coopération entre les entités concernées qui l'approuvent par une loi, un décret ou une ordonnance, sans débat.

Cette situation doit-elle nous inquiéter ? Elle doit en tout cas retenir notre attention. Ces outils ébranlent, en particulier, deux principes fondateurs de la matière dont la raison d'être réside pourtant dans l'évitement de risques majeurs. Il s'agit du principe de légalité et du principe de *privacy by design*. Par ailleurs, le rôle du Comité de sécurité de l'information se voit confirmé et renforcé, ce qui interpelle également.

Ces évolutions préoccupantes font l'objet des lignes qui suivent.

Section 1. Des balises juridiques et techniques : les principes de légalité et de *privacy by design*

§ 1. Principe de légalité

Article 8 C.E.D.H. et article 22 de la Constitution. Lorsque l'État collecte, enregistre et réutilise les données des citoyens, il effectue des traitements de données à caractère personnel. Ceux-ci constituent des ingérences dans le droit fondamental à protection de la vie privée, comme l'a affirmé à plusieurs reprises la Cour européenne des droits de l'homme[6]. Dès lors, ces traitements de données sont soumis au respect de l'article 8 de la Convention européenne des droits de l'homme et l'article 22 de la Constitution selon lesquels de telles ingérences sont admissibles à la condition d'être organisées par « une loi ».

En Belgique, ce principe de légalité impose une double exigence, celle de la légalité formelle et celle de la légalité matérielle des traitements de données.

Légalité formelle. S'agissant de la légalité formelle, chaque ingérence dans la vie privée des citoyens doit être organisée par une loi au sens formel du terme, c'est-à-dire une loi, un décret ou une ordonnance bruxelloise.

5. Pour le moment, seuls l'accord de coopération « Traçage » et, bientôt, l'accord de coopération « Vaccination » font l'objet de normes d'assentiment.
6. Voy. not. Cour E.D.H., 16 février 2000, *Amann c. Suisse*, n° 27798/95, § 65 ; Cour E.D.H., 4 mai 2000, *Rotaru c. Roumanie*, n° 28341/95, § 43 ; Cour E.D.H., 21 juin 2011, *Shimovolos c. Russia*, n° 30194/09, §§ 69 et 70.

La Cour constitutionnelle l'a d'ailleurs déjà rappelé à plusieurs reprises, affirmant que « bien que, en utilisant le mot "loi", l'article 8.2 de la Convention européenne [des droits de l'homme] n'exige pas que l'ingérence qu'il permet soit prévue par une "loi", au sens formel du terme, le même mot "loi" utilisé à l'article 22 de la Constitution désigne une disposition législative »[7].

Légalité matérielle. La seule existence d'une loi ne peut suffire pour encadrer les traitements de données des citoyens. Encore faut-il que cette loi soit de qualité suffisante pour permettre à chacun de déterminer, clairement et précisément, ce qu'il va advenir des données collectées à son sujet.

La Cour constitutionnelle rappelle d'ailleurs régulièrement que l'article 22 de la Constitution « garantit à tout citoyen qu'il ne pourra être porté atteinte au respect de sa vie privée qu'en vertu d'une disposition législative, et dans les conditions que celle-ci prévoit, de manière à ce que chacun puisse savoir à tout moment à quelles conditions et dans quelles circonstances les autorités publiques pourraient s'ingérer dans ce droit »[8]. Dans le même sens, la Cour européenne des droits de l'homme insiste sur le caractère compréhensible et prévisible de la loi, en soutenant que la loi doit être « énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant, au besoin, de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable, les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé »[9].

S'inspirant de la jurisprudence de la Cour européenne des droits de l'homme[10], la Cour constitutionnelle et la section de législation du Conseil d'État ont dégagé les « éléments essentiels du traitement »[11], c'est-à-dire les éléments que le législateur doit déterminer dans la loi organisant le traitement de données envisagé[12]. Cette jurisprudence a

7. C. const., 18 octobre 2006, n° 151/2006, pt B. 5.6. Voy. égal. C. const., 18 mars 2010, n° 29/2010, p. 19, pt B. 10.2. ; C. const., 21 décembre 2004, n° 202/2004, pt B.4.3.
8. C. const., 21 décembre 2004, n° 202/2004, pt B.4.3. Voy. égal. C. const., 16 mai 2013, n° 66/2013, pt B.11.1.
9. Voy. not. Cour E.D.H., 26 avril 1979, *Sunday Times c. Royaume-Uni*, n° 6538/74 ; 2 août 1984, *Malone c. Royaume-Uni*, § 67 ; 16 février 2000, *Amann c. Suisse*, n° 27798/95, §§ 75 et 76 et 26 mars 1987, *Leander c. Suède*, n° 9248/81, § 50.
10. Cour E.D.H., 4 mai 2000, *Rotaru c. Roumanie*, n° 28341/95, § 57, *Rev. trim. D.H.*, 2001, pp. 137 et s., note O. De Schutter. Cet arrêt est fondamental en la matière car, pour la première fois, la Cour y dégage les éléments des traitements de données qui doivent figurer dans la loi pour que celle-ci soit précise et prévisible.
11. Voy. not. C. const., n° 202/2004, pts B.6.2. et B.6.3.
12. Voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée*, *op. cit.*, n° 103 et références citées.

d'ailleurs été rappelée maintes fois par l'Autorité de protection des données (A.P.D.) à propos, notamment, de la mise en place des bases de données liées au traçage et à la vaccination[13].

En somme, pour chaque traitement de données, le législateur doit déterminer quelle institution a accès à quelles données, pour quoi faire et pendant combien de temps. La détermination de ces éléments doit être l'occasion d'effectuer l'examen de proportionnalité des traitements de données par rapport à l'objectif poursuivi, en évaluant la pertinence et la nécessité des mesures envisagées.

Ainsi, le législateur doit définir lui-même les *données* utilisées et leur *mode de collecte*.

L'*objectif* poursuivi par le traitement, appelé également « finalité » du traitement, est un élément essentiel de celui-ci.

Par ailleurs, le législateur doit mentionner les *personnes autorisées* à consulter une base de données ainsi que les *conditions* de cette consultation.

Il en va de même de la *durée de conservation* des données. Cela suppose que le législateur fixe au moins les délais maximums de conservation des données[14].

Enfin, la *communication* des informations, dite aussi « réutilisation », doit également être organisée par le législateur lui-même[15].

Raison d'être de l'exigence de légalité. Si une loi claire, précise et prévisible est nécessaire pour encadrer les traitements de données à caractère personnel, c'est parce qu'il est primordial que les représentants du peuple qui siègent au Parlement mènent un débat démocratique sur ces questions.

Ce débat démocratique doit être *éclairé*. Les questions sont souvent techniques, abstraites. Les auditions au Parlement, notamment, permettent d'auditionner publiquement des experts sur les enjeux de

13. Voy. not. A.P.D., avis n° 36/2020 du 29 avril 2020 sur une demande d'avis concernant un avant-projet d'arrêté royal portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19 (CO-A-2020-042), n^{os} 38 et s. ; A.P.D., avis n° 42/2020 du 25 mai 2020 sur une demande d'avis concernant une proposition de loi portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19 (CO-A-2020-048), n^{os} 16 et s.

14. Avis L. 37.748 et 37.749/AG du 23 novembre 2004 sur un avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (37.748/AG) et sur un avant-projet de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité (37.749/AG), *Doc. parl.*, Ch., sess. 2004-2005, n^{os} 1598/1 et 1599/1.

15. Voy. not. avis L. 42.064 du 24 janvier 2007 sur un avant-projet de loi « relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances. », *Doc. parl.*, Ch. repr., n° 52-3064/1.

cette matière. S'ensuivent des débats axés sur les éléments essentiels des traitements de données envisagés. S'agissant, par exemple, de la vaccination, un tel débat aurait pu amener à réfléchir à plusieurs questions importantes. Quelles sont les finalités exactes poursuivies par la base de données vaccination ? Est-il proportionné, au regard de ces finalités, d'enregistrer ces données pendant trente ans après la date de vaccination ? Quelles autorités auront accès à ces données et pour quoi faire ?

Mener un débat sur ces questions afin de bien encadrer l'utilisation des données à caractère personnel est d'autant plus important que la vie privée est le socle des autres libertés. Par exemple, si les données de santé sont mal utilisées, cela pourrait porter atteinte à la vie privée mais également au droit à l'égalité et à la non-discrimination, au droit d'aller et venir, à la liberté de culte[16], à la liberté d'expression[17], etc. Protéger la vie privée, c'est protéger l'ensemble des libertés[18].

Ce débat doit également être *éclairant*. Grâce, notamment, aux médias qui relaient ce débat, il est l'occasion d'informer le public sur les questions en jeu, la difficulté d'organiser la balance entre l'efficacité de l'État, d'une part, et la protection des libertés, d'autre part. Par exemple, en expliquant le raisonnement suivi pour encadrer la vaccination, le public aurait pu comprendre pourquoi il était nécessaire, le cas échéant, d'enregistrer les données de vaccination si longtemps et à quoi cela allait servir. Cela aurait été un élément permettant de gagner la confiance des citoyens, à propos de la gestion de leurs données mais également de la vaccination elle-même.

Cet effort de pédagogie et de publicité est d'autant plus important que la vie privée est une liberté particulière. À la différence d'autres libertés, on ne voit pas très bien ce que représente la vie privée, ni quand il y est porté atteinte. Lorsque le droit de rassemblement est suspendu, ne fût-ce que quelques jours, on l'éprouve. Tandis que la mise en place d'une grande base de données comprenant beaucoup d'informations à notre sujet ne crée pas d'effets perceptibles par chacun, du moins à court terme. On peut raisonnablement penser que l'invisibilité de la vie privée explique, en partie, les craintes des citoyens à l'égard

16. Dans l'hypothèse, par exemple, où les données de traçage révèlent la fréquentation d'un lieu de culte précis.
17. Dans l'hypothèse, par exemple, où il est demandé à une personne de révéler l'identité du journaliste à qui elle a parlé car il s'agirait d'un cas contact.
18. En ce sens, voy. not. Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in K. Benyekhlef et P. Trudel (éd.), *État de droit et virtualité*, Montréal, Thémis, 2009, p. 210.

de la gestion de leurs données par l'État. Ces craintes doivent être entendues, car elles pourraient mettre à mal la confiance des citoyens pourtant nécessaire pour lutter contre le virus[19], mais aussi, plus généralement, pour permettre à l'État d'utiliser les données des citoyens afin d'effectuer ses missions au quotidien et simplifier les démarches administratives de chacun. Cela justifie que l'on manie la vie privée avec particulièrement de clarté, de transparence et d'explication.

En d'autres termes, à condition de respecter l'exigence de légalité formelle et matérielle, le régime juridique de la protection des données n'empêche pas que des données soient utilisées par l'État, même à des fins de contrôle des citoyens, à condition qu'ils soient encadrés par une loi, au terme d'un débat ayant permis, notamment, de faire l'examen de proportionnalité des traitements de données envisagés et de déterminer clairement les éléments essentiels de ces derniers.

Par exemple, serait-il envisageable d'utiliser les données du *Passenger Locator Form*[20] pour contrôler, dans une école, la présence d'enfants revenus de vacances en zone rouge et censés être en quarantaine[21] ? Ce n'est ni permis ni interdit. C'est au Parlement de le décider. Si celui-ci, au terme d'un débat démocratique, estime qu'une telle utilisation des données des citoyens est nécessaire pour lutter contre une pandémie, et qu'il détermine les éléments essentiels de ces traitements, noir sur blanc, dans une loi accessible au citoyen, de tels traitements seront encadrés légalement. En l'occurrence, le législateur devrait donc déterminer lui-même quelles données vont être transmises aux écoles (la seule indication du fait qu'il s'agit d'une zone rouge suffit-elle ou doit-on également mentionner le pays de vacances voire le lieu de villégiature ?). Au sein de l'école, qui aura accès au fichier transmis (le directeur uniquement ou également, les instituteurs et les surveillants ?) ? Pendant combien de temps ces données seront-elles gardées par l'école (deux semaines ? deux mois ? vingt ans ?) ? Par ailleurs, il faut qu'une publicité autour de la loi soit assurée, de manière à ce que le citoyen soit au courant de ces mesures et ne soit pas surpris lors

19. À cet égard, il est à présent clair que la confiance des citoyens est essentielle dans la lutte contre une pandémie. « Il n'existe pas de modèle idéal, à répliquer pour combattre le Covid. Mais les pays qui y parviennent le mieux ont un point commun : l'adhésion » (www.lecho.be/economie-politique/international/general/le-secret-des-pays-efficaces-face-a-la-pandemie-de-coronavirus/10258607.html).
20. Il s'agit du formulaire que doivent remplir les voyageurs avant de traverser la frontière vers la Belgique.
21. Cet exemple s'inspire de l'audition de la directrice de l'Autorité de protection des données à la Commission intérieure de la Chambre à propos de l'avant-projet de loi « Pandémie » le 12 mars 2021. Cette audition est accessible sur www.lachambre.be/media/index.html?language=fr&sid=55U1505.

du contrôle effectif qui sera effectué à son égard ou à l'égard de ses enfants[22]. En respectant des balises, il est possible d'utiliser ces données pour contrôler les citoyens.

§ 2. Principe de *privacy by design*

Principe. Le principe de *privacy by design*, ou « protection des données dès la conception », consacré à l'article 25 du R.G.P.D.[23], consiste à intégrer la protection de la vie privée en amont dans la conception même du système informatique, plutôt que de créer ce système et de penser seulement ensuite à protéger la vie privée par des normes[24]. Pour le dire autrement, il s'agit de créer des outils qui, en eux-mêmes, présentent des garanties de protection pour la vie privée des personnes concernées.

De cette manière, la protection de la vie privée est soutenue par la technique, en sus d'être organisée par des normes. Ensemble, ils constituent « un rempart efficace contre les excès rendus possibles par le progrès »[25].

La Belgique pionnière. Ce principe a été mis en œuvre en Belgique, bien avant sa concrétisation par le R.G.P.D.

En effet, au moment de la création des premières bases de données au sein de l'administration[26], plutôt que d'enregistrer les données dans une seule même base de données[27], ce qui aurait créé des risques importants en cas de piratage de celle-ci, la Belgique a fait le choix de

22. Il faut ainsi éviter, notamment, la situation révélée dans la presse d'une fille de 12 ans que la directrice de l'école a exclue de sa classe après avoir découvert qu'elle revenait de vacances en Suisse. Voy. not. www.lematin.ch/story/viree-de-sa-classe-pour-des-vacances-en-suisse-161824350251.
23. Originairement, cette idée a été développée dans les années nonante par Ann Cavoukian, commissaire à la protection de la vie privée de l'Ontario, au Canada, qui y consacre un site internet (www.privacybydesign.ca). Voy. A. Cavoukian, *Privacy by Design… Take the Challenge*, s.l., 2009.
24. Voy. *ibid.*., p. 3 ; J. Le Clainche, « Consentement et traitements de données à caractère personnel », in D. Le Métayer (dir.), *Les technologies de l'information au service des droits : opportunités, défis, limites*, Bruxelles, Bruylant, 2010, pp. 166-169 ; M. Groothuis, « De digitale overheid en de menselijke maat », *Computerrecht*, 2009, p. 240.
25. J. Le Clainche, « Consentement et traitements de données à caractère personnel », *op. cit.*, p. 168.
26. Le Registre national est la première base de données créée en Belgique en 1968. Elle a été légalement encadrée en 1983. Le premier réseau d'administrations est le réseau de la sécurité sociale, qui comprend en son cœur la première banque-carrefour, la Banque-carrefour de la sécurité sociale.
27. La Belgique a tiré les leçons de l'expérience de la France, qui avait tenté de mettre en place le projet SAFARI (acronyme de « Système automatisé pour les fichiers administratifs et le répertoire des individus ») consistant à centraliser toutes les données des citoyens

l'administration en réseaux et de l'enregistrement décentralisé des données des citoyens. En somme, il s'agit d'identifier des administrations qui ont une matière en commune (la sécurité sociale, par exemple) et de placer celles-ci dans un réseau d'administrations (comme le réseau de la sécurité sociale). Ensuite, on désigne pour chaque administration les types de données qu'elle enregistre dans sa base de données (ainsi, l'adresse est au Registre national, tandis que les données de pension sont à l'Office national des pensions et les allocations familiales à Famifed). Au sein de ce réseau, on place une institution, appelée « banque-carrefour » ou « intégrateur de services », qui achemine les données vers les administrations qui en ont besoin mais ne les détiennent pas.

Ainsi, on maximise l'efficacité de l'administration, qui n'a plus à demander de multiples fois la même information au citoyen puisqu'elle peut y accéder rapidement *via* le réseau, on n'exige plus du citoyen qu'il donne ses informations à répétition. Dans le même temps, la séparation physique des données des citoyens, enregistrées à des endroits différents de l'administration, constitue un rempart technique supplémentaire aux risques de piratage et d'abus dans l'accès aux données.

Section 2. Démantèlement des principes fondateurs

§ 1. Absence de débat démocratique

Arrêtés royaux et arrêtés ministériels. Tant le traçage[28] que le fichage des personnes vaccinées[29] et le profilage[30] ont été mis en place par un arrêté royal ou un arrêté ministériel.

dans une seule base de données. Celle-ci a rapidement été qualifiée d'outil de « chasse aux Français ». Pour plus d'informations, voy. E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée*, *op. cit.*, n° 63.

28. Le traçage a été mis en place par l'arrêté royal de pouvoirs spéciaux n° 44, exécuté par l'arrêté royal du 17 septembre 2020 portant exécution de l'arrêté royal n° 44 du 26 juin 2020.

29. La base de données « vaccination » est organisée par l'arrêté royal du 24 décembre 2020 concernant l'enregistrement et le traitement de données relatives aux vaccinations contre le Covid-19.

30. Le profilage est organisé par l'arrêté ministériel du 30 juin 2020 (art. 18*bis*). Il a été remplacé par l'article 22 de l'arrêté ministériel du 28 octobre 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, lui-même modifié, pour en étendre sa portée, par l'arrêté ministériel du 12 janvier 2021 modifiant l'arrêté ministériel du 28 octobre 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19.

Ce faisant, ni la nécessité ni les éléments essentiels de ces outils de traitement de données n'ont fait l'objet d'un débat démocratique et d'une définition claire dans une loi. L'Autorité de protection des données n'a pas manqué de le souligner.

En guise d'illustration, le *traçage numérique* s'avère aujourd'hui être un « flop »[31]. Cette situation peut s'expliquer notamment par un manque de confiance de la population dans ce dispositif technique difficilement compréhensible et dont l'efficacité n'est pas démontrée[32]. En définitive, cette application est-elle suffisamment efficace pour lutter contre la pandémie ? Et constitue-t-elle la mesure la moins intrusive pour y arriver ? Ce sont les questions posées par l'Autorité de protection des données. Dans son avis n° 34/2020, l'Autorité de protection des données rappelle qu'une loi est nécessaire pour encadrer le traçage numérique et exige du Gouvernement qu'il apporte lui-même la preuve de la nécessité d'une application de traçage numérique, et pas seulement la preuve que celle-ci respecte le R.G.P.D. Elle réclame « une estimation du pourcentage de la population qui en fera usage, sur la base de sondages récents d'intention », de même qu'« une étude relative au taux d'utilisation requis pour que le système produise des résultats »[33]. Et d'ajouter qu'« une campagne de test de l'efficacité des mesures envisagées nous semble également indispensable, notamment afin d'éviter au maximum les faux positifs et le stress injustement généré chez les personnes contactées à tort »[34].

Un débat démocratique au Parlement aurait permis de mettre en évidence, par exemple, le risque de « faux positifs » liés au fait que cette technologie est aveugle et ne voit pas le respect des gestes barrières. Des solutions auraient alors pu être envisagées pour endiguer ce problème qui, en plus de générer du stress inutile, charge davantage les

31. Voy. not. A. Cloot, « Coronalert, le flop », https://plus.lesoir.be/341784/article/2020-12-04/coronalert-le-flop.
32. Observatoire international sur les impacts sociétaux de l'I.A. et du numérique (Canada), *Efficacité et enjeux sociétaux des apps de traçage de contacts*, 27 avril 2020, accessible sur : https://observatoire-ia.ulaval.ca/3674/. À propos de l'acceptabilité sociale des applications de traçage, des chercheurs de l'université d'Oxford ont mené une étude au mois de mars 2020, en France, en Allemagne, au Royaume-Uni, en Italie et aux États-Unis. Cette étude est accessible sur : https://osf.io/24uan/.
33. A.P.D., avis n° 34/2020 du 23 juin 2020 relatif à une demande d'avis concernant un avant-projet d'arrêté royal n° XXX portant exécution de l'article 5, § 1er, 1° de la loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus Covid-19 (II), dans le cadre de l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus Covid-19 parmi la population (CO-A-2020-041), n° 9. Cette demande renvoie au fait que les applications de traçage ne fonctionnent qu'à la condition d'être massivement téléchargées par la population, par au moins 60 % de la population.
34. *Ibid.*

centres de test de personnes qui n'ont en réalité aucun risque d'avoir été contaminées. Par ailleurs, par sa publicité, pareil débat aurait pu mettre en évidence, le cas échéant, la nécessité, démontrée par le Gouvernement, de recourir à cet outil et convaincre la population de cette solution. Malheureusement, il n'en fut rien.

Accords de coopération et normes d'assentiment. En matière de traçage et de vaccination, aux arrêtés royaux succède un accord de coopération entre l'État fédéral et chaque entité fédérée compétente. Ainsi, l'accord de coopération du 25 août 2021 organisant le traçage a reçu l'assentiment du Parlement fédéral et du Parlement de chaque entité fédérée compétente, conformément à l'article 92*bis*, paragraphe 1, de la loi spéciale du 8 août 1980 de réformes institutionnelles[35]. Il en va de même de l'accord de coopération relative à la vaccination du 12 mars 2021[36].

Le traçage et la vaccination sont donc, formellement, encadrés par des normes de valeur législative. Néanmoins, les accords de coopération qui s'y appliquent ont été négociés entre cabinets ministériels et soumis ensuite à l'assentiment des parlements, sans être soumis à une discussion, comme en témoignent les travaux préparatoires de ces normes. En d'autres termes, le traçage et la vaccination sont encadrés par des normes qui pourraient perdurer, sans que l'essence même du principe de légalité n'ait été respectée, à savoir un débat démocratique sur les éléments essentiels de ces outils et une définition claire de ceux-ci.

Cette situation interpelle d'autant plus que ce cadre normatif pourrait survivre à la crise. Certes, l'accord de coopération du 25 août 2021 précise qu'il prendra fin « […] le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus Covid-19 »[37]. Mais peut-on raisonnablement croire qu'il y aura, un jour, un arrêté proclamant

35. Pour le traçage, l'accord de coopération « Traçage » du 25 août 2020 a reçu l'assentiment de la loi du 9 octobre 2020, du décret wallon du 30 septembre 2020, du décret flamand du 2 octobre 2020 et l'ordonnance bruxelloise du 1er octobre 2020.
36. L'accord de coopération « Vaccination » du 12 mars 2021 a reçu l'assentiment de la loi du 2 avril 2021 portant assentiment à l'accord de coopération du 12 mars 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre le Covid-19, du décret wallon du 1er avril 2021 du décret de la Communauté française du 25 mars 2021, du décret de la Communauté germanophone du 25 mars 2021, du décret flamand du 2 avril 2021 et de l'ordonnance bruxelloise du 2 avril 2021.
37. Art. 19, § 2 de l'accord de coopération « Traçage » du 25 août 2020. Quant à l'accord de coopération « Vaccination », il précise en son article 12 qu'il « produit ses effets jusqu'à sa révision ou sa révocation qui intervient le jour où le Secrétariat central du Comité

la fin de l'épidémie comme on signe l'armistice ? À l'heure de la multiplication des variants et de l'annonce d'autres pandémies, on peut douter du caractère provisoire de ce texte. Si l'on peut comprendre que l'urgence qui s'est imposée au début de la crise ait justifié qu'on se passe de débat démocratique sur ces questions, il est préoccupant que le traçage et la vaccination soient désormais bétonnés dans des normes de valeur législative, qui survivront peut-être aux vagues successives du virus, sans qu'aucun débat ait eu lieu à leur sujet, malgré les critiques, parfois nombreuses, émises en la matière[38].

À notre sens, la pertinence et la nécessité de ces outils devraient être réévaluées et faire l'objet d'un débat démocratique éclairé et éclairant pour être intégrés, le cas échéant, dans une loi spécifique sur la gestion des données en cas de pandémie, comme nous l'évoquerons au terme de cette étude.

§ 2. De nombreuses données centralisées

Privacy by design fissuré. Alors que depuis longtemps une attention particulière est portée à la décentralisation des données réparties entre différentes administrations, depuis quelques années, on assiste à un démantèlement de cette séparation physique des données, avec une centralisation plus forte des informations entre les mains de certaines institutions.

Juridiquement, ce démantèlement ne se fait pas très franchement à la lumière du jour mais plutôt par à-coup, dans des lois fourre-tout[39], des lois adoptées à la fin de l'été[40], des normes adoptées le 24 décembre[41], etc., voire pas de norme du tout[42].

---

de concertation a reçu l'accord écrit de toutes les parties pour mettre fin à l'accord de coopération et après la publication d'une communication confirmant cet accord écrit au *Moniteur belge* », sans référence à la fin de la pandémie…

38. Voy. *infra*.

39. Voy. par ex. la loi du 1er mars 2007 portant des dispositions diverses (III) (*M.B.*, 14 mars 2007) qui comprend 165 dispositions. Trente-neuf d'entre elles modifient la loi sur la Banque-carrefour de la sécurité sociale, à laquelle les discussions préparatoires n'ont consacré que quelques brèves explications (voy. le rapport fait au nom de la Commission des affaires sociales par Mme Maggie De Block concernant le projet de loi portant des dispositions diverses [III] [art. 34 à 61, 68 à 80 et 87 à 89], *Doc. parl.*, Ch. repr., sess. 2006-2007, n° 51-2788/013, 24 janvier 2007, pp. 11-15).

40. Voy. la loi du 5 septembre 2018 instituant le Comité de sécurité de l'information […], voy. *infra*.

41. La base de données « vaccination » contre le Covid a été créée par l'arrêté royal du 24 décembre 2020 concernant l'enregistrement et le traitement de données relatives aux vaccinations contre le Covid-19.

42. Depuis 2005, l'État belge utilise un outil appelé OASIS (pour Organisation anti-fraude des services d'inspection sociale) qui n'est encadré par aucune loi ni même aucun arrêté

Cette tendance s'est également manifestée pendant la crise. À cet égard, l'article 8 de l'arrêté ministériel du 12 janvier 2021 est un exemple marquant de ce phénomène[43]. Il dispose que « dans le cadre de la lutte contre le coronavirus Covid-19, l'Office national de sécurité sociale peut, en qualité de sous-traitant pour le compte de tous les services et institutions chargés de la lutte contre la propagation du coronavirus Covid-19, ainsi que de tous les services ou institutions chargés de surveiller le respect des obligations prévues dans le cadre des mesures d'urgence prises pour limiter la propagation du coronavirus Covid-19, collecter, combiner et traiter, y compris via le datamining et le datamatching, des données concernant la santé relatives au coronavirus Covid-19, des données de contact, d'identification, de travail et de résidence relatives aux travailleurs salariés et travailleurs indépendants, en vue de soutenir le traçage et l'examen des clusters et des collectivités ».

Ainsi donc, la seule ministre de l'Intérieur, Annelies Verlinden, habilite l'O.N.S.S. à faire beaucoup de choses (« collecter, combiner et traiter, y compris via le datamining et le datamatching »), avec beaucoup de données (« des données de santé relatives au coronavirus […], des données de contact, d'identification, de travail, de résidence »[44]), à propos de beaucoup de citoyens (« travailleurs salariés et travailleurs indépendants »), pour rendre service à beaucoup d'institutions (« tous les services et institutions chargés de la lutte contre la propagation du coronavirus […], ainsi que de tous les services ou institutions chargés de surveiller le respect des obligations prévues dans le cadre des mesures d'urgence prises pour limiter la propagation du coronavirus […] »). Et ce, dans le but, très ample lui aussi, « de soutenir le traçage et l'examen des clusters et des collectivités ».

Faut-il comprendre par là que les données Covid, initialement collectées pour aider le citoyen à sortir de la crise, vont à présent être utilisées pour le surveiller ?

À ce stade, il n'y a pas de réponse précise. Aucune loi n'a été adoptée pour encadrer ces nouvelles utilisations de données à caractère personnel. Cela aurait pourtant été l'occasion, en respectant le principe de légalité rappelé précédemment, de débattre notamment de la réutilisation de telles données à des fins de contrôle.

royal. À ce sujet, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée*, *op. cit.*, nos 43 et s.

43. Les développements qui suivent s'inspirent de l'article suivant : E. Degrave, « Les citoyens contrôlés par leurs données Covid ? Le datamatching et le datamining utilisé par l'État », *J.T.*, 2021, pp. 125-128.

44. Nous qualifions l'ensemble de ces données de « données Covid » dans la suite de l'étude.

En outre, l'article 8 de l'arrêté ministériel ne contient pas de balises claires, l'usage des termes anglicisants *datamatching* et *datamining* en complique encore davantage la compréhension. Ces termes inquiètent, aussi. Le *datamatching*[45] consiste à « croiser » les données, c'est-à-dire les rassembler et les comparer entre elles. La seconde étape est le *datamining*[46]. On applique aux données des algorithmes[47] qui vont induire de ces données des informations nouvelles, comme le ferait une boule de cristal. Cela permet de réaliser du profilage[48], c'est-à-dire de prédire la probabilité, pour chaque individu, d'adopter le comportement de tel profil d'individu (le profil de fraudeur par exemple[49]).

Cela signifie-t-il que les données Covid vont être utilisées pour rattacher un individu à un profil ? Et si oui, de quel profil va-t-il s'agir ? Pour en tirer quelles conséquences ? L'idée est-elle, par exemple, de rattacher toutes les personnes ayant « oublié » de faire un test à leur retour de vacances à un profil de fraudeur ? Juridiquement, rien ne semble l'interdire actuellement.

Section 3. Un législateur masqué : le Comité de sécurité de l'information

Loi du 5 septembre 2018. La loi du 5 septembre 2018 institue un nouvel organe de contrôle, le Comité de sécurité de l'information (ci-après C.S.I.), composé d'« experts »[50], et à qui est déléguée la compétence de déterminer, seul, quelles autorités sont habilitées à

45. En français : « couplage de données ».
46. En français : « extraction de données ».
47. Un algorithme peut être défini comme « un ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations » (dictionnaire *Larousse*).
48. L'article 4.4 R.G.P.D. définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».
49. En guise d'exemple simple, prenons le cas de John, dont les données fiscales montrent qu'il gagne 2 000 euros par mois. Or, ses données à la D.I.V. montrent qu'il détient sept Ferrari neuves. Le Registre national indique qu'il est propriétaire de deux châteaux. Les algorithmes « anti-fraude » vont cibler John. Il sera rattaché à la catégorie des présumés fraudeurs fiscaux et sociaux et un contrôle fiscal et/ou social sera encouragé.
50. Sur la composition et le fonctionnement du C.S.I., voy. C. De Terwangne et E. Degrave (avec la coll. de A. Delforge et L. Gerard), *La protection des données à caractère personnel en Belgique – Manuel de base*, Bruxelles, Politeia, 2019, pp. 174 et s.

(ré)utiliser quelles données et pourquoi[51], ce qui, rappelons-le, devrait pourtant être défini par le législateur lui-même. Par exemple, comme l'affirme la loi précitée, le C.S.I. peut autoriser la réutilisation, pour des finalités indéterminées, des données détenues par toute institution de sécurité sociale[52].

La compétence large déléguée au C.S.I. a déjà été critiquée à plusieurs reprises par la section de législation du Conseil d'État. Dernièrement, dans l'avis qu'elle a rendu au sujet de l'encadrement de la vaccination contre le Covid[53], se fondant sur l'avis qu'elle a rendu il y a quelques mois au sujet du traçage[54] et sur celui qu'elle a rendu au moment de la création du C.S.I.[55], elle rappelle notamment que « l'attribution d'un pouvoir réglementaire à un organisme public, comme le comité de sécurité de l'information[56], n'est en prin-

51. Outre le fait que ces décisions ne sont pas débattues démocratiquement, elles sont difficiles à trouver. Elles sont accessibles sur www.ksz-bcss.fgov.be/fr/protection-des-donnees/comite-de-securite-de-linformation-csi. Depuis 2018, 734 décisions ont été adoptées, parmi lesquelles il est impossible de faire une recherche par mots-clés ou par type de décision.

52. Art. 18 de la loi C.S.I.

53. C.E., section de législation, avis, 18 février 2021, n° 68.844, sur un avant-projet de loi « portant assentiment à l'accord de coopération du 12 mars 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 », n° 28.

54. C.E., section de législation, avis, 15 juillet 2020, n° 67.719/VR, sur un avant-projet devenu la loi du 9 octobre 2020 « portant assentiment à l'accord de coopération du 25 août 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspection d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus Covid-19 se fondant sur une base de données auprès de Sciensano », www.raadvst-consetat.be/dbx/adviezen/67719.pdf.

55. C.E., section de législation, avis, 26 avril 2018, n° 63.202/2, sur un avant-projet devenu la loi du 5 septembre 2018 « instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE », *Doc. parl.*, Ch., sess. 2017-2018, n° 54-3185/001, pp. 140 et s.

56. *Note 49 de l'avis cité :* voy. d'ailleurs à cet égard la critique qu'avait déjà formulée le Conseil d'État en la matière dans son avis C.E. n° 63.202/2 du 26 avril 2018 sur un avant-projet devenu la loi du 5 septembre 2018 « instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE », *Doc. parl.*, Ch., sess. 2017-2018, n° 54-3185/001, pp. 140-142.

cipe pas conforme aux principes généraux de droit public en ce qu'il est ainsi porté atteinte au principe de l'unité du pouvoir réglementaire et qu'un contrôle parlementaire direct fait défaut. En outre, les garanties dont est assortie la réglementation classique, telles que celles en matière de publication, de contrôle préventif exercé par le Conseil d'État, section de législation, et de rang précis dans la hiérarchie des normes, sont absentes. Pareilles délégations ne se justifient dès lors que dans la mesure où elles sont très limitées et ont un caractère non politique, en raison de leur portée secondaire ou principalement technique. Les organismes qui doivent appliquer la réglementation concernée doivent être soumis à cet égard tant à un contrôle juridictionnel qu'à un contrôle politique […]. En conclusion, les délégations visées accordées au Comité de sécurité de l'information doivent être transformées en délégations à un accord de coopération d'exécution, à l'instar de l'article 14, § 9, de l'accord de coopération, pour autant du moins qu'il ne règle aucun nouvel élément essentiel du traitement des données à caractère personnel, mais concrétise tout au plus ce qui découle déjà de l'actuel accord de coopération. Si cela ne s'avère pas possible, cet accord de coopération sera d'abord complété »[57].

Ainsi donc, les avis de la section de législation du Conseil d'État soulignent sans détour le manque de contrôle parlementaire, juridictionnel et politique sur le C.S.I. En outre, les décisions du C.S.I. ne bénéficient pas d'une publicité suffisante, ne sont pas soumises au contrôle préventif de la section de législation du Conseil d'État et leur statut n'est pas clair.

Covid et C.S.I. Malgré ces critiques sévères, le Gouvernement persiste à confier au C.S.I. des compétences importantes.

57. *Note 50 de l'avis cité :* comparer avec les critères d'évaluation qu'utilise la Cour constitutionnelle pour apprécier les délégations de pouvoir réglementaire par le législateur à une autorité administrative autonome ou à un organisme public décentralisé ; voy. C. const., 11 juin 2015, n° 86/2015, pt B.22.4, et C. const., 9 juin 2016, n° 89/2016, pt B.9.6.4 : « Les articles 33, 105 et 108 de la Constitution ne s'opposent pas à ce que, dans une matière technique déterminée, le législateur confie des compétences exécutives spécifiques à une autorité administrative autonome soumise tant au contrôle juridictionnel qu'au contrôle parlementaire et n'interdisent pas au législateur d'accorder des délégations à un organe exécutif, pour autant qu'elles portent sur l'exécution de mesures dont le législateur compétent a déterminé l'objet, en particulier dans les matières techniques et complexes » ; voy. égal. C. const., 19 novembre 2015, n° 162/2015, pt B.8.4 : « L'article 33 de la Constitution et l'article 20 de la loi spéciale du 8 août 1980 ne s'opposent pas à ce que le législateur confie des compétences exécutives spécifiques à un organisme public décentralisé qui est soumis à une tutelle administrative et à un contrôle juridictionnel ».

S'agissant du *traçage*, le C.S.I. est compétent, notamment, pour autoriser la réutilisation de données enregistrées dans les bases de données de Sciensano alors que les éléments essentiels de pareilles réutilisations ne sont pas fixés dans l'accord de coopération ayant reçu l'assentiment des législateurs compétents. Selon l'Autorité de protection des données, qui l'a rappelé dans trois avis différents à propos du traçage, « ni l'article 8 de la CEDH, ni l'article 22 de la Constitution, ni le RGPD, en particulier l'article 6.3., ne permettent un tel "chèque en blanc" ». Et d'affirmer, notamment que « l'accord de coopération doit donc déterminer lui-même quels sont les "tiers" à qui Sciensano peut communiquer des données qu'il désigne et les raisons pour lesquelles ces données leur seront communiquées », ce qui est particulièrement important vu « la quantité et la sensibilité des données en question (données relatives à la santé, données relatives à une présomption d'infection suite à un contact) et de la possibilité pour leurs destinataires potentiels d'effectuer des recoupements entre ces différents types de données »[58].

Pour la *vaccination*, le C.S.I. peut autoriser la communication des données relatives à la vaccination « à des personnes ou des instances chargées d'une mission d'intérêt public par ou en vertu d'une loi, d'un décret ou d'une ordonnance », sans que ces destinataires ne soient clairement déterminés. Or, ils sont potentiellement nombreux. À titre d'exemple, les sociétés de transport en commun (S.N.C.B., S.T.I.B., etc.) et les universités répondent à cette qualification. Certes, la communication desdites données à ces instances ne peut avoir lieu qu'à la condition de ne transmettre que « les données pertinentes pour les finalités de l'article 4 ». Mais ces finalités sont elles-mêmes définies largement. Il est notamment question de traiter les données pour « l'information et la sensibilisation des personnes concernant la vaccination contre la Covid-19 par les prestataires de soins et les organismes assureurs »[59]. Aux termes de cette disposition, on ne

58. A.P.D., avis n° 64/2020 du 20 juillet 2020 relatif à une demande d'avis concernant un projet d'accord de coopération entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus Covid-19 sur la base d'une base de données auprès de Sciensano (CO-A2020-076), n^{os} 60 et 61.

59. Art. 4, 11° de l'accord de coopération concernant le traitement de données relatives aux vaccinations contre le Covid-19, tel qu'il figure dans le projet de loi portant assentiment à l'accord de coopération du 12 mars 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone,

peut donc exclure que le C.S.I. puisse autoriser que les données de vaccination soient transmises aux organismes assureurs. Ainsi donc, une banque pourrait-elle refuser à un client d'assurer son emprunt hypothécaire au motif qu'il n'est pas vacciné ? Le flou du texte ne permet pas de l'exclure.

Cette délégation de compétence va à l'encontre de l'avis de la section de législation du Conseil d'État précité, mais également de l'Autorité de protection des données. À plusieurs reprises, celle-ci a critiqué le recours à la notion d'« instance ayant une mission d'intérêt public ». Elle affirme notamment qu'« étant donné que la vaccination sur le territoire belge est déjà en cours depuis 1 à 2 mois, l'Autorité estime qu'il doit être possible de déterminer les flux de données nécessaires à cette fin vers des destinataires tiers ». Et de qualifier l'article 5 de l'accord de coopération de « chèque en blanc laissant ouvertes de larges possibilités de partage ultérieur des données avec des instances qui ne sont pas encore spécifiées, en vue de finalités qui ne sont pas strictement délimitées ». L'A.P.D. recommande dès lors que « les flux de données complémentaires [qui s'avéraient nécessaires » à l'avenir fassent « l'objet d'un encadrement législatif »[60].

Quant au *profilage* organisé par l'arrêté ministériel du 12 janvier 2021, compte tenu de la large compétence du C.S.I. comme utilisé précédemment concernant les données de sécurité sociale, on peut raisonnablement en déduire que ce dernier est compétent pour autoriser, seul, la réutilisation, pour des finalités autres que sanitaires, des données Covid centralisées par l'O.N.S.S.[61], y compris pour les croiser avec différentes données et y appliquer des algorithmes de *datamining* à des fins de lutte contre la fraude fiscale[62] et/ou sociale[63], et ce, sans être soumis au respect de critères clairs fixés par le législateur.

Contrôle technique. Devrait-on supprimer le C.S.I. ? Pas nécessairement. À la base, l'idée n'est pas mauvaise. Cet organe pourrait constituer une « couche » de contrôle supplémentaire dans les

la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre le Covid-19, *Doc. parl.*, Ch. repr., sess. 2020-2021, n° 55-1853/001, p. 113.

60. A.P.D., avis n° 16/2021 du 10 février 2021 concernant un projet d'accord de coopération entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre le Covid-19 (CO-A-2021-021), n° 44.
61. En vertu de l'art. 18 de la loi C.S.I.
62. Art. 71, al. 2, de la loi C.S.I.
63. Art. 13, al. 3, de la loi C.S.I.

matières délicates que sont la sécurité sociale et la santé, voire pour l'ensemble des données traitées par l'État[64], à la condition que ce contrôle soit balisé clairement par des critères fixés dans la loi et qu'il prenne la forme de décisions publiques, aisément accessibles et susceptibles de recours. Il s'agirait, par exemple, de vérifier que les données dites « anonymisées » le sont réellement, avant d'en autoriser le transfert. Le C.S.I. réaliserait là un contrôle technique, à l'image d'un contrôle technique pour les automobiles, chargé de vérifier l'état de la voiture avant de prendre la route et non de définir l'âge légal pour conduire…

L'Autorité de protection des données abonde d'ailleurs en ce sens, affirmant qu'« une délibération du Comité de sécurité de l'information peut évidemment apporter une plus-value en précisant davantage les modalités d'exécution, notamment au niveau de la sécurité de l'information », à la condition qu'« outre la description fonctionnelle des systèmes d'information et des flux d'informations qui ont fait l'objet d'une délibération […] les délibérations proprement dites du Comité de sécurité de l'information soient aussi publiées immédiatement et intégralement et qu'elles puissent être consultées pendant une longue période »[65].

Mais actuellement, ces balises sont quasiment inexistantes. Le pouvoir discrétionnaire du C.S.I. est si large que ce dernier se substitue au législateur et ses délibérations aux lois. Par ailleurs, ces délibérations, dont le statut juridique est incertain, sont difficilement accessibles[66].

64. Il s'agirait ainsi de faire du C.S.I. un « super D.P.O. », c'est-à-dire un délégué à la protection des données qui chapeauterait l'ensemble des autorités publiques, chargé d'aider les administrations à mettre en place des collectes et des échanges de données en toute légalité.
65. A.P.D., avis n° 16/2021 du 10 février 2021 relatif à un projet d'accord de coopération entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre le Covid-19 (CO-A-2021-021), n° 45.
66. Enfin, les décisions modifiées à une certaine date ne sont pas reprises à la date de modification mais à la date initiale d'adoption, ce qui rend par exemple très compliqué, voire impossible, le fait de retrouver, par exemple, les décisions du C.S.I. au sujet de l'utilisation des données Covid à des fins de profilage. À cet égard, voy. www.ksz-css.fgov.be/sites/default/files/assets/protection_des_donnees/deliberations/20_178_f036.pdf.

Conclusion

La centralisation des données par l'État n'a pas été provoquée par le Covid. C'est une tendance lourde et insidieuse qui se dessine depuis plusieurs années déjà. La pandémie a accentué ce phénomène et a donné un coup de projecteur salutaire aux enjeux démocratiques qui la sous-tendent.

Dans l'opacité de l'administration et la technicité de la matière, la gestion des données par l'État risque de devenir une affaire de technocrates, à qui l'on confie la mise en place d'un outil performant. Ces personnes ne sont pas nécessairement malveillantes, mais on ignore quels sont leurs intérêts économiques et politiques. Et si le projet mené n'est pas liberticide aujourd'hui, qu'en sera-t-il demain, à l'heure où la montée de l'extrême droite n'est plus une hypothèse en Europe ? En outre, pour remplir leur mission, ces technocrates n'auront-ils pas à cœur de poursuivre un objectif d'efficacité, laissant de côté, peut-être, les réflexions relatives à la protection des libertés citoyennes, risquant alors de nuire encore davantage à la confiance du citoyen en l'État ?

Aujourd'hui, il importe que l'État puisse s'aider du numérique pour accomplir ses missions. Des traitements de données doivent être mis en place pour soutenir notamment la lutte contre un virus. Mais, pour autant, il convient de ne pas basculer dans un État automatisé recourant à des outils dont il n'aurait déjà plus lui-même la maîtrise, construits en dehors de tout débat démocratique et sans être soutenus par des mesures de transparence permettant de maintenir le dialogue entre un État efficace et un citoyen qui pose des questions, hésite, remet en question, cherche des réponses à ses interrogations. Il faut également veiller à ce que les troubles créés aujourd'hui par la mise en place des bases de données liées au Covid n'ébranlent pas la confiance des citoyens en l'État au point de remettre en question toute utilisation de données par l'administration, y compris celles qui sont nécessaires et légitimes dans l'accomplissement des missions quotidiennes du service public[67].

C'est pourquoi la gestion des données en cas de pandémie mérite que l'on s'y penche en profondeur aujourd'hui, pour préparer demain. Il serait ainsi utile de faire le point sur les outils de traitement de données nécessaires en cas de crise et de les encadrer dans une loi claire et prévisible. À cet égard, l'expérience du Covid est d'ailleurs riche d'enseignements. Il s'agirait de rédiger une loi spécifique sur la gestion des

67. On pense notamment aux mesures de simplification administratives, comme le paiement automatique de certaines allocations ou le pré-encodage des déclarations fiscales.

données par l'État en cas de pandémie, en encadrant, dès à présent, et si le Parlement les estime nécessaires, le traçage, la vaccination et, le cas échéant, le profilage, d'une manière plus satisfaisante que les normes actuelles dont la présente étude a souligné les faiblesses[68]. Le rôle du C.S.I. doit également être revu, pour en faire un organe qui peut certes être utile, mais doit se limiter à réaliser un contrôle technique.

La pandémie nous aura rappelé que ce qui est technologiquement faisable n'est pas nécessairement démocratique acceptable. Le numérique, plutôt que de traquer le citoyen, doit lui permettre de s'impliquer en société. Pour qu'il n'éteigne pas la démocratie, mais au contraire la stimule. C'est là un magnifique défi pour le droit public.

*

* *

68. C'est d'ailleurs ce que nous avons suggéré à la commission justice de la Chambre lors des auditions au sujet de l'avant-projet de loi « Pandémie » le 10 mars 2021.