

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Les droits fondamentaux à l'épreuve du confinement et du déconfinement

Parsa, Saba; Poulet, Yves

Published in:

La pandémie de Covid-19 face au droit

Publication date:

2020

[Link to publication](#)

Citation for pulished version (HARVARD):

Parsa, S & Poulet, Y 2020, Les droits fondamentaux à l'épreuve du confinement et du déconfinement: le tracing. dans *La pandémie de Covid-19 face au droit*. Anthemis, Limal, pp. 137-217.
<<http://www.crid.be/pdf/crid5978-/8670.pdf>>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Les droits fondamentaux à l'épreuve du confinement et du déconfinement : le *tracing*¹

Saba PARSA

Avocate au barreau du Brabant wallon
Première Vice-Présidente du Conseil supérieur de l'audiovisuel
Professeure de droit à la HE2B
Déléguée à la protection des données des Ordres et du barreau de Bruxelles

Yves POULLET²

Professeur émérite à la Faculté de droit de Namur
Professeur associé à l'UCLille
Membre de l'Académie royale de Belgique

Introduction

1. L'enjeu du débat. La gestion de la pandémie de Covid-19 a mis à l'épreuve nos sociétés, nos gouvernements et nos concitoyens. La solidarité et la coopération, montées en étendard dans la lutte contre ce virus, soutiennent les mesures liberticides qui se démultiplient dans tous les domaines du droit. Confinement de la population, fermeture des commerces, théâtres et salles de cinéma, fermeture des frontières, mise en œuvre à grande échelle de tests sérologiques ou virologiques, isolement des malades ou des personnes à risque, prise de température par caméra thermique, *tracing* de la population, de telles mesures arrêtées au nom de l'état d'urgence sanitaire menacent aujourd'hui, parfois de manière durable, nos droits fondamentaux. Pourtant, dans nos sociétés démocratiques modernes, ces mêmes droits sont inscrits explicitement dans nos Constitutions ou dans des textes à valeur constitutionnelle, ainsi que dans des conventions internationales et européennes qui leur sont spécifiquement dédiées³. La Présidente de la Commission européenne, Madame Ursula von

¹ La présente contribution est arrêtée en date du 20 octobre 2020.

² L'auteur peut être contacté à l'adresse : yves.poullet@unamur.be.

³ Notamment : la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, 4 novembre 1950, entrée en vigueur le 14 juin 1955, *M.B.*, 19 août 1955, ci-après la CEDH ; la Charte des droits fondamentaux de l'Union européenne, du 12 décembre 2007, 2016/C 202/02, Version consolidée, *J.O.*, 7 juin 2016, ci-après la Charte ; le Pacte international relatif aux droits économiques, sociaux et culturels, résolution 2200 A (XXI) des Nations Unies, du 16 décembre 1966, entré en vigueur le 21 juillet

der Leyen, s'est ouvertement inquiétée en rappelant qu'«il est crucial que les mesures d'urgence qui sont prises ne le soient pas au détriment de nos valeurs et des principes fondamentaux énoncés dans les traités»⁴. En ce sens, la Secrétaire générale du Conseil de l'Europe, Madame Marija Pejčinović Burić, a publié une «boîte à outils» sur le respect des droits de l'homme destinée à tous les gouvernements européens pour les accompagner dans la gestion de la crise du Covid-19⁵. Ne serait-il pas important de s'interroger sur la façon dont la Belgique justifie dès lors les limitations, voire les dérogations apportées à certains droits fondamentaux⁶?

Dans la lutte contre le virus, le «numérique» est apparu comme la solution à tous les maux. Ayant définitivement gagné la bataille de la connexion de nos foyers et de nos entreprises, il a sauvé l'économie grâce à la digitalisation des services et la vente en ligne et ambitionne maintenant de prévenir ou protéger les populations face au fléau sanitaire par un traçage systématique et automatique des personnes concernées. Ces solutions sont, à raison, accompagnées de leurs lots de contestations sur fond de droits fondamentaux, avec une ardeur parfois étonnante eu égard au peu d'intérêt apporté aux autres restrictions imposées par nos gouvernements. Le combat numérique semble avoir cristallisé les revendications des défenseurs de l'État de droit et des libertés fondamentales.

Partant, dans la première partie de cette contribution seront abordées brièvement les ingérences à l'ensemble des droits fondamentaux dans le cadre de la gestion de la pandémie de Covid-19 (section 1) pour ensuite, de manière plus spécifique, s'attarder, à propos de l'utilisation du numérique dans cette lutte, sur la question relative à la protection de la vie privée et des données à caractère personnel (section 2).

1983, M.B., 6 juillet 1983, ci-après le PIDESC; le Pacte international relatif aux droits civils et politiques, résolution 2200 A (XXI) des Nations Unies, du 16 décembre 1966, entré en vigueur le 21 juillet 1983, M.B., 6 juillet 1983, ci-après le PIDCP; la Déclaration universelle des droits de l'homme, résolution 217 III A des Nations Unies, 10 décembre 1948, entrée en vigueur le 31 mars 1949, M.B., 31 mars 1949, ci-après la DUDH.

⁴ https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_1657; consulté en dernier lieu le 15 octobre 2020.

⁵ Document d'information SG/Inf(2020)11, disponible à l'adresse: <https://rm.coe.int/sg-inf-2020-11-respecter-la-democratie-l-etat-de-droit-et-les-droits-d/16809e1f3f>; consulté en dernier lieu le 18 septembre 2020.

⁶ Voy. *infra*, n° 5.

Section 1

Restriction, limitation, dérogation... Les droits fondamentaux contaminés par la gestion de la pandémie**2. Le respect des droits humains : de l'ardente obligation aux limites.**

Au terme d'un processus de développement remarquable depuis la Seconde Guerre mondiale, les droits de l'homme n'ont cessé de se réinventer. Tels qu'ils sont actuellement consacrés dans les textes internationaux et dans notre Constitution, ils apparaissent comme un ensemble très diversifié de valeurs et d'intérêts dont le respect est jugé indispensable pour garantir la liberté et la dignité humaine⁷. Ils appartiennent à tout individu⁸ et s'imposent aux autorités publiques (effet vertical), qui doivent également mettre en œuvre des mesures adéquates pour en assurer le respect par les individus dans leurs interactions (effet horizontal). Cette évolution entraîne des conséquences certaines, notamment dans l'établissement des limites particulières que se voient imposer certains droits individuels ou l'importance spécifique que se voient accorder d'autres droits en fonction du rôle qu'ils jouent dans les rapports sociaux et politiques⁹.

Dès lors, lorsqu'en Belgique, le rapport entre les assemblées législatives et les gouvernements mais, également, l'équilibre entre les différents niveaux de pouvoir, sont malmenés au nom de l'état d'urgence sanitaire par l'adoption de lois d'exception par les gouvernements, les droits de l'homme s'en retrouvent indéniablement écorchés, par des mesures qui s'apparentent plus à des dérogations qu'à des limitations¹⁰. Pour ce faire, dans un premier temps, le cadre légal des restrictions ou dérogations sera dressé (§ 1), afin de pouvoir au mieux examiner la légalité des mesures qualifiées de « liberticides » qui sont prises dans le contexte de la crise sanitaire (§ 2).

⁷ Pour reprendre les termes du Professeur Frédéric Sudre, les droits de l'homme doivent être entendus comme « les droits et facultés assurant la liberté et la dignité de la personne humaine et bénéficiant de garanties institutionnelles », in Fr. SUDRE, *Droit européen et international des droits de l'homme*, 10^e éd., Paris, PUF, 2011, p. 13 ; en ce sens K. VASAK, « Les différentes catégories des droits de l'homme », in A. LAPEYRE, F. DE TINGUY et K. VASAK (dir.), *Les dimensions universelles des droits de l'homme*, t. I, Bruxelles, Bruylant, 1990, pp. 301-309 ; Chr. TOMUSCHAT, *Human Rights. Between Idealism and Realism*, Oxford, Oxford University Press, 2003, pp. 24-52.

⁸ En ce sens : P. GÉRARD, « Chapitre I^{er} – L'esprit des droits », in *L'esprit des droits*, Bruxelles, Larcier, 2016, p. 15. *Contra* : M. DEFLEM et S. CHICOINE, « The Sociological Discourse on Human Rights: Lessons from the Sociology of Law », *Development and society*, juin 2011, vol. 40, n° 1, p. 104 ; voy. également L. DAMAY, F. DELMOTTE, « Les droits de l'homme entre ruptures et continuité : un éclairage historico-sociologique/ Human Rights between Disruption and Continuity: A Historical-Sociological Clarification », *J.E.D.H.*, 2016/2, p. 167.

⁹ P. GÉRARD, « Chapitre II – La légitimité des droits », in *L'esprit des droits*, Bruxelles, Larcier, 2016, p. 69.

¹⁰ Voy. pour la différence *infra*, n° 5.

§ 1. Des droits fondamentaux et de leurs restrictions ou limitations

3. Un difficile équilibre au temps de la pandémie de Covid-19.

Confrontés à une situation caractérisée par une grande incertitude, nos gouvernements, tant à l'échelon fédéral que fédéré, ont pris des mesures fortes visant à restreindre strictement les contacts entre personnes¹¹, telles que la fermeture des écoles, des commerces non alimentaires, des maisons de repos, la limitation des contacts intrafamiliaux. L'objectif principal était de limiter la saturation des services hospitaliers et particulièrement les soins intensifs, au risque de voir le taux de mortalité fortement augmenter. Ces mesures à caractère clairement liberticide et avec des effets négatifs encore difficiles à évaluer sur l'économie, visaient, et pour partie visent encore, à assurer les droits fondamentaux à la vie et à la santé.

Ce jeu d'équilibre entre les droits fondamentaux à charge des États est connu. De tout temps, les droits fondamentaux ont connu des limitations ou restrictions¹². Elles découlent des conflits entre les obligations concrètes¹³ découlant du besoin de protection inhérent à certains droits fondamentaux¹⁴ ou à certains objectifs d'intérêt général, tels que la santé publique¹⁵.

4. Les limites des droits fondamentaux – La Déclaration des droits de l'homme. Déjà en 1789, la Déclaration des droits de l'homme et du citoyen prévoyait en ses articles 4 et 5 ce qui suit :

- Article 4 : « La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui ; ainsi l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la loi ».
- Article 5 : « La loi n'a le droit de défendre que les actions nuisibles à la société. Tout ce qui n'est pas défendu par la loi ne peut être empêché et nul ne peut être contraint de faire ce qu'elle n'ordonne pas ».

¹¹ Il s'agit principalement des mesures de confinement, la définition de « bulles » de contact et de distanciation sociale, ou physique.

¹² Les notions de restrictions et de limitation des droits fondamentaux sont ici entendues comme synonymes, on parlera communément de limitation de l'exercice des droits fondamentaux pour la Charte et de restriction de l'exercice des droits fondamentaux pour la Convention européenne des droits de l'homme. Dans les deux cas, ces mesures sont perçues comme énonçant les conditions auxquelles une restriction de l'exercice d'un droit fondamental protégé par ses instruments internationaux peut être justifiée, nous parlerons de manière générale alors « d'exceptions ».

¹³ Ces obligations peuvent être positives ou négatives et revêtir soit la forme d'obligation de respecter un droit (droit-liberté) ou d'obligation de protéger (droits-créances).

¹⁴ S. BESSON, *The Morality of conflict. Reasonable Disagreement and the law*, Oxford-Portland (Oregon), Hart Publishing, 2005, p. 465.

¹⁵ Intérêt reconnu par la Charte, en son article 52, § 1, in S.-U. COLELLA, « Chapitre 1 – L'acceptation des notions de restriction, limitation et dérogation », in *La restriction des droits fondamentaux dans l'Union européenne*, Bruxelles, Bruylant, 2018, p. 126.

Le prescrit des dispositions de ces deux articles témoigne que la mise en œuvre des droits fondamentaux implique nécessairement, et dès l'origine, une démarche conciliatoire, dans un système qui refuse toute hiérarchie entre ces normes à valeur constitutionnelle. Dès lors, lorsque surgit un conflit entre plusieurs de ces droits fondamentaux, le seul moyen de le résoudre consiste à limiter ou restreindre ces droits en vue d'assurer ainsi leur coexistence, par l'examen, en termes de proportionnalité, des atteintes respectives portées à ceux-ci, sans jamais aboutir à dénaturer les droits en conflit¹⁶.

5. Limitation ou dérogation. La limitation des droits fondamentaux ne doit pas être confondue avec la dérogation ou suspension de ces droits. Les dérogations mettent «entre parenthèses» les libertés fondamentales pour une période donnée, dans des circonstances exceptionnelles données, telles que l'état d'urgence sanitaire, les atteintes terroristes, l'état de guerre¹⁷. Il s'ensuit que les États ne sont plus alors contraints de satisfaire les conditions de justification imposées pour les restrictions aux droits fondamentaux lorsqu'ils se trouvent dans ces circonstances spécifiques de dérogation¹⁸.

Un examen des modalités de la mise en œuvre des dérogations et des limitations des droits fondamentaux prévues par la Charte des droits fondamentaux de l'Union européenne (ci-après la Charte) et par la Convention européenne des droits de l'homme (ci-après la Convention ou CEDH) (A) permettra de mieux appréhender la légalité des mesures prises par les gouvernements et leur conformité à la Constitution (B).

A. Les droits de l'homme protégés par les deux «Europes»

6. Une double consécration européenne. Si les droits de l'homme sont garantis par de nombreux instruments internationaux, cette contribution se limitera à l'examen de la Charte et de la CEDH, ces deux instruments s'étant rapidement invités à la table des discussions, et à raison¹⁹. Il n'est pas question en l'occurrence de s'attarder sur les distinctions entre les limitations des droits fondamentaux de la Charte et les restrictions aux droits dans la Convention, mais bien de définir un commun dénominateur dans les conditions requises à la mise en œuvre des mesures restrictives des libertés fondamentales à l'occasion de la gestion de la pandémie.

¹⁶ Fr. SUDRE, «Les conflits de droits. Cadre général d'approche dans la jurisprudence de la Cour européenne des droits de l'homme», in L. POTVIN-SOLIS (dir.), *La conciliation des droits et libertés dans les ordres juridiques européens*, Bruxelles, Bruylant, 2012, pp. 233-262.

¹⁷ S.-U. COLELLA, «Chapitre 1 – L'acception des notions de restriction, limitation et dérogation», *op. cit.*, p. 126.

¹⁸ O. DE SCHUTTER, *International Human Rights Law. Cases, Materials, Commentary*, 2^e éd., Cambridge, Cambridge University Press, 2014, p. 585.

¹⁹ À l'occasion de cette contribution, notre attention portera uniquement sur la protection offerte aux droits fondamentaux par ces deux instruments.

7. L'approche de l'Union européenne: de l'affirmation des droits à leurs limites: l'article 52 de la Charte. L'Union européenne a pris part au débat de manière critique. Le 10 juin, le Parlement européen, le Conseil européen, le Comité économique et social européen et le Comité des régions ont émis une communication relative à la lutte « contre la désinformation concernant la Covid-19 – Démêler le vrai du faux »²⁰, au vu de la montée des rumeurs et des désinformations présentes sur les plateformes²¹ de partage de contenu, également appelées les réseaux sociaux. Dans le même esprit, la Commission invite les États membres « à intensifier leurs efforts en ces temps de crise pour que les journalistes puissent travailler en toute sécurité, dans de bonnes conditions, et à reconnaître les médias d'information comme un service essentiel », assurant ainsi la liberté d'expression et le droit à l'information qui en est le corollaire²².

Outre cette intervention thématique et ciblée de l'Union européenne, c'est dans la formule de l'article 52 de la Charte européenne que sont consacrées les modalités de limitation des droits fondamentaux énoncées dans la Charte²³:

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être *prévue par la loi* et respecter le contenu essentiel desdits droits et libertés. Dans le respect du *principe de proportionnalité*, des limitations ne peuvent être apportées que si elles sont *nécessaires et répondent effectivement à des objectifs d'intérêt général* reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui »²⁴.

En outre, en son second paragraphe, l'article 52 rappelle l'importance du contexte juridique qui entoure la limitation d'un droit, en ce qu'il énonce que :

« Les droits reconnus par la présente Charte qui trouvent leur fondement dans les traités communautaires ou dans le traité sur l'Union européenne s'exercent dans les conditions et limites définies par ceux-ci ».

Cette précision est d'autant plus importante dans le contexte des mesures prises pour endiguer la pandémie que ces mesures ont impacté lourdement la liberté de circulation des citoyens européens, notamment par la fermeture des fron-

²⁰ Accessible à l'adresse: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation_fr; consulté en dernier lieu le 20 octobre 2020.

²¹ Cette communication, qui met l'accent sur la responsabilité des plateformes, s'inscrit dans la ligne de la politique européenne de corégulation en matière de désinformation, ou « fake news » qui avait poussé à la rédaction d'un Code européen de bonnes pratiques contre la désinformation. La Commission souligne la nécessité d'« intensifier leur coopération avec les vérificateurs de faits et à proposer de façon proactive l'accès à leurs programmes de vérification des faits aux organisations de tous les États membres de l'UE, ainsi que de son voisinage, dans toutes les langues »; voy. les rapports de GDI: <https://disinformationindex.org/2020/05/why-is-tech-not-defunding-covid-19-disinfo-sites/>; consulté en dernier lieu le 20 octobre 2020.

²² À ce propos, lire « Dix choses que fait l'UE pour lutter contre la Covid-19 et assurer la relance », détaillée sur le site (mise à jour le 21 octobre): www.consilium.europa.eu/fr/policies/coronavirus/10-things-against-covid-19/.

²³ Elle répond à celle utilisée par la Convention européenne des droits humains.

²⁴ Nous soulignons.

tières. Cette liberté de se déplacer est consacrée par les dispositions des articles 45 de la Charte, 21 du TFUE²⁵, qui doivent donc également trouver à s'appliquer. L'article 21 du TFUE énonce que « [t]out citoyen de l'Union a le droit de circuler et de séjourner librement sur le territoire des États membres, sous réserve des limitations et conditions prévues par les traités et par les dispositions prises pour leur application ». Enfin, parmi ces dispositions, la directive 2004/38/CEE prévoit en son chapitre VI les modalités relatives aux limitations « du droit d'entrée et du droit de séjour pour des raisons d'ordre public, de sécurité publique ou de santé publique ».

8. Le Conseil de l'Europe – Des limites et des dérogations. Le Conseil de l'Europe a également adressé des recommandations aux États membres en précisant les règles applicables aux dérogations telles que définies à l'article 15 de la Convention²⁶. En ce qui concerne les prescrits de la Convention de manière générale, les restrictions aux droits sont non pas regroupées dans un article valable pour l'ensemble des libertés proclamées, mais organisées dans le texte des dispositions qui consacrent le droit lui-même.

Ainsi, à titre exemplatif, l'article 10 de la Convention relatif à la liberté d'expression énonce en son paragraphe 2 que :

« L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, *restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires*, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire »²⁷.

Par ailleurs, en son article 17, la Convention énonce de manière plus générale le principe d'interdiction d'abus²⁸, de la sorte :

« Aucune des dispositions de la présente Convention ne peut être interprétée comme impliquant pour un État, un groupement ou un individu, un droit quel-

²⁵ Traité sur le fonctionnement de l'Union européenne, 2012/C 326/01, Version consolidée (ci-après TFUE), <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A12012E%2FTXT>; consulté en dernier lieu le 20 octobre 2020.

²⁶ Art. 15 CEDH.

²⁷ Nous soulignons.

²⁸ La jurisprudence relative à l'article 17 est rare et s'est principalement développée en matière de liberté d'expression et discours haineux. La Cour a ainsi jugé que certains propos, en raison de l'atteinte qu'ils portent à la démocratie, ne sont pas protégés par la liberté d'expression figurant à l'article 10 de la Convention. Il en va ainsi des discours injuriant un groupe de personnes pour des motifs discriminatoires ou légitimant la violence envers eux : les thèses négationnistes (Cour eur. D.H., arrêt *Garaudy c. la France*, 24 juin 2003, n° 65831/01; Cour eur. D.H., arrêt *M'Bala M'Bala c. la France*, 20 octobre 2015, n° 25239/13.), les propos islamophobes (Cour eur. D.H., arrêt *Norwood c. le Royaume-Uni*, 16 novembre 2004, n° 23131/03) ou antisémites (Cour eur. D.H., arrêt *Pavel Ivanov c. la Russie*, 20 février 2017, n° 35222/04), ou encore les propos justifiant des crimes de guerre comme la torture et les exécutions sommaires (Cour eur. D.H., arrêt *Orban et autres c. la France*, 15 janvier 2009, n° 20985/05) tombent dans le champ d'application de l'article 17.

conque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Convention ou à des limitations plus amples de ces droits et libertés que celles prévues à ladite Convention».

Ainsi, le régime général de la Convention autorise les restrictions, si ces dernières trouvent une base légale pour les fonder, que cette base poursuit un but légitime et que la restriction est proportionnée et strictement nécessaire à atteindre cet objectif²⁹. Ce régime est donc proche de celui énoncé par la suite à l'article 52 de la Charte.

Enfin, au-delà de ce régime, l'article 15 de la CEDH³⁰ autorise en outre, moyennant préalable information du Secrétaire général de la Convention, des dérogations à l'application des droits en cas d'état d'urgence :

« *En cas de guerre ou en cas d'autre danger public menaçant la vie de la nation, toute Haute Partie contractante peut prendre des mesures dérogeant aux obligations prévues par la présente Convention, dans la stricte mesure où la situation l'exige et à la condition que ces mesures ne soient pas en contradiction avec les autres obligations découlant du droit international* ».

Les dispositions de cet article de la Convention visent à introduire la théorie de l'état de nécessité, en imposant aux États membres des conditions strictes en vue d'encadrer l'exercice des dérogations³¹. On ajoute qu'il n'existe pas de disposition similaire dans la Charte européenne.

Parmi les conditions fixées au régime des dérogations de la Convention, on distingue trois conditions matérielles³² :

- premièrement, la survenance de circonstances graves telles qu'une guerre ou d'autres dangers publics menaçant la vie de la nation ;
- deuxièmement, une nécessité absolue ;
- troisièmement, le respect des autres obligations découlant du droit international.

²⁹ Il n'est pas ici le lieu d'énoncer les différences dans l'application du régime des limitations de la Charte et celui des restrictions de la Convention, mais bien de définir le plus petit commun dénominateur à charge des États.

³⁰ À propos de cet article invoqué par quelques pays membres du Conseil de l'Europe à d'autres occasions que la pandémie et souvent pour des raisons de lutte contre le terrorisme, voy. notamment, J.-Fr. RENUCCI, *Droit européen des droits de l'homme*, 6^e éd., Paris, LGDJ, 2015, pp. 33-35.

³¹ Il est intéressant de noter que la Belgique, à ce moment-ci, n'a pas (encore) utilisé cette exception à l'occasion de la pandémie, alors que d'autres pays ont démarré les procédures depuis la mi-mars, ainsi l'Arménie, l'Estonie, la Géorgie, la Lettonie, la République de Moldavie, la Roumanie, la Serbie, Saint-Marin, rejoints plus tard par le Royaume-Uni, l'Irlande, la France ; voy. Conseil de l'Europe (Press unit), « Fiche thématique : Dérogation en cas d'état d'urgence », septembre 2020, p. 2 ; www.echr.coe.int/documents/fs_derogation_fra.pdf ; consultée en dernier lieu de 20 octobre 2020 ; voy., pour des informations détaillées s'agissant du contexte dans lequel ces dérogations ont été formulées, la page internet du Bureau des Traités du Conseil de l'Europe.

³² Conseil de l'Europe, « Guide sur l'article 15 de la Convention européenne des droits de l'homme, Dérogation en cas d'état d'urgence », mis à jour le 31 décembre 2019 ; consulté en dernier lieu le 18 septembre 2020 sur le site : www.echr.coe.int/Documents/Guide_Art_15_FRA.pdf.

Sans doute les allusions de certains hommes politiques aux « temps de guerre »³³ accréditent-elles que l'urgence sanitaire est à mettre sur le même pied que la lutte contre l'ennemi armé. On regrette cette référence qui hante les esprits mais peut amener à justifier des exceptions, ou à tout le moins la durée de certaines de ces mesures au-delà de ce qui est nécessaire et tolérable dans un État de droit dans le cadre de la gestion d'une pandémie.

À ces conditions de fond, il faut rajouter une condition de forme, à savoir la notification au Secrétaire général du Conseil de l'Europe, tant des mesures prises que des motifs qui les ont inspirés, conformément au troisième paragraphe de l'article 15. Les États doivent également informer le Secrétaire général du Conseil de l'Europe de la date à laquelle « les dispositions de la Convention reçoivent de nouveau pleine application ». À partir de la mi-mars 2020, certains États membres du Conseil de l'Europe ont commencé à activer la possibilité de déroger aux obligations prévues par la Convention européenne des droits de l'homme en cas d'état d'urgence³⁴ et deux ont même déjà mis fin à la dérogation. Néanmoins, la Belgique n'a pas encore affirmé vouloir s'appuyer sur cette disposition, et ce, malgré l'adoption de mesures liberticides ; peut-être y procédera-t-elle à l'occasion de la seconde vague. Pour mémoire, c'est la première fois que cette clause est activée dans le cadre d'une crise sanitaire.

Il s'ensuit que, à défaut d'avoir notifié le Secrétaire général du Conseil de l'Europe de sa volonté de déroger à ses obligations, la Belgique doit se référer au régime général de la Convention et de la Charte applicable aux restrictions des droits fondamentaux. Dès lors, les exceptions aux libertés individuelles mises en œuvre par la Belgique, pour être conformes au droit européen et international, doivent, selon la jurisprudence du Conseil de l'Europe et le libellé de l'article 52 de la Charte européenne, répondre aux exigences suivantes³⁵ :

- se fonder sur une « loi » au sens large du terme ;
- ne pas heurter le « contenu essentiel » des droits et libertés en cause ;

³³ Nous faisons allusion notamment aux déclarations du Président Macron le 16 mars 2020, où il annonce aux Français que des mesures de confinement sont nécessaires pour freiner la propagation du Covid-19, et déclare sur un ton grave : « Nous sommes en guerre » ; www.lemonde.fr/politique/article/2020/03/17/nous-sommes-en-guerre-face-au-coronavirus-emmanuel-macron-sonne-la-mobilisation-generale_6033338_823448.html ; consultée en dernier lieu le 20 octobre 2020.

En France, le fondement légal du confinement s'inspire de deux origines militaires, de sorte que la référence à la guerre est bien plus qu'une métaphore, ainsi un premier décret du 16 mars 2020 en appelait à la théorie des circonstances exceptionnelles, remontant à la Première Guerre mondiale.

³⁴ Les premiers États ayant notifié le Secrétariat sont l'Arménie, l'Estonie, la Géorgie, la Lettonie, la Moldavie et la Roumanie.

³⁵ J. VELU, « Le droit pour les États de déroger à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales en cas de guerre ou d'autre danger public menaçant la vie de la nation », in *Les clauses échappatoires en matière d'instruments internationaux relatifs aux droits de l'homme*, Bruxelles/Louvain-la-Neuve, Bruylant/Cabay, 1982, pp. 71-147 ; R. ERGEC, *Les droits de l'homme à l'épreuve des circonstances exceptionnelles*, Bruxelles, Bruylant, 1987, 427 p.

- être justifiées par l'intérêt général ou les libertés d'autrui ;
- être proportionnées à ces objectifs légitimes poursuivis et être nécessaires dans une société démocratique.

Ce premier constat posé, il est possible de s'attarder sur les formalités imposées par le Constituant au législateur, dans le cadre des restrictions aux libertés fondamentales consécutives à la gestion de la pandémie.

B. La Constitution belge une protection sans failles des droits fondamentaux ?

9. Limitations ou suspension de droits au regard de la Constitution belge. Étonnamment, et nonobstant ce qui précède, par leur étendue, certaines limitations aux droits fondamentaux dictées par la lutte contre le Covid-19 ressemblent à s'y méprendre à de pures et simples suspensions de droits. Or, en Belgique, de telles suspensions ne sont pas autorisées par la Constitution. En effet, adopté en 1831, l'article 187 de la Constitution dispose que « la Constitution ne peut être suspendue en tout ni en partie ». Cette interdiction proscriit formellement l'instauration d'un « état d'urgence » ou d'un « état d'exception »³⁶, sauf en temps de guerre, en application de l'arrêté-loi du 11 octobre 1916 relatif à l'état de guerre et à l'état de siège³⁷. L'esprit du Constituant de 1831³⁸ est clair, sa volonté était d'empêcher la mise en place de régimes d'exception où les droits fondamentaux sont suspendus, même au nom de l'intérêt de la nation³⁹.

³⁶ M. VERDUSSEN, « Démocratie, État de droit et droits fondamentaux face à la pandémie de Covid-19 : perspectives croisées. La situation en Belgique », note de travail pour l'Unité mixte de recherche (UMR) « DICE – Droits International, Comparé et Européen », 15 avril 2020, p. 2 ; https://dice.univ-amu.fr/sites/dice.univ-amu.fr/files/public/m._verdussen-note_de_travail_ndeg_1-15_avril_2020.pdf?fbclid=IwAR2_eRA-ZRKInvMhmMZfzR-vW0qei-AP0ecaHmurErJCaBpD74mylz-qgbo ; consulté en dernier lieu le 20 octobre 2020.

³⁷ Les arrêtés-lois de guerre sont des règles exceptionnelles, de nature législative, adoptés durant les deux dernières guerres mondiales, ainsi pour les arrêtés-lois dits « du Havre », (arrêté-loi du 11 octobre 1916 relatif à l'état de guerre et à l'état de siège, *M.B.*, 15 octobre 1916 ; arrêté-loi du 11 octobre 1916 créant un service de la sûreté militaire, *M.B.*, 15 octobre 1916), adoptés durant la Première Guerre mondiale, ou pour les arrêtés-lois dits « de Londres », adoptés durant la Seconde Guerre mondiale ; leur adoption a été rendue nécessaire par l'impossibilité des Chambres législatives de se réunir librement sur le territoire national. C'est la Cour de cassation qui a reconnu force de loi aux arrêtés-lois, considérant que « l'impossibilité pour l'une ou pour l'autre branche du pouvoir législatif d'exercer librement la souveraineté nationale concentre la totalité du pouvoir législatif entre les mains de celle qui a ou qui ont conservé cette liberté », Cass., 11 février 1919, *Pas.*, 1919, I, p. 9 et Cass., 11 décembre 1944, *Pas.*, 1945, I, p. 65.

³⁸ François Van Snick, auteur de l'amendement qui a introduit l'article 187 dans la Constitution, lors des travaux du Congrès, s'exprime ainsi : « Les pouvoirs constitutionnels n'existant que par la Constitution, ils ne peuvent, dans aucun cas, ni sous aucun prétexte, en suspendre l'action [...]. Tous les pouvoirs qui se sont succédé en France, ont tour à tour violé et suspendu les constitutions qui devaient régir ce pays, et ce, en invoquant à chaque fois la grande loi : *Salus populi suprema lex esto* » (Congrès national, séance du 5 février 1831).

³⁹ Ch. HUBERLANT, « État de siège et légalité d'exception en Belgique », in J. VERHAEGEN (dir.), *Licéité en droit positif et références légales aux valeurs. Contribution à l'étude juridique du règlement des conflits de valeurs en droit pénal, public et international*, Bruxelles, Bruylant, 1982, p. 401.

Ceci vaut à la Constitution belge la qualification de « Constitution de temps de paix »⁴⁰.

La formule de l'article 187 implique que « les pouvoirs doivent continuer à être exercés même dans des circonstances de crise et de transition », car « même en pareilles circonstances, l'autorité doit défendre l'intérêt général et rencontrer les besoins collectifs »⁴¹. Enfin, rappelons que la formule de l'article 187 est restée intacte depuis 1831, et ce, nonobstant les nombreuses révisions auxquelles la Constitution a été soumise⁴². Ce constat est d'autant plus préoccupant que la Belgique n'a pas fait usage de son droit de notifier « l'état d'urgence », préalablement à l'adoption des mesures liberticides, au Secrétaire général de la Convention, conformément aux dispositions de l'article 15 de la CEDH.

Dès lors, les seules exceptions aux droits fondamentaux admises dans le cadre de la gestion de cette crise seront qualifiées de « limitations » et devront nécessairement passer l'examen de la balance des intérêts en exergue et à tout le moins répondre aux principes de légalité (§ 2, A) et de proportionnalité (§ 2, B) applicables au régime ordinaire de limitation des droits fondamentaux en vue de garantir l'État de droit⁴³.

§ 2. Les droits fondamentaux et leurs limitations sur fond de crise sanitaire en Belgique

10. Crises sanitaires et limitations des droits fondamentaux. De 1918 à 1919, de 1957 à 1958 et ensuite dix ans plus tard, en 1968, le monde a connu trois pandémies d'une ampleur aussi importante⁴⁴ que celle que l'on connaît

⁴⁰ Expression empruntée à Sébastien Van Drooghenbroeck in « L'article 187 de la Constitution », *Revue belge de droit constitutionnel*, n° 3, Bruxelles, Bruylant, 2006, p. 293.

⁴¹ J. VELAERS, « Les principes généraux du droit à "valeur constitutionnelle" : des incontournables de notre ordre constitutionnel », in I. HACHEZ (dir.), *Les sources du droit revisitées*, vol. 1, Normes internationales et constitutionnelles, Limal, Anthemis, 2012, p. 559.

⁴² Pour rappel, notre ordre juridique ne connaît qu'un « état de guerre » ou un « état de siège », tous deux prévus par un arrêté-loi relatif à l'état de guerre et à l'état de siège du 11 octobre 1916, *M.B.*, 15 octobre 1916. Cet arrêté envisage le transfert d'une série de pouvoirs des autorités civiles vers les autorités militaires et interdit les contacts avec l'ennemi.

⁴³ Cf. notamment Conseil d'État, section de législation, avis n° 67.142/AG, 25 mars 2020, p. 25. Dans ce contexte, la Ligue des droits humains (ci-après LDH) a adressé une lettre aux parlementaires et au gouvernement. La LDH ne conteste pas le principe des restrictions exceptionnelles mais attire l'attention sur les limites à ne pas dépasser. LDH, « Covid-19. Pouvoirs spéciaux : la Ligue des droits humains adresse une lettre aux parlementaires et au gouvernement », 26 mars 2020, www.liguedh.be/covid-19-pouvoirs-speciaux-la-ligue-des-droits-humains-adresse-une-lettre-aux-parlementaires-et-au-gouvernement/ ; consulté en dernier lieu le 20 octobre 2020.

⁴⁴ « Au cours du XX^e siècle, trois pandémies grippales sont survenues successivement. En 1918-1919, la pandémie dite de la "grippe espagnole" due au virus A(H1N1) a touché le monde entier. Les estimations accessibles sur le site de l'Organisation mondiale de la santé (OMS) indiquent qu'au moins 40 millions de personnes en seraient décédées. Les pandémies suivantes ont été beaucoup moins sévères : en 1957-58, la "grippe asiatique" liée au virus A(H2N2) et en 1968-69, la "grippe de Hong-Kong" due au virus A(H3N2). En 2009, une nouvelle pandémie est survenue, due à un nouveau virus A(H1N1) pdm09 qui résultait d'une combinaison de différents virus grippaux d'origine aviaire, porcine et humaine » (www.santepubli-

avec le Covid-19, sans pour autant restreindre les droits et libertés fondamentaux de manière aussi drastique.

À l'inverse, la crise sanitaire actuelle a été l'occasion, dès le 18 mars 2020⁴⁵, de restrictions importantes de nos droits et libertés fondamentaux⁴⁶. La première liberté restreinte a été la liberté d'aller et venir⁴⁷, sauf en cas de nécessité ou de raisons urgentes, suivie de l'interdiction de quitter le pays par la fermeture des frontières, sauf exception. Ensuite, les libertés de réunion⁴⁸ et de religion⁴⁹ et le droit à l'enseignement⁵⁰ ont été sévèrement limités⁵¹. Le droit au respect de la vie privée et familiale n'a pas non plus été épargné⁵², les personnes âgées ont été isolées⁵³. Enfin, le droit au travail⁵⁴ et la liberté d'entreprendre⁵⁵ ont été suspendus par la contrainte imposée aux entreprises de fermer afin de limiter la propagation du virus et atteindre l'objectif de santé publique en évitant essentiellement la saturation des hôpitaux.

Les conséquences de ces restrictions aux libertés pour les citoyens et les entreprises sont donc loin d'être anodines. L'UNIA le souligne lors d'une communication du 20 mars 2020 par trois exemples concrets au cœur de ses compétences :

« Les parents d'enfants handicapés placés en institution sont confrontés à un choix déchirant : soit ramener leur enfant lourdement handicapé à la maison et s'en occuper eux-mêmes, soit le laisser dans l'institution pendant les semaines de confinement avec peu de possibilités de communication.

Les personnes qui ont besoin d'une protection internationale ignorent totalement si elles pourront introduire une demande d'asile. Elles sont entre-temps privées du droit d'accueil et ne savent pas où aller.

quefrance.fr/maladies-et-traumatismes/maladies-et-infections-respiratoires/grippe/articles/les-grippes-pandemiques; consulté en dernier lieu le 20 octobre 2020; voy. également www.who.int/bulletin/volumes/90/4/12-020412/fr/; consulté en dernier lieu le 20 octobre 2020).

⁴⁵ Déjà dès le 13 mars, avec l'arrêté ministériel du 13 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, *M.B.*, 13 mars 2020, mais de manière conséquente à partir du 18 mars avec l'arrêté ministériel du 18 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, *M.B.*, 18 mars 2020.

⁴⁶ Arrêté ministériel du 23 mars 2020, portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, *M.B.*, 23 mars 2020; cet arrêté sera le texte fondateur de la grande majorité des mesures liberticides, il sera modifié au gré des Conseils nationaux de sécurité.

⁴⁷ Consacré notamment aux articles 12 de la Constitution, 2, § 1^{er}, du protocole n° 4 à la CEDH, 45 de la Charte, 5 de la CEDH, 12 du PIDCP.

⁴⁸ Consacré aux articles 26 de la Constitution, 11 de la CEDH, 12 de la Charte, 21 du PIDCP.

⁴⁹ Consacré aux articles 19 de la Constitution, 9 de la CEDH, 10 de la Charte, 18 du PIDCP.

⁵⁰ Consacré aux articles 24 de la Constitution, 2 du premier protocole à la CEDH, 14 de la Charte, 13 du PIDESC.

⁵¹ Les rassemblements ont été interdits, sous réserve d'exceptions très strictes.

⁵² Consacré aux articles 22 de la Constitution, 8 de la CEDH, 17 du PIDCP, 7 de la Charte.

⁵³ Pour la Région de Bruxelles-Capitale, l'arrêté du ministre-président du 7 avril 2020 prolongeant l'interdiction des visites dans les maisons de repos et de soins dans le cadre de mesures d'urgence pour limiter la propagation du Coronavirus – Covid-19, *M.B.*, 14 avril 2020.

⁵⁴ Consacré aux articles 23 de la Constitution, 6 du PIDESC, 15 de la Charte.

⁵⁵ Consacré à l'article 7 de la loi des 2 et 17 mars 1791 (décret d'Allarde), à l'article 1^{er} du premier protocole à la CEDH, et surtout à l'article 16 de la Charte.

Les personnes en situation de pauvreté et de précarité n'ont pas toujours accès aux ordinateurs et aux tablettes, ni à l'information diffusée électroniquement et par le biais des réseaux sociaux. Les enfants et les jeunes qui se trouvent dans de telles situations éprouvent de nombreuses difficultés dans le cadre de l'enseignement à distance actuellement préconisé. Les mesures renforcent donc les inégalités existantes en matière d'information et d'éducation»⁵⁶.

Pour ce qui concerne la liberté d'aller et venir, la liberté de se rassembler et de manifester, la suspension de l'enseignement, la liberté d'entreprendre, l'intensité et l'ampleur des limitations étaient telles qu'elles s'apparentent davantage à une véritable suspension de ces droits. Il en va de même des restrictions apportées au droit d'entreprendre, comme en témoigne le nombre d'entreprises qui, à la suite de leur fermeture rendue obligatoire sur pied des arrêtés de pouvoirs spéciaux, devront mettre la clé sous la porte. De telles suspensions voient leur légalité compromise par l'article 187 de la Constitution et par l'absence de notification de la Belgique au Secrétariat du Conseil de l'Europe.

Enfin, il ne faut pas non plus négliger les sanctions⁵⁷ qui accompagnent ces mesures, en vue d'en garantir l'effectivité. Assez naturellement, ces mesures suscitent des questions quant à leur légalité. À raison, l'on peut se demander si, au nom de l'état d'urgence et des impératifs de santé publique par ailleurs consacrés dans les textes internationaux relatifs aux droits humains, l'État n'a pas « oublié » les principes qui doivent s'appliquer à l'occasion de la dérogation aux droits fondamentaux.

Partant du constant qu'il ne peut s'agir de dérogations au risque de violer le prescrit de notre Constitution, notre examen les différentes mesures prises qui doivent respecter les conditions posées par le régime « ordinaire » des limitations inscrit tant dans les systèmes constitutionnels que conventionnels de protection des libertés fondamentales portera, d'une part, sur la légalité de ces mesures (A) et, d'autre part, sur leur nécessité (B) au regard de l'objectif exprimé.

A. Le principe de légalité des limitations

11. La double signification du principe de légalité. Le principe de légalité est une exigence de l'État de droit, il postule que le gouvernement n'agit que dans les limites de ses compétences établies par la loi. Dès lors, et dans le respect de la hiérarchie de normes qui prévalent en droit belge, il ne fait pas de doute qu'une ingérence dans un droit fondamental doit reposer sur un fondement puisé dans une norme législative et s'y conformer. L'exigence de

⁵⁶ www.unia.be/fr/articles/covid-19-des-mesures-de-protection-dans-le-respect-des-droits-fondamentaux; consulté en dernier lieu le 20 octobre 2020.

⁵⁷ Belga, « Coronavirus à Bruxelles: plus de 6000 PV dressés pour non-respect du confinement, les magistrats vont travailler durant l'été », le 11 juin 2020, RTBF info, site internet consulté en dernier lieu le 20 octobre 2020.

légalité revêt un aspect formel (1) et un aspect matériel (2), aspects examinés ci-après⁵⁸.

1. La légalité formelle

12. La légalité formelle et les pouvoirs spéciaux. Ce principe de légalité formelle implique sur le plan constitutionnel la nécessaire intervention d'un Parlement⁵⁹ dans l'adoption des règles restreignant les droits fondamentaux. Une délégation à un autre pouvoir reste néanmoins possible, aux conditions énoncées par l'article 105 de la Constitution. Une habilitation doit alors être définie de manière précise et les éléments essentiels de la mesure doivent être fixés préalablement par le législateur. En Belgique, déjà en 2009, le Parlement, en prévention de l'épidémie de grippe H1N1⁶⁰, pour cause d'urgence sanitaire, avait octroyé des pouvoirs spéciaux au Roi, pour une durée de six mois⁶¹. Cette loi permettait, en son article 3, par exemple de réquisitionner des professionnels autres que du personnel de santé pour aider en cas de vaccination massive. L'habilitation octroyée à l'occasion de l'adoption de cette loi de pouvoirs spéciaux présentait moins de risque de porter atteinte à nos libertés fondamentales. Néanmoins, en son article 3, alinéa 2, les arrêtés pris sur cette base permettaient d'abroger et d'amender les dispositions légales alors en vigueur et le Roi était également habilité à prévoir des sanctions administratives, civiles et pénales applicables en cas d'infraction à ces arrêtés.

En 2020, à l'occasion de la gestion de la pandémie Covid-19 la Belgique, alors sans gouvernement de plein exercice, fait à nouveau appel aux dispositions de

⁵⁸ La Cour européenne des droits de l'homme procède à une interprétation large de notion de « loi » et vise tant la loi au sens formel, qu'au sens matériel. La Cour estime que la question de l'appréciation de la nature d'une règle limitative d'un droit dépend avant tout des autorités nationales. La notion de loi peut donc recouvrir des textes non législatifs ou une jurisprudence constante et bien connue. En ce sens Cour eur. D.H., arrêt *De Wilde, Ooms et Versyp*, 18 juin 1971, série A, n° 12, p. 45, § 93; Cour eur. D.H., arrêt *Sunday Times*, 26 avril 1979, série A, n° 30, p. 30, § 47.

⁵⁹ En ce sens, la Cour de justice de l'Union européenne n'a pas hésité à écarter des limitations aux droits garantis pour lesquelles il n'existait aucune base législative, en constatant : « En l'absence de base légale expressément prévue à cet effet, une telle limitation est contraire aux principes fondamentaux de légalité et de respect des droits de la défense. Il convient, au demeurant, de relever que le droit à un recours effectif et à l'accès à un tribunal impartial est garanti par l'article 47 de la Charte des droits fondamentaux de l'Union européenne qui, conformément à l'article 6, paragraphe 1, premier alinéa, TUE, a la même valeur juridique que les traités. Selon l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et libertés reconnus par celle-ci doit être prévue par la loi » (CJUE, 1^{er} juillet 2010, *Knauf Gips KG*, C-407/08P).

⁶⁰ Loi du 16 octobre 2009 accordant des pouvoirs au Roi en cas d'épidémie ou de pandémie de grippe, *M.B.*, 21 octobre 2009, donc l'article 2 énonce ce qui suit : « Afin de permettre à la Belgique de se préparer et de réagir à une épidémie ou une pandémie de grippe qui présenterait un risque particulier et grave pour la santé publique, le Roi peut, par arrêté délibéré en Conseil des ministres, prendre les mesures visées à l'article 3 ».

⁶¹ L'habilitation a pris fin le 21 avril 2010, à l'expiration du délai de six mois prévu par le législateur, et ce, après la confirmation, par la loi du 23 mars 2010 de confirmation des arrêtés royaux pris en application des articles 2 et 3 de la loi du 16 octobre 2009 accordant des pouvoirs au Roi en cas d'épidémie ou de pandémie de grippe, *M.B.*, 29 mars 2010.

l'article 105 de la Constitution pour justifier l'adoption le 27 mars 2020 d'une loi habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus⁶² pour une première durée de trois mois. Cette habilitation sera néanmoins nettement plus large de celle octroyée en 2009⁶³. On note que les gouvernements fédérés ont réclamé la même délégation de compétences. Cette délégation large à des organes peu visibles et peu contrôlés démocratiquement n'est pas sans poser problème, car elle extrait du débat démocratique la gestion de la crise. En ce sens, dans son avis relatif à la proposition de loi de pouvoirs spéciaux habilitant le gouvernement (le Roi) à prendre des mesures nécessaires à la lutte contre la propagation du coronavirus⁶⁴, le Conseil d'État avait averti du risque que de nombreuses mesures portent atteinte aux droits fondamentaux en vigueur dans l'ordre juridique belge. Il invita le gouvernement fédéral à vérifier, soigneusement et *in concreto*, le respect par ces mesures des conditions permettant de déroger aux droits fondamentaux.

13. Les arrêtés ministériels de mars 2020 et leur légalité. Pourtant, l'illégalité du premier texte instituant les premières privations de liberté est évidente⁶⁵, et ne fut pas corrigée immédiatement. En effet, au regard de l'urgence et en violation du principe de légalité formelle, en date du 13 puis du 18 mars 2020, et enfin du 23 mars 2020, soit encore quatre jours avant le vote de la loi d'habilitation, par voie d'arrêté, le Ministre de l'Intérieur, Monsieur de Crem, adoptera seul, par voie d'arrêté ministériel, de nombreuses mesures restrictives des droits fondamentaux. Ainsi, il y est énoncé, de manière laconique : l'obligation de télétravail à domicile ; la fermeture des principaux commerces ; la restriction d'accès aux grandes surfaces ; la fermeture des marchés ; l'interdiction de principe des « rassemblements » ; l'interdiction des « activités à caractère privé ou public, de nature culturelle, sociale, festive, folklorique, sportive et récréative », ou encore « religieuses » ; l'interdiction des « excursions scolaires » ou des « mouvements de jeunesse » ; la suspension de l'enseignement fonda-

⁶² Loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus Covid-19 (II), M.B., 30 mars 2020.

⁶³ À la lecture du texte de la loi, l'objectif cité à l'article 2 et les mesures énoncées à l'article 5 sont limités par les dispositions des articles 2 et 3. Ces limitations formulées de manière peu précise sont source d'insécurité juridique, suivant l'avis du Conseil d'État (avis n° 67.142/AG du 25 mars 2020, *op. cit.*, p. 30). Ces articles disposent que : « Art. 3. Les arrêtés royaux pris en vertu de la présente loi ne peuvent pas porter atteinte au pouvoir d'achat des familles et à la protection sociale existante » ; « Art. 4. Les arrêtés royaux pris en vertu de la présente loi ne peuvent pas adapter, abroger, modifier ou remplacer les cotisations de sécurité sociale, les impôts, les taxes et les droits, notamment la base imposable, le tarif et les opérations imposables ».

⁶⁴ Conseil d'État, section de législation, avis n° 67142/AG du 25 mars 2020, *op. cit.*, §§ 6.1.1 et 6.1.2.

⁶⁵ En ce sens, le Tribunal de police du Hainaut, division de Charleroi, a considéré dans un jugement du 21 septembre 2020 que le confinement imposé par l'arrêté ministériel du 23 mars 2020, modifié le 3 avril était illégal. Le juge considère que la Constitution belge n'a pas été respectée. Le juge stipule que : « Sans doute, la répression est-elle nécessaire pour appréhender certains comportements dans le cadre d'une gestion d'une épidémie, mais pas au détriment de l'État de droit. Seul le législateur est habilité à prendre de telles décisions. Il dispose seul de la légitimité démocratique d'évaluer tous les intérêts et valeurs en présence et de les mettre en balance. Dans une démocratie, la fin ne justifie pas les moyens ».

mental et l'obligation d'enseignement à distance dans les niveaux supérieurs. Le ministre s'est fondé sur diverses dispositions législatives⁶⁶ pour adopter ces mesures d'urgence visant à limiter la pandémie de coronavirus ; or, le choix même des dispositions n'est pas sans poser problème quant à la légalité des restrictions apportées au droit.

En ce sens, Marc Verdussen précise que : « Parmi ces dispositions, le fondement sur l'article 182 de la loi du 15 mai 2007, qui prévoit que "[l]e ministre [ayant l'intérieur dans ses attributions] ou son délégué peut, en cas de circonstances dangereuses, en vue d'assurer la protection de la population, obliger celle-ci à s'éloigner des lieux ou régions particulièrement exposés, menacés ou sinistrés, et assigner un lieu de séjour provisoire aux personnes visées par cette mesure ; il peut, pour le même motif, interdire tout déplacement ou mouvement de la population", semble douteuse. Cette disposition ne précise pas, selon nous, les éléments essentiels des mesures, et n'encadre pas davantage les objectifs à poursuivre lors de leur adoption. La base légale semble donc insuffisante pour rencontrer l'exigence de légalité formelle »⁶⁷.

La jurisprudence des juridictions ordinaires tend à rejoindre cette position, et à ce titre, le Tribunal de police du Hainaut, division de Charleroi, considère dans un jugement du 21 septembre 2020 que le ministre de l'Intérieur ne pouvait pas prendre des mesures sur la base de l'article 182 de la loi du 15 mai 2007 relative à la protection civile⁶⁸. Le juge précise que : « les mesures de police générale décidées par voie d'arrêtés ministériels tendant à interdire un certain nombre de rassemblements, à limiter les déplacements et à imposer une distance physique entre les individus ne peuvent se voir assortir de sanctions prévues par l'article 187 de la loi sur la sécurité civile [...]. Dès lors, condamner à une peine en dehors du cadre strict de l'article 182 de la loi sur la sécurité civile violerait non seulement la loi mais aussi la Constitution ». Ces ingérences dans les droits des citoyens belges, initialement prévues jusqu'au 5 avril 2020⁶⁹, feront l'objet de plusieurs prolongations⁷⁰, puis de modifications au gré des conférences du Conseil de sécurité, dont elle devient le bras armé juridique.

⁶⁶ À savoir, la loi du 31 décembre 1963 sur la protection civile, de la loi du 5 août 1992 sur la fonction de police et de la loi du 15 mai 2007 relative à la sécurité civile.

⁶⁷ S'agissant du choix des dispositions voy. M. VERDUSSEN, « Démocratie, État de droit et droits fondamentaux face à la pandémie de Covid-19 : perspectives croisées. La situation en Belgique », *op. cit.*, p. 2.

⁶⁸ En ce sens, le Tribunal de police du Hainaut, division de Charleroi, a considéré dans un jugement du 21 septembre 2020 que le confinement imposé par l'arrêté ministériel du 23 mars 2020 est illégal. Le jugement fait l'objet d'un appel.

⁶⁹ Arrêté ministériel du 13 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, *M.B.*, 13 mars 2020 ; arrêté ministériel du 18 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, *M.B.*, 18 mars 2020 ; arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, *M.B.*, 23 mars 2020.

⁷⁰ L'article 13 de l'arrêté ministériel du 23 mars 2020, portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, *M.B.*, 23 mars 2020, tel que remplacé le 3 avril 2020 par la disposition suivante : « Les mesures prescrites par le présent arrêté sont d'application jusqu'au 19 avril 2020 inclus. Elles peuvent être prolongées de deux semaines après évaluation », cet arrêté a été modifié en dernier lieu

Ainsi, l'arrêté ministériel du 23 mars, originellement appelé arrêté « confinement », deviendra, dès la fin du mois de mars, l'arrêté « déconfinement ». Ajoutons à cela que certaines mesures incluses dans l'arrêté ministériel empiètent de manière flagrante sur les compétences des autorités fédérées.

Enfin, il faut également questionner cette nouvelle « pratique légistique », pour le moins surprenante consistant à communiquer, voire compléter les textes législatifs par ce qui est communément appelé des FAQ ou « Questions fréquemment posées ». L'importance du recours aux FAQ a été souvent soulignée lors des débats au Parlement. Si, en théorie, elles demeurent juridiquement subordonnées à l'adoption de l'arrêté qu'elles entendent expliquer de manière plus pédagogique, dans les faits, elles les ont régulièrement précédés et complétés en violation de la jurisprudence du Conseil d'État sur l'admissibilité des circulaires émanant d'une administration. Rappelons à la faveur d'une jurisprudence récente du Conseil d'État que ces FAQ ne peuvent rajouter des contraintes ne figurant pas dans la législation⁷¹ ou de nouvelles conditions.

2. La légalité matérielle

14. La légalité matérielle – Signification. Dans la droite ligne de la jurisprudence strasbourgeoise, la légalité matérielle concentre aujourd'hui de nombreuses revendications en matière de légalité. Ce principe suppose, notamment, que le fondement légal de la restriction soit prévisible, à savoir clair et précis. Dans la jurisprudence européenne, une ingérence pour se conformer à l'exigence de légalité doit présenter deux qualités fondamentales : son accessibilité et sa prévisibilité. La jurisprudence de la Cour européenne des droits de l'homme considère, en effet, que, pour que l'ingérence soit acceptable, la loi « soit suffisamment accessible et 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 dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé »⁷².

Or, le libellé des interdictions, souvent vague et ambigu⁷³, qui se succèdent laisse perplexe. Si les lecteurs les plus expérimentés⁷⁴ se posent de multiples questions

le 5 juin 2020, et abrogé par l'arrêté ministériel 30 juin 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, lui-même modifié à de nombreuses reprises.

⁷¹ C.E., arrêt n° 241.673 du 30 mai 2018, ASBL *le Théâtre-Poème*; C.E., arrêt n° 243.790 du 22 février 2019, SA *Ufund*.

⁷² Cour eur. D.H. (Gde Ch.), arrêt *Dubská et Krejzová c. République tchèque*, 15 novembre 2016, requêtes n°s 28859/11 et 28473/12, n° 167.

⁷³ En ce sens : Fr. LOUIS, « PV classés sans suite ? L'arrêté ministériel sur le confinement, un texte qui favorise l'insécurité juridique », 15 avril 2020, RTBF, www.rtbf.be/info/regions/detail_l-arrete-ministeriel-sur-le-confinement-un-texte-qui-favorise-l-insecurite-juridique?id=10481972; consulté en dernier lieu le 20 octobre 2020.

⁷⁴ Avis de Nicolas Thirion in Fr. LOUIS, *ibid.*; J. PIERET, « Carnet de crise #16 du 20 avril 2020 : la gestion de la pandémie du Covid-19 et les dérogations aux droits et libertés : faut-il recourir à l'article 15 de la Convention européenne des droits de l'homme? », in *Carnet de crise du centre de droit public de l'ULB*, 20 avril

à leur lecture, qu'en est-il dès lors des citoyens novices dans le décryptage de textes techniques. D'autant que les formulations officielles sont elles-mêmes parfois victimes de traductions approximatives du fait de la hâte dans laquelle les textes sont adoptés⁷⁵. À titre exemplatif, citons les aberrations relevées par le professeur Nicolas Thirion.

« Si vous interprétez à la lettre l'article 5 de cet arrêté (*ndla*: sont interdites "les activités à caractère privé ou public, de nature culturelle, sociale, festive, folklorique, sportive et récréative"), il n'est plus permis d'écouter un disque ou de lire un livre dans son salon... Il y a aussi des oublis. Par exemple, le texte interdit les déplacements non essentiels de ou vers la Belgique, mais aucune sanction n'a été prévue pour cette interdiction. Le droit pénal étant de stricte interprétation, en principe, un juge ne pourrait infliger aucune sanction pour cette infraction ».

Plus récemment, les textes déposés en matière de *tracing* manquent également de clarté ou de cohérence dans l'ensemble législatif existant⁷⁶. Il faut également relever les écueils liés à une latitude trop importante laissée aux policiers ou aux fonctionnaires communaux chargés de faire appliquer les règles sur le terrain. L'application des arrêtés et la sanction de leur violation ont donné lieu à de nombreuses situations de confusion et d'incertitude.

L'on peut donc légitimement s'interroger sur le respect de la légalité formelle, par les rédacteurs des propositions de lois ou projets de décrets ou arrêtés royaux. Il serait donc opportun de penser les limitations en termes d'efficacité mais aussi de lisibilité. À force de vouloir mélanger ou cumuler les objectifs, le contenu des textes perd en clarté. À considérer que la « loi » surmonte l'écueil de la clarté, encore faut-il que l'ingérence soit nécessaire pour atteindre l'objectif visé et ne soit pas disproportionnée au regard des intérêts, droits et libertés en jeu.

B. Le principe de proportionnalité des mesures prises

15. La proportionnalité – Rappel et application du principe. Le principe de proportionnalité implique que, pour être acceptable dans une société démocratique, une mesure de limitation d'un droit fondamental, doit être

2020, publié sur: https://droit-public.ulb.ac.be/carnet-de-crise-16-du-20-avril-2020-la-gestion-de-la-pandemie-du-covid-19-et-les-derogations-aux-droits-et-libertes-faut-il-recourir-a-l'article-15-de-la-convention-europeenne-des-droits/#_ftnref12; consulté en dernier lieu le 20 octobre 2020; voy. également en matière de migration: Ch. ALLEN et J. PIOLAT, « Migrations et discriminations: comment penser le déconfinement en contexte de confinements structurels », in Y. MOREAU et O. SERVAIS (dir.), *Déconfinement sociétal. Apport d'expertises académiques*, version 1.1., 17 avril 2020, sur le site https://07323a85-0336-4ddc-87e4-29e3b506f20c.filesusr.com/ugd/860626_731e3350ec1b4fcc4e9a3fae-deca133.pdf; consulté en dernier lieu de 20 octobre 2020.

⁷⁵ Ainsi, on observe souvent à peine deux à sept jours entre la publication officielle des mesures et la date du Conseil national de sécurité qui le précède. Ce délai trop court participe sans doute à la mauvaise qualité des textes; à titre exemplatif: l'arrêté royal du 17 avril 2020 suivra le Conseil national de sécurité du 15 avril 2020.

⁷⁶ Voy. *infra*, n^{os} 37 et s.

nécessaire au regard du but poursuivi par la limitation et des moyens utilisés par l'autorité pour y parvenir. La proportionnalité apparaît comme un « mécanisme de pondération entre des principes juridiques de rang équivalent, simultanément applicables mais antinomiques »⁷⁷.

En l'occurrence, les restrictions sont justifiées par la protection de la santé publique. L'objectif de santé publique constitue évidemment un objectif légitime au regard des exigences du droit constitutionnel mais également du droit international. La protection de la santé publique relève tant d'un intérêt public supérieur, que d'obligations précises à charge des États sur pied de conventions internationales. Ainsi, l'article 35 de la Charte dispose que :

« Toute personne a le droit d'accéder à la prévention en matière de santé et de bénéficier de soins médicaux dans les conditions établies par les législations et pratiques nationales. Un niveau élevé de protection de la santé humaine est assuré dans la définition et la mise en œuvre de toutes les politiques et actions de l'Union ».

En outre, l'article 2 de la CEDH, dont se déduit par « ricochet » le droit à la santé devant la Cour européenne des droits de l'homme, énonce :

« § 1. Le droit de toute personne à la vie est protégé par la loi. La mort ne peut être infligée à quiconque intentionnellement, sauf en exécution d'une sentence capitale prononcée par un tribunal au cas où le délit est puni de cette peine par la loi.

§ 2. La mort n'est pas considérée comme infligée en violation de cet article dans les cas où elle résulterait d'un recours à la force rendu absolument nécessaire :

- a) pour assurer la défense de toute personne contre la violence illégale ;
- b) pour effectuer une arrestation régulière ou pour empêcher l'évasion d'une personne régulièrement détenue ;
- c) pour réprimer, conformément à la loi, une émeute ou une insurrection ».

Pour autant, la simple poursuite de l'objectif de santé publique, aussi légitime qu'il soit, ne peut suffire à justifier les atteintes aux droits fondamentaux. La proportionnalité nécessite *a minima* un double test⁷⁸. Il faut, d'une part, vérifier la nécessité de la mesure, autrement dit vérifier si la mesure permet d'atteindre l'objectif en jeu de manière efficace. Ensuite, il faut s'assurer que la mesure constitue la voie la moins attentatoire aux droits fondamentaux. Cet examen se

⁷⁷ « La police ne doit pas tirer sur les moineaux à coups de canon » disait en 1912 l'auteur allemand Fleiner dans son commentaire de la décision *Kreuzberg* du 14 juin 1882, cité par B. STIRN, *Vers un droit public européen*, 2^e éd., Paris, LGDJ, 2015, p. 93.

⁷⁸ La proportionnalité, dans son volet substantiel, suppose trois conditions : premièrement, l'ingérence doit être appropriée ou de nature à atteindre la finalité recherchée ; deuxièmement, elle doit être nécessaire, à savoir la moins attentatoire aux droits et libertés en concurrence ; et, troisièmement, assurer la proportionnalité au sens strict ; en ce sens, voy. S. VAN DROOGHENBROECK, *La proportionnalité dans le droit de la Convention européenne des droits de l'homme – Prendre l'idée simple au sérieux*, Bruxelles, Bruylant, 2001, pp. 31 à 38 ; « Conservation des données à caractère personnel. Accès par les autorités. Droit au respect de la vie privée. Non-violation », *Obs. Bxl*, 2020/3, n° 121, pp. 61-62.

fait *in concreto*, pour chaque limitation⁷⁹. Ensuite, la question mérite sincèrement d'être posée concernant les mesures adoptées dans le cadre de l'organisation de la justice et des juridictions. Ces mesures semblent ne pas répondre au prescrit du principe de proportionnalité est l'ingérence du pouvoir exécutif à l'égard de l'ordre judiciaire, alors que celui-ci avait déjà pris les mesures que les chefs de corps estimaient nécessaires.

Enfin et pour être complet, si l'on devait ultérieurement confirmer la proportionnalité des mesures au regard du niveau de gravité de la situation, écartant ainsi la possibilité d'une violation des droits fondamentaux⁸⁰, il serait encore possible de considérer les limitations comme admissibles au regard de l'état des connaissances des autorités au moment de la prise de décision.

Il n'en demeure pas moins que durant la première étape de la gestion de la pandémie, à savoir celle du confinement, de nombreuses ingérences à l'ensemble des droits fondamentaux ont été mises en œuvre sous le couvert de « l'état d'urgence sanitaire » par nos gouvernements, profitant du blanc-seing « des pouvoirs spéciaux », qui leur a été remis par les parlements du pays. Ensuite, bousculé par l'impact socio-économique mais également psychosocial de la crise, la seconde phase de la gestion de la pandémie, à savoir celle du déconfinement, repose plus que jamais sur les technologies de l'information et le numérique. Partant, le combat contre la maladie se joue armé d'outils informatiques. Assez logiquement, le combat des droits de l'homme se cristallise autour de la protection de la vie privée et la protection des données à caractère personnel. À ce titre, la deuxième partie de cette contribution s'attarde sur les enjeux plus emblématiques du déconfinement et, particulièrement, les questions posées par l'utilisation des technologies numériques.

⁷⁹ À ce titre, il est à noter que s'agissant du confinement, un expert de l'UCL, Monsieur Vincent Laborderie, suivant une étude comparative entre les Pays-Bas et la Belgique, suggère que les mesures les plus strictes ne sont pas véritablement les plus efficaces, cité par S. ROSENFELD et X. GÉRARD, « Coronavirus en Belgique : une étude de l'UCLouvain recommande la fin d'un confinement strict », RTL info, le 16 avril 2020, www.rtl.be/info/belgique/societe/coronavirus-en-belgique-une-etude-de-l-ucl-recommande-la-fin-du-confinement-1212172.aspx; consulté en dernier lieu le 20 octobre 2020.

⁸⁰ Au regard de la jurisprudence de la Cour européenne des droits de l'homme, la question de savoir ce que l'autorité connaissait ou aurait dû connaître est déterminante pour apprécier les mesures prises. Cour eur. D.H. (Gde Ch.), arrêt *Fernandes de Sousa c. Belgique*, 31 janvier 2019, § 110; Cour eur. D.H. (Gde Ch.), *O'Keeffe c. Belgique*, 28 janvier 2014, § 144.

Section 2

Protection de la vie privée et des données à caractère personnel dans le cadre de la crise sanitaire : un déconfinement « numérique »⁸¹

Cette seconde partie, consacrée au droit à la vie privée et familiale (§ 1) et à la protection de données à caractère personnel (§ 2), se centre sur la phase dite de « déconfinement », dans le processus actuel de la gestion de la crise sanitaire.

§ 1. La protection de la vie privée dans le cadre de la gestion de pandémie, la nécessaire question de l'application du RGPD

16. De la vie privée au RGPD et à sa mise en application à l'heure de la lutte contre le Covid-19. À l'heure où le recours aux techniques de traçage digital s'invite dans notre quotidien, d'importantes questions relatives à la conception du droit au respect de la vie privée émergent. Il est certain que, depuis l'entrée en vigueur du RGPD, la sauvegarde de la vie privée et la protection des données à caractère personnel sont devenues des sujets de premier plan, parfois au même titre que la sauvegarde de la santé. Le phénomène a été accentué par les nombreuses interventions, dans les débats et dès les premiers jours de la crise des autorités de contrôle au travers de toute l'Europe. Les autorités de protection des données de la plupart des pays ont publié des déclarations ou des directives sur le traitement et le partage des données dans le contexte de la pandémie : en Belgique, ce fut le fait de l'Autorité de protection des données (ci-après l'APD)⁸² ; en France, de la Commission nationale de l'informatique et des libertés (ci-après la CNIL)⁸³ ; au niveau européen du Comité européen de protection des données (ci-après le CEPD ou EDPB en anglais)⁸⁴, et du Conseil de l'Europe⁸⁵. Par ailleurs, il est rappelé, que le paragraphe 4 de l'article 36 du RGPD prévoit que « les États membres consultent

⁸¹ La présente section s'inspire pour certaines parties, particulièrement celles relatives au *tracing*, du texte de Y. POULLET, « Pandémie, numérique et droits de l'homme – un étrange cocktail ! », *J.D.E.*, 2020/6, n° 270, pp. 246 à 263.

⁸² APD, avis relatifs au Covid-19, disponible à l'adresse : www.autoriteprotectiondonnees.be/professionnel/themes/covid-19; consulté en dernier lieu le 20 octobre 2020.

⁸³ CNIL, Thématique « Coronavirus (Covid-19) », disponible à l'adresse : www.cnil.fr/fr/coronavirus-covid-19; consulté en dernier lieu le 20 octobre 2020.

⁸⁴ EDPB, « Statement on the processing of personal data in the context of the Covid-19 outbreak », 20 mars 2020, disponible à l'adresse : https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_fr; consulté en dernier lieu le 20 octobre 2020.

⁸⁵ Déclaration de la Présidente du comité consultatif de la Convention n° 108 et du DPO du Conseil de l'Europe, disponible à l'adresse : www.coe.int/fr/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter. Cette déclaration a été complétée par les mêmes personnes, au vu des questions nouvelles soulevées par le déconfinement : www.coe.int/en/web/data-protection/contact-tracing-apps; site consulté en dernier lieu le 20 octobre 2020.

On ajoute que le CEPD a, par ailleurs, augmenté le rythme de ses réunions afin de répondre au mieux et au plus vite aux enjeux de la protection des données dans le cadre de la pandémie.

l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement». Ce que la Belgique ne manqua pas de faire même si on regrette la précipitation avec laquelle notre autorité de protection des données a dû rendre ses avis dans le cadre de «l'extrême urgence sanitaire»⁸⁶. Avis dont on souligne, avec d'autres, la qualité.

17. La vie privée – Un droit relatif. Cela dit, il convient de ne pas «sanctuariser» (c'est-à-dire lui reconnaître un caractère de droit absolu) la protection de la vie privée par le truchement de la protection des données, au risque d'en dénaturer sa portée. Le droit à la protection des données doit se lire à l'aune de la signification du droit à la vie privée, c'est-à-dire le droit des individus à se développer dans une société donnée.

En ce sens, le Tribunal de l'Union européenne a eu l'occasion de rappeler que :

«La protection des données à caractère personnel, consacrée actuellement à l'article 8 de la [Charte des droits fondamentaux de l'Union européenne], joue un rôle fondamental pour l'exercice du droit au respect de la vie privée, consacré actuellement à l'article 7 de ladite Charte. Le respect du caractère confidentiel des informations sur la santé constitue l'un des droits fondamentaux protégés par l'ordre juridique de l'Union (arrêt du 8 avril 1992, *Commission/Allemagne*, C-62/90, EU:C:1992:169, point 23)»⁸⁷.

Et que :

«Toutefois, les droits consacrés aux articles 7 et 8 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération au regard de leur fonction dans la société (arrêt du 17 octobre 2013, *Schwarz*, C-291/12, EU:C:2013:670, point 33)»⁸⁸.

Le droit à la protection des données ne peut être un dogme⁸⁹.

⁸⁶ Ce regret est exprimé par l'APD elle-même, notamment dans son avis n° 36/2020, concernant un avant-projet d'arrêté royal n° XXX 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), du 29 avril 2020, à l'adresse : www.autoriteprotectiondonnees.be/publications/avis-n-36-2020.pdf; consulté en dernier lieu le 20 octobre 2020.

⁸⁷ Trib. UE, 12 septembre 2019, *XI c. Commission européenne*, T-528/18, § 57.

⁸⁸ *Ibid.*, § 58.

⁸⁹ Cf. nos conclusions in Y. POULLET, *La vie privée à l'heure de la société du numérique. Essai*, Collection du CRIDS, n° 45, Bruxelles, Larcier, 2019, n° 140 : « Les législations de protection des données trouvent donc dans le concept de vie privée entendue comme "exigence d'épanouissement personnel" leur fondement, la nécessité de leur interprétation et également la pertinence de leur évolution continue. Le droit quasi constitutionnel à la protection des données n'est qu'un droit dérivé de cette exigence première de nos "États de droit", la vie privée, condition de survie de nos démocraties d'hommes libres. L'enjeu essentiel du droit à la protection de la vie privée est la défense de l'humain, de son développement et de sa dignité comme valeurs absolues et le renvoi des logiques absolues de sécurité et d'efficacité économique à leur dimension toute relative. Le concept de "protection des données" centre le débat sur la donnée au risque de la consacrer comme un bien immatériel dont la personne concernée, chaque individu, serait propriétaire aujourd'hui mais plus demain ».

Dès lors, pour appréhender l'impact de la gestion de la pandémie sur le droit à la vie privée, il y a lieu, dans un premier temps, de considérer les modalités de coexistence du droit à la santé et du droit à la vie privée (A) avant, dans un second temps, d'examiner les obligations découlant du RGPD et applicables à la gestion de la pandémie par nos gouvernements de manière générale (B).

A. La protection de la vie privée et la protection de la santé : une nécessaire opposition ?

18. La vie privée et la Constitution belge. La protection de la vie privée se voit consacrée à l'article 22 de la Constitution belge, en ces termes :

« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi ».

Cet article accorde à la vie privée une protection importante mais pas absolue, comme en témoigne la mention « sauf » qui introduit la seconde partie de la phrase. Par ailleurs, les dispositions de cet article coexistent au sein du catalogue de droits fondamentaux constitutionnels et conventionnels, avec notamment celles de l'article 7 de la Charte et de l'article 8 de la CEDH et les dispositions européennes de la directive en matière de protection des données et désormais du RGPD, formant, sur pied de la jurisprudence de la Cour constitutionnelle, un « ensemble indissociable »⁹⁰. La Cour a énoncé que « lorsqu'une disposition conventionnelle liant la Belgique a une portée analogue à une ou plusieurs des dispositions constitutionnelles précitées, les garanties consacrées par cette disposition conventionnelle constituent un ensemble indissociable avec les garanties inscrites dans les dispositions constitutionnelles en cause »⁹¹.

Dans la droite ligne de cette jurisprudence et en s'appuyant notamment sur les travaux préparatoires de l'article 22 de la Constitution, la Cour a considéré, dans un arrêt du 18 mars 2010, que les obligations internationales en matière de protection des données personnelles découlant des dispositions contenues dans les textes européens, tant de l'Union européenne que du Conseil de l'Europe, « forment un ensemble indissociable des garanties qui sont reproduites à l'article 22 de la Constitution »⁹². Elle a affirmé à plusieurs

⁹⁰ E. DEGRAVE et Y. POULLET, « XVI.F.4. – Le droit au respect de la vie privée face aux nouvelles technologies », in M. VERDUSSEN (dir.), *Les droits constitutionnels en Belgique*, 2 volumes, Bruxelles, Bruylant, 2011, pp. 1001-1035, particulièrement p. 1005.

⁹¹ C.C., n° 136/2004 du 22 juillet 2004, B.5.3. Pour une analyse de cette jurisprudence, voy. *infra*, titre liminaire, n°s 68 et s.

⁹² « Toutefois, la Cour peut examiner si le législateur a respecté les obligations internationales qui découlent des dispositions invoquées de la directive précitée et de la Convention n° 108 précitée auxquelles la loi précitée du 8 décembre 1992 et ses modifications ultérieures donnent exécution. Ces obligations forment un ensemble indissociable des garanties qui sont reproduites à l'article 22 de la Constitution. Une disposition qui est contraire à ces obligations violerait par conséquent le droit au respect de la vie privée, tel qu'il est garanti à l'article 22 de la Constitution » (C.C., arrêt n° 29/2010 du 18 mars 2010, B.5.3., www.const-court.be, consulté en dernier lieu le 20 octobre 2020; il s'agissait d'un recours en annulation de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plateforme eHealth).

reprises⁹³ cette filiation de l'article 22 de la Constitution avec les normes internationales garantissant le droit à la protection de la vie privée et des données à caractère personnel. Il s'ensuit la nécessité de se reporter à l'interprétation du prescrit de l'article 8 de la CEDH, du Protocole n° 108 de la Convention⁹⁴ mais également les articles 7 et 8 de la Charte et du RGPD pour l'application de ce droit.

19. Le droit au respect de la vie privée et le droit à la santé au regard de la CEDH. L'article 8 de la Convention énonce que :

« Droit au respect de la vie privée et familiale

1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

Le premier paragraphe assure la protection de la vie privée et, partant, des données à caractère personnel, le second paragraphe accorde un pouvoir d'ingérence aux États. Cette ingérence doit cependant être « prévue par la loi » et « nécessaire dans une société démocratique » pour atteindre l'un ou l'autre des « buts légitimes » énumérés à l'article 8⁹⁵. On est ici dans le régime ordinaire applicable aux limitations. Parmi les intérêts légitimes énoncés figure la « protection de la santé », de sorte que certaines atteintes à la vie privée peuvent donc être justifiées si la protection de la santé, que ce soit celle d'un individu ou celle de la collectivité, le requiert⁹⁶. Nous rappelons que, depuis de longues années, le droit à la santé bénéficie de la qualité de droit de l'homme dans de nombreux textes relevant d'ordres juridiques différents et ayant des objets distincts.

Cette reconnaissance apparaît dans les instruments de protection des droits de l'homme tels que l'article 12, § 1, du PIDESC de 1966⁹⁷, l'article 24, § 1, de la Convention sur les droits de l'enfant du 20 novembre 1989, l'article 25, § 1, de la DUDH, l'article 35 de la Charte. Par ailleurs, en 1946, l'Organisation mon-

⁹³ La Cour s'appuie notamment sur les travaux préparatoires de l'article 22 de la Constitution. Voy. C.C., arrêt n° 166/2011 du 10 novembre 2011, www.const-court.be, B.16.6. et également C.C., arrêt 122/2011 du 7 juillet 2011, www.const-court.be, B.3.

⁹⁴ Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE 108, 28 janvier 1981 (ci-après la Convention n° 108).

⁹⁵ Cour eur. D.H. (Gde Ch.), arrêt *Dubská et Krejzová c. République tchèque*, 15 novembre 2016, requêtes n°s 28859/11 et 28473/12, n° 166.

⁹⁶ C. DE TERWANGNE, J. VAN GYSEGHEM et Y. POULLET, « La Covid-19: la mise en perspective des droits à la vie privée et à la santé », *R.D.T.I.*, 2019/3-4, n°s 76-77, pp. 5-8.

⁹⁷ Art. 12, § 1, du PIDESC reconnaissant le « droit de toute personne de jouir du meilleur état de santé physique et mentale qu'elle soit capable d'atteindre ».

diale de la santé, l'OMS, acteur de premier rang dans la gestion de la crise⁹⁸, est créée en vue « d'amener tous les peuples au niveau de santé le plus élevé possible »⁹⁹. Les ambitions affichées des États membres ou partis ne sont donc pas des moindres en matière de santé.

20. Le droit à un environnement sain au cœur de l'interprétation de l'article 8 – Et si le droit à la santé était partie intégrante de la vie privée? Devant la Cour européenne des droits de l'homme, le droit au « bien-être » n'est pas repris dans le texte de la Convention mais est assuré par « ricochet ». La protection du droit au « bien-être », ou à la « santé », morale et physique, découle de l'interprétation évolutive et dynamique¹⁰⁰ donnée au concept du droit à la vie privée, dans la jurisprudence innovante et créative de la Cour strasbourgeoise¹⁰¹. La Cour l'a elle-même répété dans de nombreux arrêts : « les traités relatifs aux droits de l'homme sont des instruments vivants, dont l'interprétation doit être conforme à l'évolution dans le temps et, particulièrement, aux conditions de vie actuelles »¹⁰². L'article 32 de la CEDH reconnaît en effet ce droit à une interprétation large des prescrits de la **Convention** :

⁹⁸ À cet égard, se référer au message de l'OMS : « Covid 19 = Chronologie de l'action de l'OMS », disponible à l'adresse : www.who.int/fr/news/item/27-04-2020-who-timeline---covid-19 ; consulté en dernier lieu, le 24 octobre 2020.

⁹⁹ Art. 1^{er} de la Constitution de l'Organisation Mondiale de la Santé, Conférence internationale de la santé, New York, 22 juillet 1946.

¹⁰⁰ Cour eur. D.H., arrêt *Wemhoff c. Allemagne*, 27 juin 1968, p. 23, § 8, série A, n° 7. Dans l'un de ses premiers arrêts, la Cour a clairement écarté la thèse selon laquelle la Convention devait être interprétée de manière « restrictive » : « [s']'agissant d'un traité normatif, il y a lieu [...] de rechercher quelle est l'interprétation la plus propre à atteindre le but et à réaliser l'objet [du] traité et non celle qui donnerait l'étendue la plus limitée aux engagements des Parties ».

¹⁰¹ Sur cette « interprétation dynamique et évolutive », lire Fr. SUDRE, « Rapport introductif », in *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruxelles, Bruylant, 2005, p. 27 et les références y reprises à la doctrine mais également à la jurisprudence de la Cour européenne des droits de l'homme elle-même, notamment aux attendus de l'arrêt *Goodwin*. On connaît par ailleurs le célèbre attendu rendu par la Cour de Strasbourg dans l'affaire *Pretty* : « Comme la Cour a déjà eu l'occasion de l'observer, la notion de "vie privée" est une notion large, non susceptible d'une définition exhaustive. Elle recouvre l'intégrité physique de la personne [...]. Elle peut parfois englober des aspects de l'identité physique et sociale d'un individu [...]. Des éléments tels, par exemple, l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle relèvent de la sphère personnelle protégée par l'article 8 [...]. Cette disposition protège également le droit au développement personnel et le droit d'établir et d'entretenir des rapports avec d'autres êtres humains et le monde extérieur [...]. Bien qu'il n'ait été établi dans aucune affaire antérieure que l'article 8 de la Convention comporte un droit à l'autodétermination en tant que tel, la Cour considère que la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8 ».

¹⁰² Cour eur. D.H., arrêts *Tyrer c. Royaume-Uni*, 25 avril 1978, § 31, série A, n° 26 ; *Loizidou c. Turquie* (exceptions préliminaires), 23 mars 1995, § 71, série A, n° 310 ; (Gde Ch.) *Christine Goodwin c. Royaume-Uni*, n° 28957/95, § 75, 2002, VI ; *Öcalan c. Turquie*, 12 mars 2003, n° 46221/99, § 193 ; (Gde Ch.) *E.B. c. France*, 22 janvier 2008, n° 43546/02, § 92 ; (Gde Ch.) *Saadi c. Royaume-Uni*, 29 janvier 2008, n° 13229/03, § 62. Cette expression a été utilisée dans une trentaine d'affaires. Voy. L. WILDHABER, « The European Court of Human Rights in action », *Ritsumeikan Law Review*, 2004, vol. 21, p. 83 ; voy. aussi S. C. PREBENSEN, « Evolutionary interpretation of the European Convention on Human Rights », in P. MAHONEY et al. (éd.), *Protecting Human Rights: The European Perspective. Studies in memory of Rolv Ryssdal*, Cologne, Carl Heymanns Verlag KG, 2000, pp. 1123-1137.

- « 1. La compétence de la Cour s'étend à toutes les questions concernant l'interprétation et l'application de la Convention et de ses protocoles qui lui seront soumises dans les conditions prévues par les articles 33, 34, 46 et 47.
2. En cas de contestation sur le point de savoir si la Cour est compétente, la Cour décide ».

En effet, si la Cour déduit le droit à la santé du prescrit notamment de l'article 2 de la Convention, à savoir le droit à la vie, elle fonde également ce droit sur la base de l'article 8, le droit au respect de la vie privée et familiale. Aussi étonnant que cela puisse paraître, c'est, sans nul doute, l'article 8 de la Convention¹⁰³ qui est le plus mobilisé. L'élasticité ou, autrement dit, l'interprétation jurisprudentielle, innovante, créative et quasi sans limite de ce droit¹⁰⁴ lui procure en effet un avantage certain sur le droit à la vie.

Ainsi, partant du constat que la réalisation des libertés fondamentales passe par leur nécessaire effectivité, la Cour de Strasbourg admet de manière constante qu'il est rendu plus difficile lorsque la santé physique ou mentale est en danger, de garantir le respect des dispositions de l'article 8 ou de manière plus positive que le droit au développement de l'individu, objet de la reconnaissance du droit à la vie privée, exige un contexte environnemental qui le permette. C'est à l'aune de ce raisonnement que la Cour garantit la reconnaissance du « droit à un environnement sain » depuis plus de vingt ans¹⁰⁵. Il s'ensuit que, se fondant sur le droit au respect de la vie privée, familiale et du domicile, les juges strasbourgeois ont admis le lien entre des atteintes graves au bien-être et à la qualité de vie et à la santé des personnes¹⁰⁶ comme portant atteinte au droit à la vie privée.

Il est donc fondé de dire que la réalisation du droit à la vie privée non seulement est limitée par le droit à la santé (le droit de chaque personne de recevoir des soins appropriés) mais, au-delà, passe assurément par la réalisation du droit

¹⁰³ Voy. en ce sens trois récents arrêts, au fort retentissement : Cour eur. D.H., arrêt *Vilnes et crts c. Norvège*, 5 décembre 2013 ; Cour eur. D.H., arrêt *Howald Moor c. Suisse*, 11 mars 2014 ; Cour eur. D.H., *Di Sarno c. Belgique*, 10 janvier 2012, cités in J.-P. MARGUENAUD, « L'influence générale du droit du Conseil de l'Europe sur la protection de la santé », in *Droit européen et protection de la santé*, Bruxelles, Bruylant, 2015, p. 139.

¹⁰⁴ Sur cette interprétation foisonnante du droit à la vie privée, lire Y. POULLET, *La vie privée à l'heure de la société du numérique. Essai, op. cit.*, en particulier p. 50 et les nombreuses références y citées ; A. ROUVROY et Y. POULLET, « The right to informational Selfdetermination and the value of Self-development : Reassessing the importance of Privacy for Democracy », in *Reinventing Data Protection ?*, Dordrecht, Springer, 2009, pp. 159 et s.

¹⁰⁵ Conseil de l'Europe, *Manuel sur les droits de l'homme et l'environnement. Principes tirés de la jurisprudence de la Cour européenne des droits de l'homme*, Strasbourg, Éd. Conseil de l'Europe, 2006, disponible à l'adresse : www.echr.coe.int/LibraryDocs/DG2/ISBN/COE-2006-FR-9789287159793.pdf ; consulté en dernier lieu le 20 octobre 2020.

¹⁰⁶ Cour eur. D.H., arrêt *Lopez-Ostra c. Belgique*, 9 décembre 1994, § 51 ; Cour eur. D.H., arrêt *Tatar c. Roumanie*, 27 janvier 2009, § 122 ; Cour eur. D.H., arrêt *Bacila c. Roumanie*, 30 mars 2010, §§ 70-71 ; Cour eur. D.H., arrêt *Hristozov et autres c. Bulgarie*, 13 novembre 2012, Cour eur. D.H., arrêt *Vo c. Belgique*, 8 juillet 2004 ; Cour eur. D.H., arrêt *Tysiac c. Pologne*, 20 mars 2007.

à un environnement qui garantisse la santé tant physique que mentale des citoyens. Ce point est à souligner au moment d'évaluer l'ingérence du droit à la santé dans la vie privée, et ce, notamment à l'occasion des mesures visant à mettre en œuvre un logiciel de *tracing* ou l'installation de caméras thermiques, par exemple.

Cela ne signifie pas pour autant que la porte serait ouverte, au nom de la nécessité de protéger la santé, à tout type de traitement de données à caractère personnel, que ce soit par exemple via des applications sauvages de *tracking* non entourées de dispositions légales, ou la reconnaissance faciale des personnes lors de la prise de température par caméra thermique ou encore, comme au Monténégro, par la diffusion sur Internet des noms et adresses des personnes contaminées¹⁰⁷. En toutes circonstances, ces ingérences devront à tout le moins respecter les prescrits des dispositions du Règlement relatif à la protection des données.

B. Le RGPD, un cadre réglementaire nécessaire à garantir la vie privée ?

21. Les moyens mis en place pour lutter contre le Covid-19. Dans le cadre de la gestion de la pandémie, certains États, dont la Belgique¹⁰⁸, ont utilisé des instruments d'observation des pratiques collectives de mobilité et de confinement, tels que la cartographie des déplacements de populations¹⁰⁹, l'identification des sujets « contact » de type *contact tracing*, ou enfin, les contrôles d'accès des espaces publics ou privés (lieux de travail, commerces, administrations, etc.), afin de veiller au respect des mesures visant à endiguer la pandémie. À titre exemplatif, des nouveaux dispositifs de surveillance¹¹⁰, tels que les caméras

¹⁰⁷ « Coronavirus : le Monténégro balance les noms et adresses des personnes "suspectées" d'être malades », *Le Vif*, 7 avril 2020, disponible à l'adresse : www.levif.be/actualite/europe/coronavirus-le-montenegro-balance-les-noms-et-adresses-des-personnes-suspectees-d-etre-malades/article-normal-1274153.html; consulté en dernier lieu le 20 octobre 2020.

¹⁰⁸ La Belgique a, dès les premières heures de la crise, en collaboration des opérateurs de téléphonie, établi un groupe de travail : « data against Coronavirus taskforce ».

Le système proposé par les opérateurs consiste en un bornage téléphonique, qui renvoie des données agrégées et anonymes issues des appareils mobiles sans besoin d'activation par les utilisateurs. D'autres pays ont également contraint des plateformes comme Google à mettre à disposition de manière agrégée et anonyme les données GPS générées par les applications mobiles ou, à partir des données d'utilisation des cartes bancaires, en vue de suivre les déplacements des personnes. www.proximus.be/fr/id_b_cl_data_against_corona_taskforce/entreprises-et-secteur-public/blog/news-blog/innovation/data-against-corona-taskforce.html; consulté en dernier lieu le 20 octobre 2020.

¹⁰⁹ Ces systèmes nécessitant un maillage dense de caméras, de capteurs GPS, couplés à des algorithmes performants, ou une force de travail humaine considérable pour l'analyse des données, pouvant être associée à des technologies de reconnaissance faciale, « il s'agit, à partir de données agrégées fournies par les opérateurs, les systèmes de cartes bancaires ou des applications GPS d'informer les autorités, voire la population en temps réel de la propagation du virus, de détecter les migrations anormales et les lieux de rassemblement fréquentés ou de mesurer l'efficacité des politiques suivies », in Y. POULLET, « Pandémie, numérique et droits de l'homme – un étrange cocktail! », *op. cit.*, p. 248.

¹¹⁰ Pour une analyse des différents instruments utilisés par les États, voy. U. GASSER, M. IENCA, J. SCHEIBNER, J. STEIGH et E. VAYENA, « Digital tools against Covid-19 : Framing the ethical challenges and how to address

vidéo dites « intelligentes » avec ou sans prise de température, sont déployés dans des lieux publics ou dans des lieux fermés accessibles au public, tels que les aéroports, les administrations communales ou encore les salles de sport. L'objectif de veille de la santé publique assigné à ces instruments est légitime à condition que les moyens mis à disposition de cet objectif légitime respectent les lois en vigueur et notamment celles relatives à la vidéosurveillance¹¹¹ et soient proportionnés. À cet égard, l'existant actuel en termes de contrôle des lieux publics semble déjà suffisant et la lutte contre la pandémie ne nous paraît pas justifier des installations supplémentaires.

Cependant, le développement incontrôlé de ces mesures présente le risque de généraliser un sentiment de surveillance chez les citoyens et de créer un phénomène d'accoutumance et de banalisation de technologies intrusives, voire d'engendrer une surveillance accrue, susceptible de porter atteinte au bon fonctionnement de notre société démocratique¹¹². D'autant que l'espace public est un lieu où s'exercent de nombreuses libertés individuelles : droit à la vie privée et à la protection des données personnelles, liberté d'aller et venir, d'expression et de réunion, droit de manifester, liberté de conscience et d'exercice des cultes, etc.

La préservation de l'anonymat ou en tout cas d'un certain « anonymat » dans l'espace public est une dimension essentielle pour l'exercice de ces libertés et la captation de données à caractère personnel dans ces espaces est incontestablement porteuse de risques pour les droits fondamentaux. Ce traitement ne peut avoir lieu hors du cadre précis du respect des dispositions du RGPD. En effet, toute organisation, publique ou privée, qu'elle agisse en qualité de responsable du traitement ou du sous-traitant, doit respecter l'ensemble des principes généraux et des obligations qui découlent du Règlement, y compris bien évidemment si le traitement est effectué dans le cadre des mesures visant à limiter la propagation d'un virus tel que le coronavirus.

1. *Les principes généraux applicables aux traitements des données dans le cadre de la pandémie*

22. RGPD – Ses principes généraux. Les principes généraux applicables aux traitements des données à caractère personnel sont énoncés notamment

them », disponible à l'adresse : <https://arxiv.org/ftp/arxiv/papers/2004/2004.10236.pdf>; consulté en dernier lieu le 20 octobre 2020.

¹¹¹ Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance version coordonnée (modifiée par les lois des 12 novembre 2009, 3 août 2012, 4 avril 2014, 21 avril 2016, 21 mars 2018 et 30 juillet 2018), disponible à l'adresse : www.besafe.be/sites/default/files/2018-09/loi_cameras-_version_cooronnee-08-2018.pdf; consulté en dernier lieu le 20 octobre 2020.

¹¹² Aujourd'hui, la pérennisation des instruments mis en place n'est pas à exclure, en ce sens : U. GASSER, M. IENCA, J. SCHEIBNER, J. STEIGH et E. VAYENA, « Digital tools against Covid-19: Framing the ethical challenges and how to address them », *op. cit.*

aux articles 5 à 11 du Règlement. Même dans le cadre de la prise de mesures sanitaires préventives, ces dispositions doivent être appliquées à l'occasion de chaque traitement de données à caractère personnel. Ainsi, l'article 5 du RGPD énonce ce qui suit :

« Les données à caractère personnel doivent être :

- a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;
- b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;
- c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
- d) exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;
- e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;
- f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ».

2. *Principes de finalité, de licéité, de loyauté et de transparence*

23. Les premiers principes – Les bases de licéité des traitements anti-Covid-19. Parmi ces principes, l'article 5, a) et b), du RGPD retient les principes de transparence, de loyauté, de licéité et de finalité du traitement. Il s'ensuit que chaque traitement doit impérativement avoir une finalité qui doit être déterminée, explicite et légitime. Ensuite, ces finalités doivent être communiquées de manière claire et précise¹¹³, assurant ainsi le principe de transparence et de loyauté des traitements. Enfin, les traitements doivent être

¹¹³ Art. 13 et 14 du RGPD.

licites, à savoir reposer sur une des *bases de légitimité* mentionnées à l'article 6, § 1, du RGPD, pour être légaux¹¹⁴. À cet égard, l'article 6 liste les bases suivantes :

« Le traitement n'est licite *que si*, et dans la mesure où, *au moins une* des conditions suivantes est remplie :

- a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ».

La base de licéité utilisée par les autorités publiques est la nécessité du traitement en vue de « l'exécution d'une mission d'intérêt public » ou relevant « de l'exercice de l'autorité publique » dont ils sont investis en qualité de responsable du traitement¹¹⁵. La mission d'intérêt public est généralement reconnue par une loi ou une autre règle de droit¹¹⁶. « Le principe de légalité qui gouverne l'administration impose effectivement que les missions confiées aux entités du secteur public aient une base légale »¹¹⁷.

¹¹⁴ En ce sens, la délibération, en formation restreinte de la CNIL n° SAN-2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société Google LLC, disponible à l'adresse : www.legi-france.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastR eqId=2103387945 &fastPos=1 ; consulté en dernier lieu le 20 octobre 2020.

¹¹⁵ *Ibid.* ; art. 6, § 1, e), du RGPD.

¹¹⁶ Groupe de travail « Article 29 » sur la protection des données, *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, disponible à l'adresse : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf, p. 24.

¹¹⁷ Le considérant 47 du RGPD énonce, s'agissant de l'utilisation de l'intérêt légitime par les autorités publiques, ce qui suit : « Étant donné qu'il appartient au législateur de prévoir par la loi la base juridique pour le traitement des données à caractère personnel par les autorités publiques, cette base juridique (l'intérêt légitime) ne devrait pas s'appliquer aux traitements effectués par des autorités publiques dans l'accomplissement de leurs missions » ; en ce sens C. DE TERWANGNE, « Chapitre 2. – Hypothèses de licéité des traitements », in C. DE TERWANGNE et K. ROSIER (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, coll. Cahiers du CRIDS, n° 44, Bruxelles, Larcier, 2018, p. 134.

En outre, lorsque le traitement de données porte sur des catégories particulières de données¹¹⁸, telles que les données relatives à l'état de santé des personnes¹¹⁹, ce qui est bien évidemment le cas dans les hypothèses qui nous occupent les responsables de traitement doivent non seulement déterminer une base de licéité sur pied de l'article 6 du Règlement, mais ils doivent également remplir une des conditions spécifiques imposées en son article 9, qui encadrent les traitements de catégories particulières de données¹²⁰:

- « b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, [...] ;
- c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, [...] ;
- d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif [...] ;
- e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée [...] ;
- f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice [...] ;
- g) *le traitement est nécessaire pour des motifs d'intérêt public important*, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi [...] ;
- h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire [...] ;
- i) *le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique*, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux [...] ;

¹¹⁸ Sur pied des articles 9 et 10 du RGPD, les données sensibles ou particulières s'entendent « des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique » et des données « relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes [...] ».

¹¹⁹ Attention, alors que la directive semblait se référer à une définition des données par leur nature, le RGPD adopte un autre point de vue lorsqu'il dispose qu'est interdit « [l]e traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale [...] » (art. 9). C'est donc au sein du traitement et au vu de sa finalité que la donnée devient sensible.

¹²⁰ J.-M. VAN GYSEGHEM, « Titre 5 – Les catégories particulières de données à caractère personnel », in C. DE TERWANGNE et K. ROSIER (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, coll. Cahiers du CRIDS, n° 44, Bruxelles, Larcier, 2018, pp. 255 à 284.

- j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1 [...] »¹²¹.

Cumulant les articles 6 et 9, la CNIL conclut que : « Le traitement de données sensibles ne peut intervenir que si les deux conditions cumulatives suivantes sont remplies :

- le traitement est valablement fondé sur une des bases légales prévues à l'article 6 du règlement ;
- une des exceptions mentionnées à l'article 9 du règlement est applicable au traitement concerné »¹²².

Il s'ensuit que dans le cadre de la gestion de la pandémie, les traitements initiés par nos gouvernements, mais également par d'autres niveaux de pouvoir, trouvent leur base de licéité à l'article 6, paragraphe 1, point e), lu conjointement avec l'article 9, paragraphe 2, point i), du RGPD. En effet, ces traitements sont rendus nécessaires pour l'exécution de la mission d'intérêt public incombant à ces derniers et visant à assurer la salubrité et la sécurité sanitaire et à enrayer l'épidémie de coronavirus. En outre, ils peuvent également utiliser les données de santé, dès lors que le traitement de ces données est rendu nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux. Dans la mesure où les données collectées peuvent être qualifiées de données de santé, leur traitement – qu'il s'agisse de *tracing* automatique ou manuel, révélant (ou étant censé révéler) le fait soit qu'une personne a contracté (ou pense avoir contracté) le virus, soit est une personne à risque, ayant été au contact d'une personne qui a contracté le virus – doit être placé, selon l'article 9, sous la surveillance d'un professionnel de la santé. Ce point est important car peu importe que le système d'alerte mis en place soit automatique (envoi direct d'un message sur le mobile de la personne à risque) ou manuel (prise de contact par un humain avec cette dernière), il importera que ce système et ceux qui y œuvrent opèrent sous le contrôle d'une équipe de médecins ou, au sein des entreprises, sous la surveillance des médecins-conseils.

3. *Principe de minimisation*

24. La signification du principe. Le principe de minimisation et de proportionnalité consacré par l'article 5, 1., c), consiste, d'une part, à s'interroger sur la nécessité de traiter des données à caractère personnel pour atteindre les

¹²¹ Nous soulignons.

¹²² CNIL, « La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD », 2 décembre 2020, disponible à l'adresse : www.cnil.fr/fr/la-liceite-du-traitement-l-essentiel-sur-les-bases-legales-prevues-par-le-rgpd ; consulté en dernier lieu le 20 octobre 2020.

finalités recherchées par le traitement et, d'autre part, à limiter le traitement des données au minimum, en ce qui concerne¹²³ :

- les catégories de données traitées ;
- les données traitées ;
- le volume ou la quantité de données traitées.

Il s'ensuit que seule la quantité minimale nécessaire de données peut être traitée en vue d'atteindre la finalité recherchée, et ce, pour une durée minimale, à savoir en l'occurrence limitée à l'état d'urgence¹²⁴. À la « minimisation », on ajoutera le principe de sécurité, affirmé outre par l'article 5, par l'article 32 du RGPD : les mesures de sécurité nécessaires et adéquates doivent également être prises en vue de protéger les données à caractère personnel¹²⁵, particulièrement quand il s'agit de données sensibles telles que les données de santé.

25. Les principes et valeurs éthiques à prendre en compte. On comprend ainsi que le Règlement n'a pas vocation à faire cesser tous les traitements de données à caractère personnel, mais bien à les encadrer de sorte que ces derniers puissent continuer à être réalisés en assurant une garantie suffisante des droits fondamentaux protégés par la Charte et notamment le droit à la vie privée. Il s'ensuit que la mise en œuvre des principes, mais également des obligations, énoncés dans le Règlement assurera une atteinte limitée et légitime aux droits fondamentaux. À titre exemplatif, les traitements relatifs à la prise de température par caméra thermique doivent bénéficier d'une base de licéité énoncée à l'article 6 et remplir une des conditions de l'article 9 ; ils doivent en outre respecter les principes de minimisation, de rétention limitée, de sécurité adéquate et de communication transparente et loyale¹²⁶. Il en va de même pour l'utilisation par les universités d'instruments de contrôle à l'occasion de l'organisation des examens à distance des étudiants de l'enseignement supérieur.

En toute hypothèse, le mot d'ordre qui justifie le choix d'une solution plutôt qu'une autre doit se fonder sur l'analyse des risques attachés à chaque utilisation du point de vue des libertés individuelles. Sans doute est-on tenté d'y

¹²³ Y. POULLET, « Chapitre 1 – Analyse critique du RGPD », in *La vie privée à l'heure de la société du numérique*, Bruxelles, Larcier, 2019, pp. 97 à 168 ; en ce sens, la décision de l'APD : Gegevensbeschermingsautoriteit (GBA), Geschillenkamer, « Betreft: Klacht wegens gebruik van de elektronische identiteitskaart voor de aanmaak van een klantenkaart », *Beslissing ten gronde 06/2019 van 17 september 2019*, disponible à l'adresse : www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/BETG06-2019_web.pdf#overlay-context=nieuws/de-gegevensbeschermingsautoriteit-berispt-de-fod-volksgezondheid.

¹²⁴ Art. 5, § 1, d), du RGPD.

¹²⁵ Art. 32 du RGPD.

¹²⁶ En ce sens, l'APD énonce sur son site internet que : « L'APD constate que dans le cadre de la reprise de la vie sociale et économique, les responsables du traitement cherchent des solutions technologiques en vue de détecter à l'entrée de leurs bâtiments les individus qui présentent de la fièvre afin d'éviter qu'ils n'y pénètrent, et ce dans le but de prévenir d'autres contaminations au sein des bâtiments. Ils considèrent que la mise en place d'une telle politique d'accès fait partie de leur mission (à savoir protéger la sécurité et la santé des personnes concernées) » (www.autoriteprotectiondonnees.be/professionnel/themes/covid-19/prise-de-temperature ; consulté en dernier lieu le 20 septembre 2020).

ajouter le besoin de prendre en compte d'autres valeurs éthiques que celle de l'autonomie, telles celles, premièrement, de la justice sociale qui nous obligent à veiller à ce que les mesures prises n'excluent personne et, en second lieu, de la dignité des personnes¹²⁷, qui bannit la surveillance de tous les instants des personnes concernées et leur manipulation. Trois valeurs éthiques : autonomie, justice sociale et dignité que la Charte européenne des droits fondamentaux et la Convention européenne des droits de l'homme obligent à prendre en compte¹²⁸.

§ 2. Du **tracing** manuel au **tracing** automatique, quelle solution pour un déconfinement pérenne ?

26. Introduction et plan du paragraphe. Sur fond d'amorce de crise économique sans précédent, à l'heure où la recrudescence de l'épidémie bat son plein, le « numérique » est promu comme la solution pour une sortie pérenne du confinement¹²⁹. À l'instar de ce qui se fait dans l'ensemble des pays européens¹³⁰, la Belgique¹³¹ a rapidement mis en place, avec l'appui des opérateurs de mobilophonie, un système d'observation des pratiques collectives des mouvements de populations¹³². Ensuite et eu égard à l'ampleur de la pandémie, très vite, le besoin de procéder à un traçage (*tracing* en anglais) s'est fait sentir (A). La mise en œuvre de ce système de suivi a évidemment soulevé des questions en matière de protection des données à caractère personnel et de protection de la vie privée (B).

¹²⁷ Dans le même sens, l'article d'U. GASSER *et al.*, « Digital tools against Covid-19: Framing the ethical challenges and how to address them », *op. cit.*

¹²⁸ Sur la signification de ces trois valeurs éthiques dans la société numérique, nous renvoyons à l'ouvrage : Éthique et droits de l'homme dans la société du numérique, Mémoire de l'Académie royale de Belgique, 2020.

¹²⁹ Des mesures alternatives de suivi numérique des individus (bracelets, caméras) et de technologies de surveillance des mouvements de population étaient, elles, actives dans une trentaine de pays. 28 % des applications proposées à cette date ne disposaient pas de politique déclarée de respect de la *privacy*. Environ les deux tiers recourent à la technologie GPS pour suivre les déplacements des personnes, alors qu'un tiers privilégie la technologie Bluetooth. Ces développements sont tantôt le résultat d'initiatives privées, tantôt le fait d'organismes indépendants sans but lucratif, ou d'initiatives soutenues activement par les pouvoirs publics. Au total, c'est donc aujourd'hui dans bien plus d'une cinquantaine de pays que sont développées, selon des modalités très différentes, des techniques de gestion et de contrôle de la crise sanitaire par le moyen de l'outil numérique.

¹³⁰ La Belgique, la République tchèque, la Pologne et la Slovaquie ont développé des applications de *tracing* automatique. La Belgique, les Pays-Bas, le Belgique et l'Belgique travaillent sur des applications de traçage mobile. La Pologne a introduit un système d'application mobile avec géolocalisation et reconnaissance faciale pour surveiller les obligations de confinement. La Bulgarie, la République tchèque, la Pologne et la Belgique disposent de lois obligeant les opérateurs de communication à partager leurs données avec les autorités publiques aux fins de surveillance des déplacements et des lieux de rassemblement. Ce partage se fait sur une base agréée et anonyme. D'autres pays ont annoncé que ce partage a été opéré de manière volontaire.

¹³¹ Sur la discussion en Belgique, voy. Fr. BOUHON, A. JOUSTEN, X. MINY et E. SLAUTSKY, « L'État belge face à la pandémie de Covid-19: esquisse d'un régime d'exception », *Courrier hebdomadaire du CRISP*, 2020/1, n° 2446.

¹³² Il s'agit de travailler avec des données agrégées permettant de détecter des mobilités ou des rassemblements dangereux ou l'évolution de la pandémie.

A. *La petite histoire du tracing belge*

27. Une histoire en trois temps. La volonté de «déconfiner» de manière durable en ligne de mire, nos gouvernements ont mis en place un système de *tracing*¹³³, manuel puis automatique (1), et ce, dans le respect des dispositions propres à la protection des données à caractère personnel (2).

1. *Tracking ou tracing manuel et automatique, quelle voie pour garantir la protection de la vie privée ?*

28. «Tracking» ou «tracing». À côté des règles de distanciation sociale et d'hygiène, du *testing*, le dispositif de «*tracing*», en anglais, ou de suivi ou traçage des contacts, en français, apparaît partout dans le monde comme la solution nécessaire à la sortie du confinement, voire à l'éradication du virus. Le *tracing* ne doit pas être confondu avec le *tracking*¹³⁴ qui est l'aptitude à retrouver l'historique, l'utilisation ou la localisation d'une entité au moyen d'identifications enregistrées. Ainsi, les applications de suivi géographique ou d'identification automatique des contacts entre personnes («*tracking*»), d'une part, et les applications de suivi des contacts («*contact tracing*»), d'autre part, ne couvrent pas les mêmes fonctionnalités. Le *tracking*, utilisant soit les données GPS du téléphone, soit les données de la cellule radio, se montre plus attentatoire à la vie privée et la protection des données qui ne doivent pas être sacrifiées dans la lutte contre le coronavirus, sauf à démontrer son caractère strictement nécessaire.

A contrario, le *tracing* des contacts consiste à pointer les personnes ayant été en contact avec un cas confirmé de Covid-19, en vue de les isoler préventivement si elles encourent elles-mêmes un risque élevé de contamination par le virus. Cette technique ambitionne ouvertement d'éviter un second confinement en le remplaçant par une procédure débouchant sur un isolement ciblé des individus à risque, évitant ainsi une résurgence du virus¹³⁵. Ce système de suivi des

¹³³ Les autorités belges, au cœur de l'accord de coopération, justifient l'instauration du traçage dans l'analyse d'impact du traitement des données (DPIA) de l'application *tracing* comme suit : «L'assouplissement des mesures, permettant à nouveau davantage de contacts physiques entre les personnes, entraîne évidemment un risque de voir augmenter à nouveau le nombre de cas de Covid-19. Témoin le début d'une deuxième vague en juillet 2020. Il est donc nécessaire que chaque nouvelle phase d'assouplissement s'accompagne des mesures nécessaires permettant d'éviter une nouvelle propagation du virus. L'une de ces mesures concerne le traçage précoce des personnes ayant été infectées ou pour lesquelles il existe une probabilité qu'elles l'aient été, afin de pouvoir leur donner les recommandations nécessaires (quarantaine, télétravail, etc.) pour éviter qu'elles ne contaminent d'autres personnes avec le virus SARS-CoV-2» (*Application de traçage des contacts – Belgique. Analyse d'impact relative à la protection des données (AIPD)*, 15 septembre 2020, disponible à l'adresse : https://coronalert.be/wp-content/uploads/2020/09/20200915-DPIA_contactopsporingsapplicatie-Belgie-V.5_final_FR.pdf; consulté en dernier lieu le 20 octobre 2020).

¹³⁴ Cette définition est celle de référentiel normatif ISO 8402/1994, relatif au management de la qualité et assurance de la qualité; si l'idée de traçabilité des individus n'est pas familière en droit, on se référera toutefois à la définition de la traçabilité donnée par la norme internationale : ISO 8402.

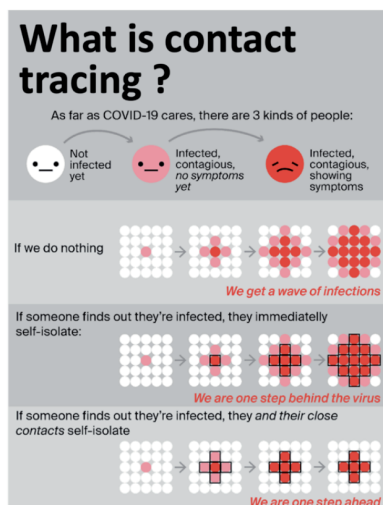
¹³⁵ Sciensano, «Suivi des contacts Covid-19, questions fréquemment posées», 2020, disponible à l'adresse : https://gcm.rmnet.be/clients/rmnet/content/medias/2_juin_2020_faq_sciensano_testing_tracing_1_.pdf; consulté en dernier lieu le 20 octobre 2020.

contacts est une méthode épidémiologique médicale utilisée depuis déjà des décennies pour lutter contre les épidémies virales. L'objectif est de suivre rapidement les chaînes d'infections et de les interrompre au plus tôt. Ce *tracing* s'organise de manière manuelle ou automatisée.

a. Le **tracing manuel**

29. Le *tracing* manuel – Schéma de fonctionnement et limites. Le *tracing* manuel repose sur la communication par des professionnels de santé des données relatives aux personnes atteintes du virus à des bases de données plus ou moins centralisées, enrichies ou non d'autres données, et permettant la prise de contact avec les personnes inscrites et de retracer leurs « contacts », avec lesquels les agents de la banque de données prendront langue dans un second temps pour les prévenir du risque particulier encouru, voire leur enjoindre le respect des obligations de confinement.

*Schéma du **tracing** par l'épidémiologiste Marcel Salathé¹³⁶*



Le *tracing* manuel sera en Belgique organisé par les trois entités fédérées¹³⁷ qui collaborent au sein d'un groupe de travail dénommé le Comité interfédéral sur le même modèle¹³⁸ afin de garantir une vue globale et permanente de la situa-

¹³⁶ Cité par B. PRENEEL, « Contact tracing apps: balancing public health and personal privacy »; présentation du 30 juin 2020, disponible à l'adresse : www.cybersecuritycoalition.be/content/uploads/preneel_proximity-tracing_june30_2020v1.pdf; consulté en dernier lieu le 20 octobre 2020.

¹³⁷ Arrêté du gouvernement wallon de pouvoirs spéciaux n° 35 du 5 mai 2020, organisant le *tracing* socio-sanitaire dans le cadre de la lutte contre l'épidémie Covid-19, M.B., 7 mai 2020.

¹³⁸ Il y est discuté les mêmes profils de fonction, les mêmes modèles types de questionnaires, les formations identiques; en ce sens, voy.: www.wallonie.be/fr/tracing-et-appli-coronalert.

tion épidémique en Belgique et de prendre, si nécessaire, les mesures harmonisées qui s'imposent¹³⁹. Elles ont mis en place des *call-centers* dont les agents sont chargés de dresser la liste de tous les contacts à haut risque croisés par une personne contaminée. Tous ces contacts étroits sont à leur tour appelés par les « traceurs »¹⁴⁰. Ils doivent se mettre en quatorzaine et se faire tester. Si le test s'avère positif, la procédure redémarre, le but étant évidemment de casser les chaînes de transmission en isolant les cas potentiellement positifs. De la sorte, il est procédé à un confinement individualisé. Enfin, on notera que dans ce système de *tracing* dit manuel mis en place par l'arrêté royal du 4 mai 2020¹⁴¹, le fait de figurer dans la banque de données est automatique pour les personnes déclarées atteintes du coronavirus et les personnes suspectées d'avoir été en contact.

Cependant, la méthode « manuelle » de *tracing* se montre attentatoire à la vie privée, elle est chronophage et coûteuse en termes de ressources humaines et ne répond pas aux exigences du modèle de propagation du coronavirus. En effet, une étude de la revue scientifique *Science*¹⁴² expose que :

« la propagation du virus est trop rapide pour être contenue par le suivi manuel des contacts, mais pourrait être contrôlée si ce processus était plus rapide et plus efficace et s'il se déroulait à grande échelle. Une application de suivi des contacts qui crée une mémoire des contacts étroits et notifie instantanément les contacts des cas positifs peut permettre de contrôler l'épidémie si suffisamment de personnes l'utilisent » (traduction libre).

La Commission européenne a également émis une recommandation en ce sens. Elle préconise une approche coordonnée de l'utilisation des applications de suivi dans la lutte contre le coronavirus¹⁴³. À ce titre, les solutions de suivi automatisé des contacts présentent des avantages non négligeables.

¹³⁹ En Wallonie, la supervision du dispositif est assurée par la Cellule des maladies infectieuses de l'AVIQ, déjà en charge de toute la procédure de « *contact tracing* » au début de l'épidémie en Belgique. Ce service dispose d'une expertise importante en matière de « *contact tracing* » puisqu'elle organise ce traçage depuis plus de dix ans pour tout type d'épidémie (rougeole, malaria...).

¹⁴⁰ À Singapour, la police est impliquée dans ce processus et dotée de pouvoirs étendus. En Corée du Sud, les autorités suivent même les itinéraires et les contacts des personnes infectées en évaluant les informations provenant des caméras de surveillance, de l'utilisation des cartes de crédit et des téléphones portables.

¹⁴¹ Arrêté royal n° 18, du 4 mai 2020, portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19, M.B., 4 mai 2020.

¹⁴² L. FERRETTI, Chr. WYMANT *et al.*, « Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing », *Science*, 31 mars 2020, disponible à l'adresse : <https://science.sciencemag.org/content/sci/early/2020/03/30/science.abb6936.full.pdf>; consulté en dernier lieu le 20 octobre 2020.

¹⁴³ Commission européenne, *Recommendation to support exit strategies through mobile data and apps*, 8 avril 2020, disponible à l'adresse : https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626; consulté en dernier lieu le 20 octobre 2020.

b. Le *tracing* automatique

30. Le *tracing* automatique et son fonctionnement. Les applications de suivi automatique des contacts s'appuient généralement sur la technologie *Bluetooth*, une technologie radio à faible distance installée sur la plupart des téléphones récents. De manière générale, le *Bluetooth* constitue la technologie qui permet de communiquer avec d'autres appareils compatibles¹⁴⁴, ou encore avec d'autres téléphones sur une courte distance. Ainsi, les applications de suivi de contacts, lorsque deux téléphones se rencontrent, échangent des numéros d'identification. Cela permet de suivre les rencontres ultérieures.

Il existe deux modèles dans la mise en œuvre de ce *tracing* utilisant la technologie *Bluetooth*, l'un, choisi notamment par la France, centralisé via un serveur et une base de données centrale et l'autre, décentralisé et préféré notamment par l'Allemagne et le Canada, impliquant la conservation des données dans chaque terminal des utilisateurs, à savoir nos smartphones. Le modèle décentralisé implique la conservation des données dans chaque terminal. Ces derniers ne s'échangent que des données dites « anonymisées », même si des systèmes d'IA prédictifs associeront à ces données un facteur de risque. Ce modèle exclut toute banque de données centrale reprenant les données échangées, ce qui a pour conséquence de rendre difficile toute étude épidémiologique depuis ces informations, mais garantit la protection de la vie privée.

Inversement, dans le modèle centralisé, si les données sont gardées dans chaque dispositif, elles sont communiquées de manière centralisée mais ne sortent jamais du terminal sous une forme brute. Les terminaux transmettent les informations masquées, via des canaux et processus sécurisés, vers une infrastructure centrale où la modélisation et la transmission des mises à jour sont traitées et renvoyées. Cette approche est très critiquée. Est dénoncée la possibilité qu'un organisme central puisse briser l'anonymisation des données avec un effort suffisant. Par exemple, des graphiques sociaux pourraient être créés qui montrent comment les individus ont été infectés les uns les autres et ces données pourraient être mises en lien avec d'autres, par exemple celles de réseaux sociaux permettant l'identification à terme des utilisateurs.

Force est de reconnaître que ce système de *tracing* par *Bluetooth* DP3T est actuellement un moyen efficace d'éviter toute centralisation excessive et inappropriée des données de contact. Sans entrer dans les détails, l'infrastructure de serveurs se compose à tout le moins de deux bases de données (ou deux plateformes) où des données sont traitées :

- 1) une application mobile ;
- 2) une infrastructure de serveurs avec bases de données.

¹⁴⁴ C'est la technologie qui permet à vos oreillettes de se connecter à votre smartphone, par exemple.

Dès lors, c'est à raison, choisissant la méthode la moins invasive, que la Belgique a développé sa propre application sur la base du modèle décentralisé de type DP3T¹⁴⁵, appelé CORONALERT et fonctionnant comme suit¹⁴⁶.

31. De l'installation et du double hachage des clés. L'application CORONALERT est installée sur le smartphone, via l'*appstore* de Google ou d'Apple. L'application génère alors une clé secrète tous les jours. Sur la base de ces clés, les *tokens*¹⁴⁷, à savoir des nombres aléatoires encryptés en 128 bits, sont ensuite générés. Ce système de « double hachage »¹⁴⁸ (ou double encryption) assure, nous semble-t-il, le niveau de sécurité adéquat exigé par l'article 32 du RGPD¹⁴⁹.

Schéma relatif à l'installation du Groupe de travail sur les propositions du Comité interfédéral¹⁵⁰



32. Le fonctionnement en cas d'utilisation du système. Chaque *smartphone* diffuse régulièrement son *token* grâce à l'application de suivi des contacts vers les autres *smartphones* situés à proximité (1,5 mètre de distance). Un *token* différent est généré toutes les 10 à 20 minutes pour éviter que ces jetons ne soient utilisés pour suivre un utilisateur¹⁵¹. Ces jetons peuvent être reçus par n'importe quel *smartphone* à proximité.

¹⁴⁵ Decentralized Privacy-Preserving Proximity Tracing; voy. *Application de traçage des contacts – Belgique. Analyse d'impact relative à la protection des données (AIPD)*, op. cit.

¹⁴⁶ Nota aan de Interministeriële Conferentie over een contacttopsporingsapp, 25 mai 2020, p. 5, disponible à l'adresse: www.esat.kuleuven.be/cosic/sites/corona-app/wp-content/uploads/sites/8/2020/07/nota_app_jmc.pdf; consulté en dernier lieu le 20 octobre 2020.

¹⁴⁷ Un *token* d'identification est un code de plusieurs chiffres et caractères, nécessaire pour associer des données d'identité à une ID numérique.

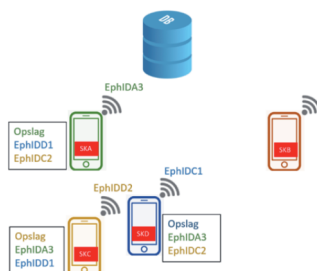
¹⁴⁸ La fonction de hachage (de l'anglais *hash function*) est une fonction qui, à partir d'une donnée fournie en entrée, calcule une empreinte numérique servant à identifier rapidement la donnée initiale, au même titre qu'une signature pour identifier une personne. Les fonctions de hachage sont utilisées en informatique et en cryptographie.

¹⁴⁹ Nota aan de Interministeriële Conferentie over een contacttopsporingsapp, op. cit., p. 5.

¹⁵⁰ *Ibid.*

¹⁵¹ *Ibid.*

*Schéma relatif au fonctionnement du Groupe de travail
sur les propositions du Comité interfédéral¹⁵²*

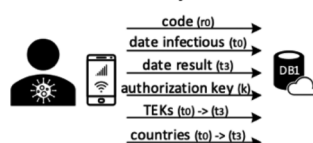


33. Quid en cas de communication par un utilisateur? En cas de contamination confirmée par un test et un médecin, la personne télécharge les clés secrètes des jours infectieux avec les données correspondantes dans une base de données centrale (la liste des *logs*). Ces clés sont retirées de cette base de données après quatorze jours. Comme le citoyen doit être mis en quarantaine aussi longtemps qu'il est contagieux, l'application doit être supprimée après le chargement des clés.

*Schéma du Groupe de travail sur les propositions du Comité interfédéral¹⁵³
ainsi du DPIA de l'application relative aux données
partagées avec Sciensano*



Schéma de l'envoi des informations à la BD1 de Sciensano pour alerter les autres citoyens



34. La fin de la pandémie. De manière générale, les clés sont supprimées après quatorze jours, de sorte qu'à la fin de l'épidémie, les serveurs pourront être démantelés après quatorze jours et Google et Apple ne supporteront plus l'API. Les utilisateurs seront alors invités à supprimer l'application.

35. Un tracing s'appuyant sur cinq bases de données. Le tracing belge a la particularité de conjuguer les systèmes de *tracing* manuel et de *tracing* auto-

¹⁵² *Ibid.*

¹⁵³ *Ibid.*, p. 6.

matique, en conservant un certain cloisonnement de sorte que pas moins de cinq bases de données sont requises¹⁵⁴ :

- *Base de données I*: de *Sciensano*, que l'on pourrait grossièrement nommée la « Base de données Coronavirus ». Les données qui y seront reprises sont communiquées notamment par les médecins.
- *Base de données II*: s'entend de la base de données existante depuis 2014 sous la responsabilité de *Sciensano* et qui regroupe des données collectées à partir de la « Base de données I » après pseudonymisation en vue de l'utilisation de ces données pour la recherche scientifique et épidémiologique.
- *Base de données III*: c'est la base de données des demandes d'appel et des demandes pour le personnel des centres de contact. Les entités fédérées, pour ce qui relève de leurs compétences respectives, sont les responsables des traitements de cette base de données.
- *Base de données IV*: s'entend des bases de données contenant les coordonnées des collectivités, à savoir des communautés de personnes pour lesquelles il existe un risque accru de propagation du virus, telles qu'un hôpital, une école, une prison, une maison de repos et de soins ; les entités fédérées sont les responsables de cette base de données pour ce qui relève de leur compétence respective. Les Bases de données III et IV échangent des données entre elles et avec la Base de données I dans le cadre du suivi des contacts.
- *Base de données V*: correspond au journal central des enregistrements qui permet de contrôler le fonctionnement de l'application numérique de traçage de contacts, dont *Sciensano est responsable*.

36. En résumé¹⁵⁵. Le système de traçage numérique belge consiste, d'une part, en une application mobile que l'utilisateur, peut installer volontairement sur son téléphone (*GSM, smartphone*) et utiliser, au moyen du *Bluetooth* générant des « ID secrets » et non permanents et effectuant des échanges avec d'autres utilisateurs disposant de la même application et avec lesquels il entre en contact rapproché. Ces contacts sont conservés temporairement dans l'application pour que des alertes puissent être envoyées en cas de contamination. D'autre part, le système comporte une infrastructure de serveurs correspondante qui facilite la consultation d'un résultat de test personnel et l'envoi anonyme d'alertes aux

¹⁵⁴ Art. 2 §§ 2 et 3, de l'arrêté royal n° 44, du 26 juin 2020, 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 des personnes (présumées) infectées par le coronavirus Covid-19 sur la base d'une base de données auprès de *Sciensano*, *M.B.*, 29 juin 2020.

¹⁵⁵ Pour plus de détails, voy. l'article du *Soir* paru le 1^{er} octobre 2020: « Coronalert: le mode d'emploi de l'application de traçage: vidéo », disponible à l'adresse: www.lesoir.be/328815/article/2020-10-01/coronalert-le-mode-demploi-de-lapplication-de-tracage-video.

contacts à risque d'une personne ayant un test de laboratoire positif¹⁵⁶. On ajoute que l'application CORONALERT est utilisable dans les pays européens qui ont adopté le même système d'application (DP3T) et avec lesquels il existe un accord.

Ensuite, l'application en termes de fonctionnalités permet à l'utilisateur de l'appareil de conserver son autonomie. Il décide lui-même de l'installation et de l'utilisation de l'application et il décide également d'échanger ou non des données avec l'infrastructure de serveurs. L'utilisateur a également toujours la possibilité de désactiver temporairement l'application sans devoir pour autant désactiver le *Bluetooth* de l'appareil. L'ensemble de ces fonctionnalités permet d'assurer le respect de la vie privée des utilisateurs de l'application. Il serait erroné de parler de *tracking*.

2. *La chronologie des interventions réglementaires*

37. La multiplication des arrêtés royaux de pouvoirs spéciaux. Pendant la première phase de gestion de la pandémie, nos gouvernements ont sévèrement restreint nos droits fondamentaux par voie d'arrêtés de pouvoirs spéciaux pour limiter la propagation du coronavirus Covid-19, au mépris des dispositions de l'article 187 de la Constitution et parfois même de l'obligation du respect des exigences de légalité formelle, en cas de limitation de ces droits¹⁵⁷. Le premier arrêté du 23 mars 2020, que l'on peut qualifier d'arrêté confinement, sera modifié à dix reprises, notamment par les arrêtés du 24 mars 2020¹⁵⁸,

¹⁵⁶ Voilà comment le Rapport au Roi qui précède l'A.R. n° 44 (déjà cité, p. 48.433) présente le système sur la base duquel fonctionne l'application CORONALERT : « Le système DP3T a été publié, et le code source est public afin qu'il puisse être vérifié par des experts indépendants. En ce sens, il répond à la recommandation de l'APD dans son avis 34/2020 consistant à demander de publier le code source.

Une application numérique de traçage de contacts basée sur le DP3T se compose d'une application mobile qui peut être installée et utilisée par l'utilisateur sur une base volontaire en local sur son appareil, et d'un journal central des enregistrements. L'application mobile enregistre les contacts entre les utilisateurs sans les identifier. Le journal des enregistrements permet à un utilisateur de transmettre volontairement une infection identifiée et le moment probable de cette infection de manière contrôlée, afin que les autres utilisateurs puissent être informés s'ils ont été en contact avec l'utilisateur infecté pendant la période où il a été contagieux, sans que l'identité de l'utilisateur infecté ou de l'autre utilisateur avec lequel il était en contact puisse être identifiée.

Une application numérique de traçage de contacts basée sur le système DP3T ne stocke que des données totalement pseudonymisées ou anonymes sur le dispositif de l'utilisateur, notamment des clés sécurisées et des numéros de série temporairement aléatoires, sans référence à l'identité des personnes entre lesquelles le contact a eu lieu ou au lieu où ce contact a eu lieu. La durée approximative du contact est conservée car elle est nécessaire pour établir si le contact a eu lieu entre le début de la contagiosité et l'établissement de l'infection ».

¹⁵⁷ Le lecteur est renvoyé *supra*, section 1, § 2, A, 1.

¹⁵⁸ Arrêté ministériel du 24 mars 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 24 mars 2020.

puis du 3 avril 2020¹⁵⁹, 17 avril 2020¹⁶⁰, 30 avril 2020¹⁶¹, 8 mai 2020¹⁶², 15 mai 2020¹⁶³, 20 mai 2020¹⁶⁴, 25 mai 2020¹⁶⁵ et 30 mai 2020¹⁶⁶; enfin, une ultime modification sera apportée le 5 juin 2020¹⁶⁷. Il sera enfin abrogé par l'arrêté du 30 juin 2020¹⁶⁸, lui-même modifié dernièrement le 18 octobre 2020, par les récentes et dernières mesures du nouveau gouvernement. Ces mesures prises par ces arrêtés à l'occasion de la phase dite de confinement, vont s'assouplir progressivement à mesure que le déconfinement s'établit notamment grâce au *tracing*. Elles viennent, tout récemment en ce mois d'octobre, de retrouver une seconde vie à l'occasion de ce qui est désormais appelé la « seconde vague » (à moins que ce ne soit simplement la « deuxième »).

a. Le *tracing* manuel dans le texte des arrêtés de pouvoirs spéciaux

38. Les A.R. de pouvoirs spéciaux n° 18 et n° 25. Initialement souhaité automatique, via la fonction *Bluetooth* des mobiles, le projet a été suspendu et la Belgique s'est orientée dans un premier temps vers un système de *tracing* dit manuel, en renvoyant la responsabilité de la mise en œuvre de ce projet aux entités fédérées, qui sont compétentes en matière de prévention¹⁶⁹. Ce *tracing* manuel est régi par plusieurs textes. À l'échelon fédéral, l'arrêté royal n° 18¹⁷⁰ du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19 ouvrira le bal et sera prorogé une première fois par l'arrêté royal n° 25¹⁷¹.

¹⁵⁹ Arrêté ministériel du 3 avril 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 3 avril 2020, *errat. M.B.*, 7 avril 2020, p. 25000.

¹⁶⁰ Arrêté ministériel du 17 avril 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 17 avril 2020; portant sur les magasins de bricolage, jardinerie, pépinières, magasins en gros pour les professionnels.

¹⁶¹ Arrêté ministériel du 30 avril 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 30 avril 2020.

¹⁶² Arrêté ministériel du 8 mai 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 8 mai 2020.

¹⁶³ Arrêté ministériel du 15 mai 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 15 mai 2020.

¹⁶⁴ Arrêté ministériel du 20 mai 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 20 mai 2020.

¹⁶⁵ Arrêté ministériel du 25 mai 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 25 mai 2020.

¹⁶⁶ Arrêté ministériel du 30 mai 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 30 mai 2020.

¹⁶⁷ Arrêté ministériel du 5 juin 2020 modifiant l'arrêté ministériel du 23 mars 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 5 juin 2020, *errat. M.B.*, 10 juin 2020.

¹⁶⁸ Arrêté ministériel du 30 juin 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus Covid-19, M.B., 30 juin 2020; lui-même modifié au gré des Conseils nationaux de sécurité successifs.

¹⁶⁹ Art. 5, § 1^{er}, l. al. 1^{er}, 8^o, de la loi spéciale du 8 août 1980 de réformes institutionnelles, M.B., 15 août 1980.

¹⁷⁰ Arrêté royal n° 18, du 4 mai 2020, portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19, M.B., 4 mai 2020.

¹⁷¹ Arrêté royal n° 25, du 28 mai 2020, modifiant l'arrêté royal n° 18 du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19, M.B., 3 juin 2020.

L'arrêté n° 18 met en œuvre les bases de données centralisées, nécessaires au *tracing* manuel, auprès du Service fédéral de la Santé publique, Sciensano. Sciensano deviendra ainsi le responsable du traitement de bases de données contenant notamment les numéros de téléphone des utilisateurs ayant été testés « positifs », les noms et numéros de téléphone des « contacts », des personnes infectées à appeler, la date et la durée de leurs contacts, etc. ainsi que d'autres données sur la base de sources diverses (médecins, labos, hôpitaux, etc.), y compris des données relatives à la santé des personnes pour lesquelles le médecin présume une infection, pour lesquelles un test a été prescrit, qui ont subi un test ou ont été hospitalisées. Ces données peuvent également concerner leurs contacts et leur médecin.

b. L'avis de l'APD sur le *tracing* manuel

39. Les avis de l'APD. Ces arrêtés ont été pris sans avis du Conseil d'État vu l'extrême urgence invoquée ; néanmoins, l'APD n'a pas manqué de largement en commenter le contenu¹⁷² dans les divers avis qui lui ont été demandés, et notamment dans les avis suivants :

- n° 34/2020, du 28 avril 2020, concernant un avant-projet d'arrêté royal n° XXX portant exécution de l'article 5, § 1^{er}, 1^o, 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 population¹⁷³ ;
- n° 36/2020, du 29 avril 2020, concernant un avant-projet d'arrêté royal n° XXX portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19 ;
- n° 42/2020, 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 ;
- n° 44/2020, du 5 juin 2020, concernant des amendements formulés au sujet d'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 ;
- n° 46/2020, du 5 juin 2020, concernant un amendement formulé au sujet d'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.

¹⁷² APD, avis 36/2020, du 29 avril 2020, concernant un avant-projet d'arrêté royal n° XXX 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), disponible à l'adresse : www.autoriteprotectiondonnees.be/publications/avis-n-36-2020.pdf; consulté en dernier lieu le 20 octobre 2020.

¹⁷³ Disponible à l'adresse : www.autoriteprotectiondonnees.be/publications/avis-n-34-2020.pdf; consulté en dernier lieu le 20 octobre 2020.

40. Les critiques de l'APD. L'APD a critiqué, à plusieurs égards, le prescrit du texte de l'arrêté n° 18, mais également celui de deux propositions de loi¹⁷⁴, l'une portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus et l'autre relative à l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus parmi la population. Elle y souligne, de manière répétée, la violation des principes généraux énoncés dans le RGPD, et notamment les principes de minimisation et de proportionnalité énoncés à l'article 5, 1., c), du Règlement, en ce que des données, qui semblent éloignées du but initial, sont collectées ; à titre exemplatif, elle énonce ce qui suit¹⁷⁵ :

« L'Autorité n'est pas en mesure d'examiner si ces données sont effectivement, conformément à l'article 5.1.c) du RGPD, "adéquates, pertinentes et limitées à ce qui est nécessaire au regard [de la finalité pour laquelle elles sont traitées]" . L'Autorité se demande, en particulier, ce que recouvre "le statut professionnel" et la pertinence de cette information au regard de la finalité poursuivie. Mais il en va de même pour l'ensemble des données reprises dans ce paragraphe ».

À cette première observation s'ajoute l'interrogation de l'APD sur « la nécessité d'intégrer à la base de données de Sciensano les données des personnes avec lesquelles le patient est entré en contact dans la base de données centrale gérée par Sciensano qui reprendra également les données relatives aux personnes infectées, présumées infectées, à qui un test a été conseillé, etc. avec les risques de recoupement évidents qu'implique cette centralisation. Ne serait-il pas possible d'atteindre l'objectif recherché sans intégrer ces données dans cette base de données centralisée auprès de Sciensano, mais dans une base de données gérée par le centre de contact ? Le centre de contact pourrait alors communiquer des données anonymisées (ou à tout le moins pseudonymisées) »¹⁷⁶.

L'APD souligne, avec ténacité, l'illicéité de la centralisation des données dans une énorme base de données gérée par Sciensano, en affirmant que :

« La création d'une base de données centralisée, en particulier lorsque celle-ci reprend des données sensibles (à savoir, en l'occurrence, des données concernant la santé), provenant de sources diverses et qu'elle poursuit plusieurs finalités distinctes, constitue une ingérence importante dans le droit à la protection des données à caractère personnel. L'Autorité rappelle, à cet égard, que toute ingérence dans le droit au respect de la protection des données à caractère personnel, en particulier lorsque l'ingérence s'avère importante, n'est admissible que si elle est nécessaire et proportionnée à l'objectif (ou aux objectifs) qu'elle

¹⁷⁴ C.E., avis n° 67.425/3, du 26 mai 2020, sur 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.

¹⁷⁵ APD, avis 36/2020, *op. cit.*, p. 8, § 24.

¹⁷⁶ APD, avis 36/2020, *op. cit.*, p. 11, § 32.

poursuit et qu'elle est encadrée par une norme suffisamment claire et précise et dont l'application est prévisible pour les personnes concernées».

Ainsi, elle «se demande, en outre, pourquoi les données qui sont communiquées aux services d'inspection de la prévention en matière de santé doivent être centralisées chez Sciensano? Pourquoi n'est-il pas suffisant de prévoir une communication directe entre les centres de contact et ces services? Ou alors ces "services d'inspection de la prévention en matière de santé" sont-ils ces centres de contact de sorte que les première et troisième finalités se recoupent en réalité, du moins partiellement?»¹⁷⁷.

Par ailleurs, l'arrêté royal n° 18, en son article 4, § 1^{er}, laisse à la Chambre «Sécurité sociale et santé» du Comité de sécurité de l'information le soin de déterminer les données à transmettre à Sciensano, ce qui est pour le moins discutable au regard des exigences jurisprudentielles du Conseil de l'Europe et de l'article 22 de la Constitution belge¹⁷⁸. Nous reviendrons sur ce point (*infra*, n° 43).

41. La centralisation des données auprès de Sciensano et la répartition des compétences dans notre Belgique fédérale. Enfin, dans un avis ultérieur du 25 mai 2020, n° 42/2020, et concernant cette fois la proposition de loi portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus, l'APD confirme avec vigueur sa position et rappelle qu'une base centralisée de données ne se justifie pas en l'occurrence¹⁷⁹. Elle affirme que :

«Plus fondamentalement, l'Autorité constate que la proposition de loi qui, malgré une rédaction qui manque de clarté et de cohérence, semble vouloir mettre en place un système de traçage des contacts mais organise en réalité, sans nécessité apparente, la centralisation d'une quantité indéfinie (et indéfinissable) de données (y compris sensibles ou dont l'accès est restreint de par des lois spécifiques) au sein d'une banque de données constituée et gérée par une instance qui n'en fait pas usage».

Elle persiste en ce sens, à l'occasion de son avis n° 46/2020, dans lequel elle précise, en arguant du partage des compétences entre État fédéral et entités

¹⁷⁷ APD, avis 36/2020, *op. cit.*, p. 5, § 13.

¹⁷⁸ En ce sens, nous renvoyons à l'avis du Conseil d'État, section de législation, notamment n° 67.953/1/V, du 31 août 2020, sur un projet d'arrêté royal portant exécution de l'arrêté royal n° 44 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.

¹⁷⁹ APD, avis 42/2020, du 25 mai 2020, 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), disponible à l'adresse : www.autoriteprotectiondonnees.be/publications/avis-n-42-2020.pdf; consulté en dernier lieu le 20 octobre 2020.

fédérées en ce qui concerne les moyens à mettre en place dans la lutte contre le virus¹⁸⁰, ce qui suit :

« Il ressort d'une lecture combinée de l'avis de l'Autorité et de l'avis du Conseil d'État relatifs à la proposition de loi, que : [...] »

c) il appartient aux institutions désignées par ces entités fédérées, en leur qualité de responsables des traitements effectués par leurs centres de contact, de déterminer si elles souhaitent faire appel à un/des sous-traitants (notamment pour la conservation et la gestion des données utilisées) et, dans ce cas, à quel(s) sous-traitant(s) ; il n'appartient donc pas à l'État fédéral d'imposer le recours à Sciensano comme entité chargée de la centralisation et de la gestion des données collectées, utilisées ou générées par ces centres de contact ;

[...]

l'Autorité considère que la centralisation des données dans une banque de données unique apparaît *a priori* injustifiée et disproportionnée ».

Vu, précisément, la reconnaissance de la compétence des entités fédérées, il est rappelé tant l'arrêté du gouvernement wallon de pouvoirs spéciaux n° 35¹⁸¹ que les arrêtés du gouvernement de la Communauté germanophone¹⁸² et du gouvernement flamand¹⁸³ portant création d'un centre de contact. Ces différents textes se fondent sur les compétences en matière de médecine préventive des entités fédérées et instituent les centres régionaux et communautaire de *contact tracing*, en charge du *tracing* manuel.

c. Le *tracing* automatisé dans le texte des arrêtés de pouvoirs spéciaux

42. Le cadre «légal» de cette application. Ensuite, l'application « traçage » numérique ou automatisé, qui facilite la détection précoce des personnes infectées ou potentiellement infectées a été mise sur pied et fonctionne depuis le mois de septembre. L'ambition et la finalité annoncées sont, en l'occurrence, de tracer rapidement les signes d'infection et d'informer à un stade précoce les

¹⁸⁰ APD, avis 46/2020, du 5 juin 2020, concernant un amendement formulé au sujet d'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, p. 3 § 5 et p. 9 § 22, disponible à l'adresse : www.autoriteprotectiondonnees.be/publications/avis-n-46-2020.pdf ; consulté en dernier lieu le 20 octobre 2020.

¹⁸¹ Arrêté du gouvernement wallon de pouvoirs spéciaux n° 35, du 5 mai 2020, organisant le *tracing* socio-sanitaire dans le cadre de la lutte contre l'épidémie Covid-19, M.B., 7 mai 2020.

¹⁸² Arrêté du gouvernement de la Communauté germanophone du 7 mai 2020, portant création d'un centre de contact chargé du suivi de la chaîne d'infection dans le cadre de la lutte contre la crise sanitaire provoquée par le coronavirus (Covid-19), M.B., 18 mai 2020. APD, avis 50/2020, du 5 juin 2020, concernant un projet de décret de la Communauté germanophone relatif au suivi de la chaîne d'infection dans le cadre de la lutte contre la crise sanitaire provoquée par le coronavirus (Covid-19) (CO-A-2020-047) ; disponible à l'adresse : www.autoriteprotectiondonnees.be/publications/avis-n-50-2020.pdf ; consulté en dernier lieu le 20 octobre 2020.

¹⁸³ Arrêté du gouvernement flamand, du 8 mai 2020, ajustant les procédures et délais administratifs dans la réglementation du domaine politique du Bien-être, de la Santé publique et de la Famille à la suite de la propagation du Covid-19 et modifiant divers arrêtés du gouvernement flamand dans ce domaine politique, M.B., 26 mai 2020.

personnes concernées en vue de leur isolement. Après l'échec de la proposition de loi relative à l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus Covid-19 parmi la population, c'est par la voie d'un arrêté numéroté que procédera le gouvernement fédéral. Ainsi, au mépris du principe de légalité et en violation des règles répartitrices des compétences¹⁸⁴, le sort de cette application sera réglé par l'arrêté royal n° 44 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 (présümées) infectées par le coronavirus Covid-19¹⁸⁵. Le projet d'arrêté fera l'objet de vives critiques tant du Conseil d'État¹⁸⁶ que de l'APD¹⁸⁷.

d. Les avis du Conseil d'État et de l'APD

43. Les critiques du Conseil d'État. Le Conseil d'État n'a pas manqué de relever l'illégalité formelle originelle qui entachait l'arrêté royal. Il précise à cet égard que :

« Dans sa forme actuelle, la proposition de loi soumise pour avis ne peut se concrétiser que si elle est transformée en un accord de coopération, pour lequel l'assentiment parlementaire est requis. Cet accord pourrait en effet lier les Belges individuellement et il concerne des matières qui – eu égard au principe de légalité inscrit à l'article 22 de la Constitution – doivent être réglées par la loi. Pareil accord de coopération offre au demeurant la meilleure sécurité juridique. Dans les circonstances données, et compte tenu du fait que l'arrêté royal n° 18 du 4 mai 2020 est déjà d'application dans la pratique, l'accord de coopération peut se voir attribuer un effet rétroactif au 4 mai 2020, à savoir au jour où l'arrêté concerné est entré en vigueur (voir à ce sujet l'observation 16.1) »¹⁸⁸.

¹⁸⁴ En ce sens, voy. C.E., avis n°s 67.425/3, 67.426/3 et 67.427/3, du 26 mai 2020, sur 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 » (*Doc. parl.*, Ch. repr., sess. 2019-2020, n° 55-1249/001); un amendement sur la 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 » (n° 55-1249/002); des amendements sur la 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 » (n° 55-1249/003), disponibles à l'adresse: www.raadvst-consetat.be/dbx/avis/67426.pdf#search=sciensano; consulté en dernier lieu le 20 octobre 2020.

¹⁸⁵ Arrêté royal n° 44, du 26 juin 2020, 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 (présümées) infectées par le coronavirus Covid-19 sur la base d'une base de données auprès de Sciensano, M.B., 29 juin 2020.

¹⁸⁶ C.E., avis n°s 67.425/3, 67.426/3 et 67.427/3, du 26 mai 2020, *op. cit.*

¹⁸⁷ APD, avis 43/2020, du 26 mai 2020, concernant une proposition de loi relative à l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus Covid-19 parmi la population, disponible à l'adresse: www.autoriteprotectiondonnees.be/publications/avis-n-43-2020.pdf; consulté en dernier lieu le 20 octobre 2020.

¹⁸⁸ C.E., avis n°s 67.425/3, 67.426/3 et 67.427/3, du 26 mai 2020, *op. cit.*, p. 17.

En effet, il y a lieu de rappeler que si la recherche scientifique est une compétence fédérale, la recherche des infections au coronavirus relève de la compétence des Communautés^{189 190}.

Le Conseil d'État précise à cet égard que :

« La recherche des infections au Covid-19 relève [...] de la compétence des Communautés. Cette compétence comprend également l'établissement d'une réglementation visant à protéger les personnes physiques lors du traitement de données à caractère personnel recueillies à la suite de cette recherche. Dans la mesure où la proposition de loi soumise pour avis prévoit des règles relatives au traitement de ces données à caractère personnel, elle empiète sur la compétence communautaire en matière de médecine préventive ».

Dès lors, un accord de coopération¹⁹¹ entre les entités fédérées et celui fédéral pour lequel l'assentiment parlementaire est requis¹⁹², offrant, au demeurant une meilleure sécurité juridique. D'autant que par ce truchement sera mis sur pied un Comité de sécurité¹⁹³ réunissant autour du premier ministre et le ministre de la santé fédéral auquel assistent les représentants des Régions et Communautés, et qui assure la coordination et la coopération entre les niveaux de pouvoirs.

44. Le point particulier de la délégation au Comité de sécurité de l'information. Un autre point est celui de la délégation confiée au Comité de sécurité de l'information créé par la loi du 5 septembre 2018 instituant le Comité de sécurité de l'information et modifiant diverses lois concernant la

¹⁸⁹ Les Communautés sont compétentes pour le dépistage et la lutte contre les maladies contagieuses et sociales en tant que composante de leurs compétences en matière de médecine préventive, conformément aux dispositions de l'article 5, § 1^{er}, I, alinéa 1^{er}, 8^o, de la loi spéciale du 8 août 1980 de réformes institutionnelles, M.B., 15 août 1980; voy. en ce sens *Doc. parl.*, Sénat, sess. 1979-1980, n° 434/2, p. 125; *Doc. parl.*, Ch. repr., sess. 1979-1980, n° 627/10, p. 52. Cette compétence avait été implicitement confirmée dans les avis suivants: C.E., avis n° 34.339/AG du 29 avril 2003 sur un avant-projet devenu le décret de la Communauté flamande et de la Région flamande du 21 novembre 2003 « betreffende het preventieve gezondheidsbeleid », C.E., avis n° 38.381/3 du 7 juillet 2005 sur un projet d'arrêté royal établissant les mesures prophylactiques et la déclaration obligatoire à la cellule de vigilance sanitaire de pathologies présentant un caractère épidémique et C.E., avis n° 53.018/VR du 13 mai 2013 sur un projet d'arrêté royal relatif au contrôle sanitaire du trafic international.

¹⁹⁰ En ce qui concerne la Communauté française, l'exercice de cette compétence a été transféré à la Région wallonne et à la Commission communautaire française conformément à l'article 3, 6^o, du décret spécial du 3 avril 2014 relatif aux compétences de la Communauté française dont l'exercice est transféré à la Région wallonne et à la Commission communautaire française et aux décrets parallèles de la Région wallonne et de la Commission communautaire française.

¹⁹¹ Art. 92bis, § 1^{er}, al. 2, de la loi spéciale du 8 août 1980 de réformes institutionnelles, M.B., 15 août 1980.

¹⁹² C.E., avis n°s 67.425/3, 67.426/3 et 67.427/3, du 26 mai 2020, sur 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, p. 15, disponibles à l'adresse: www.raadvst-consetat.be/dbx/avis/67426.pdf#search=sciensano; consulté en dernier lieu le 20 septembre

¹⁹³ En son article 6, l'accord de coopération définit un Comité interfédéral de *testing* et *tracing* qui se compose de représentants d'entités fédérées, de Sciensano, de la plateforme eHealth et de deux experts scientifiques. Ce comité est soutenu par un groupe de travail interdisciplinaire d'experts scientifiques.

mise en œuvre du Règlement et en particulier à la Chambre « Sécurité sociale et Santé ». L'article 10, § 3, de l'arrêté royal n° 44 prévoit en effet que :

« Les données à caractère personnel telles que communiquées et conservées dans la Base de données I, ne peuvent être transmises ultérieurement, après pseudonymisation, à la Base de données II¹⁹⁴, qu'aux fins définies à l'article 3, § 1^{er}, 4^o, conformément au Règlement Général sur la Protection des Données et à la loi du 5 septembre 2018 instituant le Comité de sécurité de l'information. Les données à caractère personnel telles que communiquées et conservées dans la Base de données II, ne peuvent être transmises à des tiers aux fins stipulées à l'article 3, § 1, 4^o qu'après la délibération, visée à l'article 11, de la Chambre "Sécurité sociale et Santé" du Comité de sécurité de l'information ».

Par ailleurs, les dispositions de l'article 5, alinéa 2, déléguaient à la même chambre le pouvoir de fixer un ensemble de délais de conservation des données pour certains traitements. Or, un tel blanc-seing n'est pas autorisé concernant au moins partiellement des éléments essentiels dont le règlement est réservé au législateur par l'article 22 de la Constitution. C'est sans doute en vue de rassurer le Conseil d'État que l'arrêté royal n° 44 a tenu à encadrer les prérogatives ainsi confiées à un organe dont la légalité, au regard des exigences du RGPD, a parfois été contestée¹⁹⁵ en précisant, en son article 11, § 1^{er} :

« Dans la mesure où cela n'est pas repris dans le présent arrêté, tant la communication de données à caractère personnel à Sciensano pour traitement dans la Base de données I que la communication ultérieure de ces données à caractère personnel par Sciensano à des tiers ont toujours lieu après délibération de la Chambre "Sécurité sociale et Santé"; la Chambre "Sécurité sociale et Santé" du Comité de sécurité de l'information ne délibère sur les communications à ou par la Base de données I de Sciensano que dans la mesure où elles servent les fins visées à l'article 3, sans que la Chambre "Sécurité sociale et Santé" du Comité de sécurité de l'information puisse déterminer elle-même une autre fin ».

Ces précautions n'ont, semble-t-il, pas été suffisantes, d'autant que, d'une part, le fonctionnement de la Chambre reste obscur et fait l'objet de peu de contrôles et, d'autre part, que l'article 11 de l'arrêté permettait à la Chambre de « préciser, pour chaque finalité de traitement définie à l'article 3, quelles données à caractère personnel spécifiques peuvent être traitées dans le cadre d'une certaine catégorie de données à caractère personnel et qui sont communiquées à

¹⁹⁴ Sur la finalité et le contenu de ces bases de données, lire l'article 1^{er}, § 1^{er}, de l'A.R. n° 44 : « Base de données I: la base de données de Sciensano qui sera créée en vertu du présent arrêté pour le traitement et l'échange de données aux fins prévues à l'article 3; Base de données II: la base de données existante auprès de Sciensano, utilisée pour la recherche scientifique et établie par la loi du 10 avril 2014 portant des dispositions diverses en matière de santé et l'accord de coopération conclu en application de celle-ci entre l'INAMI et Sciensano et la loi du 25 février 2018 portant création de Sciensano; ».

¹⁹⁵ Voy., en particulier, E. DEGRAVE, « Titre 11 – L'autorité de contrôle », in C. DE TERWANGNE et K. ROSIER (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, coll. Cahiers du CRIDS, n° 44, Bruxelles, Larcier, 2018, pp. 593-611.

l'une des Bases de données II, III et IV ou qui doivent être communiquées à partir de la Base de données IV à la Base de données I, dans la mesure où cela est utile¹⁹⁶ pour atteindre la finalité de traitement en question [...]» et de «détermine[r] ou complète[r] les données à caractère personnel dans la catégorie de données à caractère personnel définie à l'article 6 ci-dessus».

Le Conseil d'État a ainsi rejoint la position de l'APD, rappelé dans son avis n° 64/2020 du 20 juillet 2020, où elle énonce avec vigueur que :

«comme elle l'a déjà fait dans ses avis n°s 36/2020 et 42/2020, que 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". Comme l'Autorité l'a déjà souligné plus haut, tout traitement (y compris donc toute communication) de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, comme c'est le cas, en l'espèce, doit être encadré spécifiquement par un texte législatif ou réglementaire (arrêté), et **donc pas par une délibération du Comité de sécurité de l'information**¹⁹⁷. L'Autorité rappelle que cette réglementation doit être précise et définir, au moins, les éléments essentiels du traitement, dont les finalités déterminées, explicites et légitimes ; les (catégories de) données à caractère personnel qui sont pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités poursuivies ; le délai de conservation maximal des données à caractère personnel enregistrées ; la désignation du responsable du traitement ; les destinataires ou catégories de destinataires auxquels les données sont communiquées et les circonstances dans lesquelles et les raisons pour lesquelles elles seront communiquées »¹⁹⁸.

En réservant au législateur compétent le pouvoir de fixer les conditions des limitations au droit au respect de la vie privée, l'article 22 de la Constitution garantit aux individus qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. Néanmoins, une délégation n'est pas interdite si cette délégation est définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur¹⁹⁹.

¹⁹⁶ ... et non nécessaire comme l'exige pourtant le RGPD.

¹⁹⁷ Nous soulignons.

¹⁹⁸ APD, avis 64/2020, du 20 juillet 2020, 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 (présument infectées par le coronavirus Covid-19 sur la base d'une base de données auprès de Sciensano, disponible à l'adresse : www.autoriteprotectiondonnees.be/publications/avis-n-64-2020.pdf; consulté en dernier lieu le 20 octobre 2020.

¹⁹⁹ «Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur»; en ce sens, C.E., avis n°s 67.425/3, 67.426/3 et 67.427/3, du 26 mai 2020, *op. cit.*, p. 18, § 12.2; C.C., 20 février 2020, n° 27/2020, B.17; APD, avis 64/2020, du 20 juillet 2020, p. 20, § 60.

45. L'accord de coopération entre le fédéral et les entités fédérées – La base de licéité du système belge de *tracing*. Finalement, à l'heure actuelle, les traitements des données de la plateforme trouvent leur fondement juridique dans l'accord de coopération²⁰⁰ 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 dans le cadre d'un suivi des contacts auprès des personnes infectées ou supposées infectées par le coronavirus. Cet accord abroge et remplace les arrêtés royaux n° 18, n° 25 et n° 44. L'accord est complété par un accord du 13 octobre 2020, d'exécution entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92bis, § 1^{er}, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980.

La création du Conseil de sécurité²⁰¹, réunissant autour du premier ministre et du ministre de la santé fédéral les représentants des Régions et Communautés, assure cette coordination et permet cette coopération entre les niveaux de pouvoirs²⁰².

e. Les derniers avis de l'APD sur le *tracing* automatique

46. Les avis n° 79 et n° 96 de l'APD. Les avis de l'APD déjà commentés seront suivis de deux « derniers » avis. Le premier, l'avis n° 79/2020 du 7 septembre 2020, est relatif au projet d'arrêté royal portant exécution de l'arrêté

²⁰⁰ 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'inspections d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présümées) infectées par le coronavirus Covid-19 se fondant sur une base de données auprès de Sciensano, M.B., 15 octobre 2020; Accord de coopération d'exécution du 13 octobre 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92bis, § 1^{er}, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980, M.B., 10 octobre 1980.

²⁰¹ En son article 6, l'accord de coopération définit un Comité interfédéral de *testing* et *tracing* qui se compose de représentants d'entités fédérées, de Sciensano, de la plateforme eHealth et de deux experts scientifiques. Ce comité est soutenu par un groupe de travail interdisciplinaire d'experts scientifiques.

²⁰² Le Conseil national de sécurité est créé en 2015 à la suite des attentats de Paris; remplaçant le Comité ministériel du renseignement et de la sécurité, il regroupe, autour du premier ministre, les ministres de la Justice, de la Défense, de l'Intérieur et des Affaires étrangères, et les vices-premiers. Il établit la politique générale du renseignement et de la sécurité, en assure la coordination, et détermine les priorités des services de renseignement et de la sécurité, sur pied de l'arrêté royal du 28 janvier 2015. À l'occasion de la gestion de la pandémie, le CNS sort de ses attributions et s'élargit *de facto* aux ministres-présidents des différentes Régions et Communautés du pays. En vertu d'une conception élargie de la notion de sécurité, c'est cet organe qui a adopté puis annoncé les principales décisions de confinement de la population et de distanciation sociale destinées à enrayer la propagation du coronavirus.

royal n° 44 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 (présümées) infectées par le coronavirus Covid-19 sur la base d'une base de données auprès de Sciensano et d'un projet d'accord de coopération d'exécution conclu entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92bis, § 1^{er}, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980.

Enfin, le dernier avis de l'APD²⁰³ date du 2 octobre 2020. Il porte sur l'avant-projet de décret portant confirmation des arrêtés du gouvernement wallon de pouvoirs spéciaux pris dans le cadre de la gestion de la crise sanitaire liée au coronavirus pour les matières visées à l'article 138 de la Constitution.

47. Leçons à tirer des interventions de l'APD. Il faut reconnaître qu'en matière de protection de la vie privée et particulièrement de données à caractère personnel, les divers projets d'arrêtés de pouvoirs spéciaux, ou projets de décret et propositions de loi présentés tant à l'APD qu'au Conseil d'État ont entamé l'état de droit et pas toujours respecté les exigences de nos libertés fondamentales. Dans ce contexte, on ne peut que souligner le rôle bénéfique joué par l'APD et le Conseil d'État en la matière. Nos gouvernements ont été rappelés à l'ordre, de manière sévère, tant par le Conseil d'État que par l'Autorité belge de protection des données, pour les violations du RGPD et de l'article 22 de la Constitution, insérées dans le prescrit des textes soumis aux contrôles des deux hautes autorités. Ainsi, le moins que l'on puisse dire, c'est que le RGPD aura fait œuvre utile, pendant la gestion de la pandémie, tant par le contrôle opéré par l'APD, fraîchement installé, que par la médiatisation faite de cette problématique qui, sans doute à une autre époque où le RGPD n'était pas encore d'application, serait passée inaperçue.

B. Les principes généraux et les obligations du RGPD applicables au tracing

48. Propos de ce point B. Que ce soit notre APD²⁰⁴, le Conseil de l'Europe ou le CEPD, de manière unanime, il est admis que la protection des don-

²⁰³ APD, avis n° 96/2020, du 2 octobre 2020, relatif à l'avant-projet de décret portant confirmation des arrêtés du gouvernement wallon de pouvoirs spéciaux pris dans le cadre de la gestion de la crise sanitaire liée au Covid-19 pour les matières visées à l'article 138 de la Constitution, disponible à l'adresse: www.autoriteprotectiondonnees.be/publications/avis-n-96-2020.pdf.

²⁰⁴ APD, avis n° 34/2020, du 28 avril 2020, concernant un avant-projet d'arrêté royal n° XXX portant exécution de l'article 5, § 1^{er}, 1^o, 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).

nées personnelles n'est pas un obstacle à la mise en place d'outils technologiques dans le cadre de la lutte contre la pandémie, tant que ceux-ci respectent certains principes fondamentaux. Dans son avis n° 64/2020, l'Autorité belge de protection des données insiste sur le fait que toute application de traçage doit répondre aux règles et spécifications fixées par le CEPD. L'application de ces principes est essentielle afin d'assurer la légalité des traitements et la réalisation des droits fondamentaux. Il faut distinguer, une fois certaines notions de base rappelées et appliquées aux mesures de *tracing* (1), les principes généraux (2) découlant du RGPD, notamment les principes concernant les finalités (a) et la base de licéité (b), la transparence (c), la minimisation et la proportionnalité des traitements (d et e), le niveau de sécurité (f), et la durée de rétention (g), des règles positives qui y sont énoncées, telles que l'obligation de tenue d'une analyse d'impact (3) imposée par l'article 35 du RGPD.

1. *Notions de base : la donnée à caractère personnel et le responsable du traitement*

49. Les deux notions. Le caractère quelque peu hermétique de la matière de la protection des données nous enjoint dans le contexte de cette contribution un rappel de deux notions au cœur du sujet. Ainsi seront abordées et définies, d'une part, la notion de données à caractère personnel en opposition à celle de données anonymes non visées par le RGPD et souvent invoquée à propos des mesures prises par les opérateurs impliqués dans les opérations de *tracing* pour rendre difficiles l'identification des personnes concernées, d'autre part, la notion de responsable de traitement.

a. Notion de donnée à caractère personnel et anonymisation ou pseudonymisation

50. La notion. Les régimes de protection des données s'appliquent dès lors qu'il y a un traitement de données à caractère personnel. Par donnée à caractère personnel, il y a lieu d'entendre, selon le RGPD :

« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »²⁰⁵.

²⁰⁵ Article 4, 1., du RGPD. Le rapport explicatif de la Convention du Conseil de l'Europe dont l'article 2, a., reprend quasiment la même définition de la notion que le RGPD, contient cependant une remarque importante dont les juges devraient se saisir lors qu'ils seront amenés à s'interroger sur l'existence ou non d'une donnée à caractère personnel. Le rapport énonce : « Le terme "identifiable" ne fait pas uniquement référence à l'identité civile ou juridique en tant que telle de la personne, mais également à tout élément susceptible d'"individualiser" ou de distinguer (et donc de traiter différemment) une personne parmi

À l'inverse, un traitement qui ne porte pas sur des données à caractère personnel échappe au champ d'application du Règlement. Il en va ainsi des données rendues anonymes. Ce point est rappelé dans l'avis de l'EDPB du 21 avril 2020 :

«The EDPB emphasises that when it comes to using location data, preference should always be given to the processing of anonymised data rather than personal data. Anonymisation refers to the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable natural person against any “reasonable” effort. This “reasonability test” must take into account both objective aspects (time, technical means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails to pass this test, then it has not been anonymised and therefore remains in the scope of the GDPR »²⁰⁶.

Il est important de rappeler que, même si la préférence doit être réservée aux applications utilisant uniquement des données anonymes et échappant dès lors au RGPD, la notion de données anonymes est définie de façon restrictive par la jurisprudence de la Cour de justice de l'Union européenne (arrêt *Breier*) :

«l'article 2, sous a), de la directive 95/46/CE [...] doit être interprété en ce sens qu'une adresse de protocole Internet dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de cette disposition, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne »²⁰⁷.

On ne s'étonnera pas du nombre de paragraphes réservés par le CEPD à rappeler qu'anonymisation n'est pas pseudonymisation et qu'en l'occurrence, c'est bien de pseudonymisation qu'il faut parler, lorsque certes, l'identité de la per-

d'autres. Cette “individualisation” pourrait se faire, par exemple, à partir d'un numéro d'identification, d'un pseudonyme, de données biométriques ou génétiques, de données de localisation, d'une adresse IP ou d'un autre identifiant, qui renvoient à une personne donnée ou à un dispositif ou un ensemble de dispositifs (ordinateur, téléphone portable, appareil photo, console de jeu, etc.)».

Comme le notent très justement Cécile de Terwangne, Karen Rosier et Bénédicte Losdyck à la suite du rapport explicatif de la Convention n° 108 modifiée, on glisse, dans l'interprétation de la notion de données à caractère personnel, « de la notion d'identification vers un concept d'individualisation (la version anglaise utilise le terme “*singling out*” soit l'individualisation ou le ciblage) » (« Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, n° 62/2016, p. 12). La connaissance des traits de l'identité civile d'une personne n'est plus nécessaire pour l'individualiser et agir vis-à-vis d'elle : le concept d'« identifiabilité » devrait être élargi à ceux de traçabilité et de « contactibilité », et ce, notamment, pour résoudre l'éternelle question de la nature de données à caractère personnel comme l'adresse IP, les *cookies*, voire la possession d'une montre munie d'un tag.

²⁰⁶ EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak*, 21 avril 2020, disponible à l'adresse : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, n°s 14 et s.

²⁰⁷ CJUE, 19 octobre 2016, *P. Breier c. Allemagne*, C-582/14, § 65, disponible à l'adresse <http://curia.europa.eu/juris/document/document.jsf?docid=184668>; consulté en dernier lieu le 20 octobre 2020.

sonne n'est pas révélée²⁰⁸ mais que les besoins d'entrer en contact avec elle obligent bien évidemment à traiter un identifiant au sens de l'article 4, 1., a), du RGPD qui définit la donnée à caractère personnel²⁰⁹. Le RGPD doit donc s'appliquer.

b. Notion de responsable du traitement

51. La notion de responsable, en particulier de responsables conjoints.

Les acteurs intervenant dans les traitements de données à caractère personnel sont définis dans le Règlement en son article 4. Ainsi, conformément aux dispositions de l'article 4, 7., du RGPD le responsable du traitement est :

« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ; »

Avec cette définition, le Règlement confirme la possibilité pour deux ou plusieurs personnes d'intervenir ensemble dans la détermination des finalités et des moyens d'un traitement de données à caractère personnel et d'être alors considérées comme responsables conjoints ou coresponsables de traitement.

La qualification de coresponsables du traitement peut se présenter lorsque plus d'un acteur est impliqué dans le traitement. Le RGPD introduit des règles spécifiques pour les responsables de traitement conjoints et fixe un cadre pour régir leur relation. Le critère primordial de l'existence d'un contrôle conjoint réside dans la détermination des finalités et des moyens d'un traitement. Suivant les lignes directrices n° 7/2020 du CEPD²¹⁰, relatives aux notions de responsable du traitement et de sous-traitant²¹¹ :

« Joint participation can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities,

²⁰⁸ CNIL, Délibération citée, pp. 3 et 4.

²⁰⁹ On ajoute que les données de traçage enregistrées révèlent les relations entretenues entre les personnes concernées par ces traces. Par ailleurs, des travaux récents ont montré que des données affirmées comme anonymes peuvent, dans le cadre des recoupements que, précisément, permettent les outils d'intelligence artificielle, être « désanonymisées ». À cet égard, à propos des données de communications téléphoniques rendues anonymes et la possibilité de réidentifier les personnes concernées par ces données, voy. l'étude d'Y. DE MONTJOYE, S. GAMBS, V. BLONDEL *et al.*, « On the privacy-conscious use of mobile phone data », *Scientific Data*, n° 5, 11 décembre 2018, (www.nature.com/articles/sdata2018286.pdf) reprise par l'EDPB, *Guidelines 04/2020*, n° 20.

²¹⁰ EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, version 1.0, 2 septembre 2020, uniquement en anglais ; disponible à l'adresse : https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf ; consulté en dernier lieu le 20 octobre 2020.

²¹¹ Les présentes guidances sont soumises à une consultation publique actuellement ; elles ne sont donc pas définitives. Elles visent à remplacer, après leur adoption définitive, l'avis 01/2010 sur les notions de « responsable du traitement » et de « sous-traitant », du 16 février 2010, WP 169, sur le même sujet.

where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing. An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand».

La participation conjointe doit inclure la détermination des finalités, d'une part, et la détermination des moyens, d'autre part. La participation peut donc prendre la forme d'une décision commune prise par deux ou plusieurs entités ou résulter de décisions convergentes de deux ou plusieurs entités, lorsque les décisions se complètent et sont nécessaires pour que le traitement ait lieu. Un critère important est le caractère inséparable des traitements, c'est-à-dire que les traitements des entités sont inextricablement liés.

52. L'application de la notion aux banques de données utilisées dans le cadre de la crise du Covid-19. Dès lors, il paraît regrettable que Scien-sano soit actuellement encore le seul responsable du traitement de la «Base de données I», à savoir celle que nous avons nommée «Base de données Coronavirus», dès lors que les Régions et Communautés sont seules compétentes en matière de médecine préventive²¹². En effet, il ressort de l'article 5, § 1^{er}, 8^o, de la loi spéciale du 8 août 1980 de réforme des institutions que :

«Article 5. § 1. Les matières personnalisables visées à l'article 128, § 1^{er}, de la Constitution sont :

En ce qui concerne la politique de santé, [...]

8^o l'éducation sanitaire ainsi que les activités et services de médecine préventive, ainsi que toute initiative en matière de médecine préventive.

L'autorité fédérale reste toutefois compétente pour :

1^o l'assurance maladie-invalidité ;

2^o les mesures prophylactiques nationales».

Ainsi et à l'évidence, les finalités relatives à la médecine préventive réalisées depuis cette base de données le sont sur le pied des obligations et de la mission d'intérêt public conférées aux entités fédérées par le législateur spécial.

Par ailleurs, si la «Base de données I» permet également le transfert des données pseudonymisées à des fins de recherches scientifiques vers la «Base de données II», sur la base des compétences en matière de recherche scientifique de l'Autorité fédérale, l'article 6*bis* de la loi spéciale du 8 août 1980 de réforme des institutions attribue aux entités fédérées également la possibilité d'agir en cette matière, dans le cadre de leurs compétences propres.

²¹² D'autant que compte tenu du passif de cette autorité publique et de son image peu positive dans la société civile, l'on ne peut pas assurer qu'elle recueille la confiance du public au détriment de l'utilisation de l'application.

Dès lors que les finalités et moyens des deux responsables sont partagés, et leurs traitements depuis la « Base de données I » semblent inextricablement liés, la qualification de coresponsable nous paraît plus opportune. Cette répartition des rôles et des accès nous paraît plus conforme au prescrit de la législation relative à la protection des données²¹³. En toute hypothèse, cette centralisation dans les mains seules de Sciensano ne reflète pas la répartition des compétences telle que définie par la loi du 8 août 1980 relative aux réformes institutionnelles²¹⁴. Nous plaçons dès lors pour le régime de coresponsabilité, prévu par l'article 26 du RGPD²¹⁵. Ce régime suit les exigences déduites de la répartition des compétences et garantit la légalité des traitements. Il assure également une surveillance croisée, qui peut s'avérer utile dans la gestion de cette base de données.

Nous rappelons que, par ailleurs, la qualité des parties aux traitements est une réalité qui doit être établie de manière factuelle et que le juge n'est pas tenu à la qualification annoncée par les parties au traitement, même si celle-ci provient d'un texte réglementaire.

2. Les principes généraux de l'article 5 applicables aux tracings

a. Le principe de finalité du traitement

53. L'application du principe aux traitements nés du tracing. Les finalités des traitements utilisant la technologie du numérique pour lutter contre le virus peuvent être multiples et dépendent des technologies utilisées par le responsable du traitement. En l'occurrence, ce sont les finalités et bases de licéité des applications mises en place par les autorités publiques belges dans le cadre des tracings manuels et automatiques qui sont examinées. (Nous n'abordons pas celles mises en place par les entreprises ou administrations.)

La nécessité du respect strict du principe dit de finalité préside à la mise sur pied des systèmes de tracing. Le CEPD, dans ses « Lignes directrices »²¹⁶, s'agissant du tracing automatique, précise que :

²¹³ En outre, cette répartition permettra une plus grande adhésion de la population à l'outil, dès lors qu'il serait géré plus près d'eux et extrait des mains d'une administration qui souffre d'un déficit de popularité, voire de confiance.

²¹⁴ Loi spéciale du 8 août 1980 de réformes institutionnelles, M.B., 15 août 1980.

²¹⁵ L'article 26, alinéa 1^{er}, énonce : « Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord ».

²¹⁶ EDPB, *Guidelines 04/2020*, op. cit.

«These guidelines clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:

- using location data to support the response to the pandemic by modelling the spread of the virus so as to assess the overall effectiveness of confinement measures;
- contact tracing, which aims to notify individuals of the fact that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus, in order to break the contamination chains as early as possible».

On reconnaît là les deux finalités que la Belgique a distinguées comme les deux premiers temps d'action du gouvernement. La première finalité renvoie à une vérification globale de l'évolution de la pandémie (par exemple : les déplacements de population, les lieux de plus grande concentration de cas, les catégories de personnes plus vulnérables, etc.) et la seconde, déclenchée ensuite, accompagne la sortie du confinement qui correspond à un traçage individualisé²¹⁷. Ces finalités doivent également être clairement définies²¹⁸ dans les textes instituant le tracing *manuel* ou automatique et aucune utilisation des données à d'autres finalités ne peut être autorisée (par exemple : retracer les contacts d'une personne suspectée d'infractions, lutte contre la fraude à la sécurité sociale).

54. La définition des finalités dans l'accord de coopération. Fort de l'enseignement tiré des remarques émises par l'APD à l'occasion de ses avis sur les arrêtés royaux n° 18 et n° 44 notamment, l'accord de coopération a consacré

²¹⁷ Comme le notent Alessandra Pierucci et JeanPhilippe Walter dans leur « Statement » ou déclaration préparée pour le Conseil de l'Europe: *Déclaration de la Présidente du comité consultatif de la Convention n° 108 et du DPO du Conseil de l'Europe*, disponible à l'adresse: www.coe.int/fr/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter. Cette déclaration a été complétée, au vu des questions nouvelles soulevées par le déconfinement et particulièrement les applications Covid-19: www.coe.int/en/web/data-protection/contact-tracing-apps; consulté en dernier lieu le 20 octobre 2020.

²¹⁸ L'article 6.3 du RGPD qui vise les traitements, en particulier ceux « nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » (art. 6.1, e)), servira de guide en la matière.

L'article 6.1, e), stipule: « Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie: [...] e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; ». Le paragraphe 3 du même article précise que: « 3. Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par: a) le droit de l'Union; ou b) le droit de l'État membre auquel le responsable du traitement est soumis. Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi ».

un chapitre complet aux finalités des traitements, du *tracing* manuel, en son article 3. En résumé, trois grandes catégories de finalités à la création des bases de données et des traitements de données réalisés à partir de celles-ci sont décrites :

- La première finalité consiste à permettre la mise en place d'un traçage manuel des personnes (présümées) infectées et de leurs contacts.
- La deuxième finalité consiste à permettre aux équipes mobiles et aux inspections d'hygiène compétentes des Communautés de prendre des initiatives visant à prévenir l'extension des effets néfastes causés par les maladies infectieuses conformément aux missions réglementaires qui leur sont dévolues.
- La troisième finalité consiste à permettre la réalisation d'études scientifiques ou statistiques sur la lutte contre la propagation du coronavirus et/ou afin de soutenir la politique de santé publique dans le domaine de la lutte contre le coronavirus.

Dans son avis n° 64/2020 relatif à l'accord de coopération²¹⁹, l'APD paraît sensible à l'effort fourni par les auteurs du texte et constate que ces finalités sont toutes légitimes. Elle émet néanmoins une réserve :

« La légitimité de la finalité qui consiste à contacter les médecins traitants des personnes (présümées) infectées afin de les informer de la contamination (présümée) des personnes de catégories II [personnes qui ont réalisé un test de dépistage du Covid-19] et III [personnes présümées infectées] sans que leur consentement ait été obtenu, n'apparaît pas de manière évidente à l'Autorité. En effet, l'Autorité se demande s'il est bien légitime que les médecins traitants de ces personnes soient informés de leur condition médicale, y compris si celles-ci ne souhaitent pas partager cette information avec leur médecin traitant. Si l'objectif est de prévenir ces médecins afin de les protéger contre le risque de contamination lors d'une prochaine visite, ceci devrait être précisé »²²⁰.

En outre, elle invite dans son avis l'auteur du projet à clarifier certains aspects et notamment la rédaction de certaines finalités, afin qu'elles puissent être considérées comme étant suffisamment « déterminées, explicites et légitimes »²²¹ et, à titre exemplatif, énonce ce qui suit :

« Ensuite, en ce qui concerne la rédaction actuelle des finalités : premièrement, comme l'Autorité l'a déjà souligné *supra*, il convient de clarifier les conditions

²¹⁹ APD, avis 64/2020, du 20 juillet 2020, 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 (présümées) infectées par le coronavirus Covid-19 sur la base d'une base de données auprès de Sciensano, disponible à l'adresse : www.autoriteprotectiondonnees.be/publications/avis-n-64-2020.pdf; consulté en dernier lieu le 20 octobre 2020.

²²⁰ APD, avis 64/2020, *op. cit.*, p. 10, § 29.

²²¹ *Ibid.*, pp. 10 et 11, § 30.

et les circonstances dans lesquelles “une visite physique” peut avoir lieu dans le cadre du suivi manuel des personnes (présumées) infectées et de leurs contacts. [...] Le projet devrait déterminer, de manière exhaustive, les raisons pour lesquelles les centres de contact peuvent traiter les données à caractère personnel reprises dans la base de données III (qui sont, elles-mêmes, issues de la base de données I). Il convient donc de supprimer les termes “entre autres” dans l’article 3 § 1^{er}, 2.A du projet et de prévoir, dans le projet, toutes les raisons pour lesquelles les centres de contact pourront utiliser les données à caractère personnel visées dans la disposition en projet et contacter les personnes concernées. Il en est de même pour les mots “entre autres” repris dans l’article 3 § 2, 2.A du projet. [...] Il conviendrait de préciser ce qu’il faut entendre par “suivi” (quels sont la nature et l’objet de ce suivi ? S’agit-il d’un contrôle *a posteriori* du respect des “recommandations” fournies ? Est-il obligatoire ? Ce suivi implique-t-il des mesures contraignantes ?) [...]».

Les finalités jouent un rôle important, dans le contrôle de proportionnalité et l’établissement de la base de licéité. Si elles s’avèrent peu précises, l’ensemble du traitement peut se trouver alors entaché d’illégalité.

b. Le principe de licéité

55. Rappel des principes autour de la question de la notion de «loi».

Les finalités étant définies, il est possible de déterminer la base de licéité des traitements qui interviennent à l’occasion de la mise en œuvre du *tracing* manuel et automatique. À cet égard, rappelons les balises mises en place par l’article 52 de la Charte. La première est l’exigence d’une «loi» claire, précise et dont le contenu est facilement accessible. Cette balise soulève d’emblée une question : le consentement est-il une base suffisante pour permettre le traitement de données à caractère personnel²²² et sinon, quelle est la raison de son exigence à la base des deux modes de *tracing* (*infra*, n°) ?

La réponse proposée par le CEPD est peu claire. Après avoir estimé qu’en principe, seul le fondement de la tâche d’exécution d’une mission d’intérêt général pouvait être retenu, lorsque le *tracing* est mis en place par une autorité publique, le CEPD laisse entendre que :

«However, if the data processing is based on another legal basis, such as consent (Art. 6(1)(a)) for example, the controller will have to ensure that the strict requirements for such legal basis to be valid are met»²²³.

²²² Soulignons en outre qu’il peut s’agir de donnée de santé, si l’enregistrement volontaire porte sur le fait que la personne enregistrée est porteuse du virus. Dans ce cas, il est important que le consentement, conformément aux exigences du RGPD, soit spécifique. En ce qui concerne les personnes rencontrées par le porteur, on s’interroge dans la mesure où, si l’infection est une simple probabilité, la donnée enregistrée les concernant notera : «personne susceptible d’être affectée par le virus».

²²³ «When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest» (EDPB, *Guidelines 04/2020, op. cit.*, n° 31)

Il n'en demeure pas moins, que dans le cas d'une application à vocation générale pour tous les citoyens, la décision « légale » de l'autorité publique non seulement est la « base la plus appropriée », selon l'expression du CEPD, mais peut seule être retenue comme fondement des traitements institués. En matière de *tracing* manuel²²⁴, la base de licéité pour l'utilisation de l'application automatique de *tracing* est également la mission d'intérêt public fondée sur la loi, le décret ou l'ordonnance²²⁵.

Si seule la « loi » peut valoir²²⁶, la notion de « loi » s'entend, au sens de la Convention européenne, de la Charte et du RGPD, de manière très large. Elle se conçoit, comme nous l'avons dit (*supra*, section 1, § 2, A, 1.), selon la jurisprudence de la Cour européenne²²⁷, de tout acte réglementaire pris conformément aux règles constitutionnelles, voire par une jurisprudence bien établie et suffisamment connue²²⁸. En Belgique, l'article 22 de la Constitution, qui consacre le droit à la vie privée²²⁹, réserve explicitement aux pouvoirs législatifs le soin d'apporter des restrictions à ce droit fondamental²³⁰ et donc exige une loi au sens matériel du terme. Un arrêté royal de pouvoirs spéciaux suffisait-il à fonder la mise sur pied du *tracing*? Il est en tout cas regrettable que les premiers arrêtés royaux²³¹ n'aient pas été examinés, vu l'« urgence », par le Conseil d'État.

²²⁴ Arrêté royal n° 18, du 4 mai 2020, portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19, préc.

²²⁵ 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 (présümées) infectées par le coronavirus Covid-19 se fondant sur une base de données auprès de Sciensano, M.B., 15 octobre 2020.

²²⁶ Sur la notion de « loi » et ses qualités, voy. Fr. SUDRE, *Droit européen et international des droits de l'homme*, 14^e éd., Paris, PUF, 1989, pp. 204 et s.

²²⁷ « les mots "prévus par la loi" [...] veulent d'abord que la mesure incriminée ait une base en droit interne, mais ils ont aussi trait à la qualité de la loi en cause » (Cour eur. D.H., arrêt *Kruslin c. France*, 24 avril 1990, n° 5, § 27). En particulier, la jurisprudence de Strasbourg exige que la base légale réponde au principe de sécurité juridique, ce qui lui permet d'accueillir l'ensemble du droit en vigueur, qu'il soit législatif, réglementaire, voire jurisprudentiel, à condition qu'elle soit accessible, précise et prévisible.

²²⁸ À cet égard, on peut citer le cas *Ben Faiza c. France* jugé en 2018 par la Cour de Strasbourg (n° 31446/12, jugement du 8 février 2018) à propos d'un système de géolocalisation mis en place par le ministère de l'Intérieur français où le gouvernement français objectait que le manque de précision de la loi était compensé par un arrêt de la Cour de cassation. La Cour refusa l'argument.

²²⁹ Sur cet article de la Constitution, voy. E. DEGRAVE et Y. POULLET, « Le droit au respect de la vie privée face aux nouvelles technologies », in M. VERDUSSEN (dir.), *Les droits constitutionnels en Belgique*, Bruxelles, Bruylant, 2011.

²³⁰ Fr. BOUHON, A. JOSTEN, X. MINY et E. SLAUTSKY, « L'État belge face à la pandémie de Covid-19 : esquisse d'un régime d'exception », *op. cit.*, p. 16; dans le même sens, S. VAN DROOGHENBROECK et C. RIZCALLAH, « Le principe de la légalité des limitations aux droits et libertés », in L. DETROUX, M. EL BERHOUMI et B. LOMBAERT (dir.), *La légalité. Un principe de la démocratie belge en péril?*, Bruxelles, Larcier, 2019, pp. 23-69.

²³¹ Ce qui n'a pas empêché les discussions à la Chambre lors de sa réunion du mardi 28 avril 2020 et les questions parlementaires (par exemple lors de la séance plénière du jeudi 23 avril (questions au ministre

56. Quid de l'exigence de consentement? Enfin, si le CEPD exige une « loi » pour encadrer le système de *tracing*, dans le même temps, il réclame que la « loi » renvoie au consentement spécifique de l'individu dans la mise en œuvre des mesures²³², en ce qu'il dispose que :

« The legal basis or legislative measure that provides the lawful basis for the use of contact tracing applications should, however, incorporate meaningful safeguards including a reference to the voluntary nature of the application »²³³.

Cette conception privilégie, au nom de la valeur de l'autonomie ou de « self-determination » des sujets, consacrée par l'article 8 de la CEDH, la possibilité de choix de l'individu, qui permet et accrédite la confiance en la technologie. Il ne s'agit pas de fonder ainsi le *tracing* mais d'en faire une condition de son application aux personnes. L'appel au consentement en cas de *tracing* automatique est également justifié par la référence nécessaire en la matière à la directive *e-Privacy*²³⁴. Cette directive, d'une part, en ses articles 6 et 9²³⁵, exige en effet que toute transmission des données de géolocalisation par les opérateurs aux autorités publiques requiert le consentement des personnes concernées et, d'autre part, en son article 5.3, interdit, sauf consentement du possesseur d'un terminal, l'introduction de logiciels pouvant transmettre à un tiers des informations relatives à ce possesseur ou à un utilisateur du terminal²³⁶.

En résumé, la base légale est donc la loi, mais cette dernière prévoit explicitement le consentement comme condition de son application. Nous ajoutons

de Backer), (CRIV, Ch. repr., 2^e session de la 55^e législature 2019-2020, pp. 26 et s.) et le souhait exprimé par de nombreux parlementaires d'un débat parlementaire sur le contenu même des décisions. Sur ce point, cf. également, les réflexions de Th. LÉONARD, « *Tracing des citoyens comme stratégie de déconfinement* : les balises du Comité Européen de Protection des données (CEPD/EDPB) et de la Cnil », disponible à l'adresse : www.droit-technologie.org/actualites/tracing-des-citoyens-comme-strategie-de-deconfinement-les-balises-du-comite-europeen-de-protection-des-donnees-cepd-epdb-et-de-la-cnil/). Sur l'ensemble des débats menés à la Chambre, voy. l'excellent panorama proposé dans le *Courrier hebdomadaire du CRISP*, par Fr. BOUHON, A. JOUSTEN, X. MINY et E. SLAUTSKY, « L'État belge face à la pandémie de Covid-19 : esquisse d'un régime d'exception », *op. cit.*

²³² Le rapport d'experts nommés par la Commission pour étudier les bases d'une politique de partage des données entre le secteur privé et le secteur public estimait que le consentement des citoyens pour une transmission aux autorités publiques de leurs données collectées par des entreprises privées pourrait être une base légale suffisante pour justifier la création de « big data » dont l'exploitation servirait l'intérêt général. Le rapport parle de « consentement altruiste », in *Towards a European strategy on business-to-government data sharing for the public interest*, Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing, 19 février, 2020. La Commission européenne a présenté, ce même 19 février, ce document comme un des éléments de sa stratégie en matière de données.

²³³ EDPB, *Guidelines 04/2020*, *op. cit.*

²³⁴ La directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques (2002/58) dite directive *e-Privacy* (en anglais, *Directive on Privacy and Electronic Communications*), modifiée en 2009 et actuellement en cours de révision, est une directive européenne qui vise à protéger de façon spécifique la vie privée sur Internet.

²³⁵ EDPB, *Guidelines 04/2020*, *op. cit.*, n° 10.

²³⁶ Ainsi, on pourrait imaginer que la liste des contacts établie par une personne concernée contaminée soit transmise par un réseau social et croisée avec les données de déplacement pour déterminer les personnes à risque ; EDPB, *Guidelines 04/2020*, *op. cit.*, n° 15.

que ce consentement ne peut être conditionné par aucun avantage. Le rapport au Roi de l'arrêté n° 44 le rappelle :

« Ce cadre juridique est nécessaire mais ne doit pas être confondu avec le libre choix du citoyen d'installer, d'utiliser et de désinstaller une application numérique de traçage de contacts. Le présent arrêté fixe le cadre des garanties techniques et relatives aux droits humains qu'une application numérique de traçage de contacts doit respecter, mais n'impose en aucun cas au citoyen l'obligation d'installer, d'utiliser ou de désinstaller une application numérique de traçage de contacts. Sur la recommandation de l'APD dans son avis 34/2020, il est également précisé qu'un (non-)utilisateur ne peut subir aucun désavantage ou avantage de quelque manière que ce soit selon qu'il utilise ou non une application numérique de traçage de contacts. Toutefois, l'application numérique de traçage de contacts sera assortie de conditions d'utilisation en vertu desquelles l'utilisation illicite sera sanctionnée à la fois contractuellement et selon les règles du droit commun ».

c. Principes de transparence et de loyauté : la clarté et la précision

57. Rappel des exigences de la transparence des traitements et de leur caractère loyal. Les textes normatifs qui prévoient et encadrent l'utilisation de ces outils doivent notamment être précis et complets pour assurer une transparence optimale vis-à-vis du citoyen. La jurisprudence de la Cour européenne des droits de l'homme²³⁷ a souvent eu l'occasion de se prononcer à propos de la clarté et du degré de précision exigés des « lois » limitant nos *libertés* individuelles afin de rendre prévisibles au citoyen (critère de la « prévisibilité » [*foreseeability*]) les atteintes à la protection de ses données. Elle l'a fait dans un domaine proche de celui visé par les mesures de *tracing* automatique, à savoir à propos d'écoutes téléphoniques : « Les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance. L'existence de règles claires et détaillées apparaît indispensable, d'autant que les procédés techniques ne cessent de se perfectionner »²³⁸. Parmi les précisions attendues, l'arrêt *Rotaru*²³⁹ dénombre : 1) la définition précise de la ou les finalités, 2) les personnes concernées, 3) les catégories de données traitées, 4) le responsable du traitement, 5) les destinataires du traitement, 6) les mesures de sécurité, 7) la durée de conservation des données. Cette transparence est également exigée par le RGPD à travers tant

²³⁷ Cf., notamment, Cour eur. D.H., arrêts *Szabo et Vissy c. Hongrie*, 12 janvier 2016, n° 37138/14 ; *Kopp c. Suisse*, 25 mars 1998 ; *Benedik c. Sloveenie*, 24 avril 2018, n° 588/13 ; *Roman Zakharov c. Russie*, 4 décembre 2015, n° 47143/06.

²³⁸ Cour eur. D.H., arrêts *Kruslin c. France* et *Huvig c. France* 24 janvier 1999, resp. n° 11801/85 et n° 11105/84. Sur les exigences de la Cour européenne des droits de l'homme, voy. notamment, la jurisprudence reprise par P. WACHSMANN, « Le droit au secret de la vie privée », in Fr. SUDRE (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, coll. Droit et Justice, n° 63, Bruxelles, Bruylant, 2005, pp. 128 et s.

²³⁹ Cour eur. D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000, n° 28341/95. L'avis n° 36 reprend ces divers éléments pour souligner les lacunes du projet d'arrêté royal dont seules certaines ont pu être comblées.

des exigences de clarté et d'accessibilité imposées aux « lois » qui encadrent les systèmes, que par les multiples obligations d'information mises à charge du responsable du traitement²⁴⁰. De fait, comment prendre la mesure de ce qui serait bien et bon si nous ignorons les tenants et les enjeux de nos débats ?

Au-delà de ce débat général, le RGPD institue également une transparence des traitements vis-à-vis des personnes concernées par ceux-ci. Les articles 13 et 14 exigent une information sur les caractéristiques principales du traitement : qui est responsable²⁴¹ ? Pour quelles finalités ? Quelles données sont traitées ? Si la collecte vient d'un tiers²⁴², quelles sont les sources ? À qui sont-elles destinées ? À qui se plaindre ? En particulier, on mentionnera l'information relative aux coordonnées du détaché à la protection des données²⁴³, l'existence d'un droit d'accès à toutes les données, non seulement celles de base, mais également les données résultats des traitements ayant trait à la personne concernée (par exemple, la forte probabilité de la contagion, la présence de personnes infectées dans l'entourage) sous réserve que la communication ne mette pas en cause les intérêts et droits d'autrui. Les deux articles prévoient, en outre, que si le traitement aboutit à une décision, le responsable du traitement donne les informations « sur la logique sous-jacente ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ». Dans le cas du traçage, il sera utile pour la personne contactée de connaître ce qui a présidé à la décision de la contacter, les critères utilisés pour la considérer comme suspecte et les conséquences que cette alerte signifie pour elle (obligation d'aller se faire dépister, obligation de se confiner...).

58. L'application du principe aux traitements de *tracing*. Il s'ensuit que les avis de l'APD n° 36²⁴⁴ et n° 64²⁴⁵ rappellent que :

« [...] toute norme encadrant des traitements de données à caractère personnel, en particulier lorsque ceux-ci constituent une ingérence importante dans les

²⁴⁰ Art. 12, 13 et 14, du RGPD.

²⁴¹ En l'occurrence, l'arrêté royal désigne pour cette tâche Sciensano. Selon l'avis n° 34 de l'APD (avis déjà cité), « [...] si c'est Sciensano qui agit en tant que responsable des traitements visés par le présent projet d'arrêté, il lui appartient d'assumer les responsabilités qui lui incombent en cette qualité, en ce compris : de faire le choix de/des applications qui seront proposées ; de conclure les instruments contractuels nécessaires avec les sous-traitants de données (*ndla* : ce point est particulièrement important, sachant l'incapacité de Sciensano de développer elle-même les applications. Il importe donc que le nom du sous-traitant soit connu et que les applications qu'il développera soient proprement auditées) ; de garantir le respect du présent arrêté... ; de vérifier que ce soit toujours le cas suite à d'éventuelles mises à jour de ces applications ; de réaliser une analyse d'impact (AIPD) ».

²⁴² Sur ce point, on souhaiterait avec l'APD que le nom de la personne qui a livré le nom de ses contacts ne soit divulgué à ces derniers qu'avec le consentement exprès de la première.

²⁴³ L'arrêté royal prévoit la nomination pour les traitements générés par l'arrêté royal, la désignation d'un détaché *ad hoc* (art. 4, § 3, al. 2).

²⁴⁴ APD, avis n° 36/2020 du 29 avril 2020 concernant un avant-projet d'arrêté royal n° XXX 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).

²⁴⁵ APD, avis n° 64/2020, *op. cit.*

droits et libertés des personnes concernées, doit répondre aux exigences de prévisibilité et de précision de sorte *qu'à sa lecture, les personnes concernées puissent entrevoir clairement les traitements qui sont faits de leurs données et les circonstances dans lesquelles ces traitements de données sont autorisés*. En exécution de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, *les éléments essentiels du traitement doivent y être décrits avec précision*. Il s'agit, en particulier, de la ou des finalité(s) précise(s) du traitement; de l'identité du (ou des) responsable(s) du traitement; des catégories de données traitées, étant entendu que celles-ci doivent s'avérer – conformément à l'article 5.1. du RGPD, “adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées”; des catégories de personnes concernées (personnes à propos desquelles des données seront traitées); de la durée de conservation des données; des destinataires ou catégories de destinataires auxquels leurs données sont communiquées et les circonstances dans lesquelles et les raisons pour lesquelles elles seront communiquées ainsi que toutes mesures visant à assurer un traitement licite et loyal de ces données à caractère personnel».

Ces dispositions du RGPD visent à une information de chaque personne concernée. Il est patent qu'au-delà de cette approche liée à une protection individualiste, les gouvernements, sous la pression citoyenne, ont souhaité élargir à l'ensemble des citoyens le devoir d'information sur l'étendue des mesures prises et leur respect des libertés.

59. De la transparence à la personne concernée à une transparence vis-à-vis de la population et à une consultation publique. En l'occurrence, il s'agit d'éclairer le citoyen, tout citoyen, sur les enjeux d'un débat qui est certes technique, mais surtout, et en définitive, politique, au sens de conduite de la cité. Quelles solutions technologiques? Quelles alternatives? Quels acteurs derrière chaque solution? Qui gère le système, avec quelles données et comment? Ainsi, quand on parle de solution *Bluetooth*, il importe de savoir pour quelle population cette solution convient ou plutôt quelle population en sera exclue et dans ce cas, quels remèdes prévoir? Avec quels risques d'erreurs? Quels succès rencontrent les mesures prises? C'est un devoir de l'État²⁴⁶ de fournir cette information, non seulement pour permettre au citoyen de décider mais à la fois pour répondre aux demandes et inquiétudes de tous bords et permettre aux autorités publiques, Parlement en tête, de jouer leur rôle d'arbitre au regard des enjeux multiples soulevés par les mesures prises ou à prendre.

Notons, enfin, que la fourniture de toutes ces informations sur le site web de Sciensano «ne suffit pas pour que les utilisateurs potentiels des applications soient informés de manière certaine et transparente au sujet, notamment, des objectifs du système mis en place, des traitements de données auquel il donnera lieu et des parties impliquées. À propos du traçage dit automatique, une information simple et courte à ce sujet doit être fournie à l'utilisateur potentiel dans

²⁴⁶ Ou plutôt d'une commission indépendante d'experts de diverses disciplines, mise en place par l'État.

le cadre de l'opération de téléchargement de l'application. Une possibilité d'accès à une information beaucoup plus détaillée (lui permettant de comprendre le fonctionnement du système, les flux de données, ses droits, etc.) doit également être prévue et renseignée à cette occasion »²⁴⁷.

Dans un souci de légitimité, plus que de légalité, les autorités fédérales et des entités fédérées ont également procédé à une consultation publique en deux étapes²⁴⁸. Cette consultation publique est une initiative du groupe de travail interfédéral en charge du développement de l'application CORONALERT : l'application belge de traçage automatique des contacts²⁴⁹. Dans un souci de transparence, les résultats et contributions à la consultation, ainsi que les avis de confidentialité, la charte de traitements de l'application, la politique des mineurs, l'évaluation de l'impact sur la protection des données ont été établis avant le traitement, et mis à disposition sur deux sites internet. Par ailleurs, on note que l'application CORONALERT est en *open source* et que, dès lors, son fonctionnement peut être analysé par les experts y compris ceux des associations de droits civils et des libertés²⁵⁰.

On approuve les efforts importants et nécessaires qui ont été consentis afin d'assurer l'obligation de transparence, même s'il est toujours possible d'apporter des améliorations dans la communication²⁵¹. La communication et la transparence restent la clef de la confiance des utilisateurs, surtout lorsque cette utilisation est légalement prescrite sur une base volontaire. Cette transparence et dès lors cette confiance expliquent sans doute pourquoi, après seulement quinze jours de lancement, l'application a plus d'un million d'utilisateurs²⁵².

d. Principe de minimisation

60. Rappel et applications du principe. Ce principe énoncé à l'article 5 du RGPD doit guider le choix du système retenu, peu importe celui-ci : *tracing*

²⁴⁷ APD, avis 34/2020, du 28 avril 2020, p. 8, § 24.

²⁴⁸ La première du 5 au 31 août 2020, la suivante du 25 septembre au 26 octobre 2020.

²⁴⁹ Le groupe de travail est placé sous la responsabilité du Comité Interfédéral Testing/Traçage (présidé par Karine Moykens) avec des représentants et experts des entités fédérées (Régions et Communautés), Sciensano et la plateforme eHealth. Le groupe comprend trois équipes, une équipe de direction, une équipe composée d'experts techniques et juridiques, une équipe interdisciplinaire avec des experts venus du monde universitaire et industriel; voy. www.esat.kuleuven.be/cosic/sites/corona-app/fr/; consulté en dernier lieu le 20 octobre 2020.

²⁵⁰ Toutes les informations sont accessibles en suivant ce lien : <https://github.com/covid-be-app>; consulté en dernier lieu le 20 octobre 2020.

²⁵¹ Néanmoins, la partie relative aux données de la déclaration de confidentialité reste peu claire à notre sens; un schéma pourrait éventuellement clarifier le fonctionnement de l'application et l'utilisation des données à caractère personnel.

²⁵² Belga, « Coronavirus : L'application "Coronalert" téléchargée par un million de Belges », *RTBF info*, 13 mars 2020, www.rtbf.be/info/societe/detail_coronavirus-l-application-coronalert-telechargee-par-un-million-de-belges?id=10607469; « Avec son million d'utilisateurs, Coronalert devient intéressant », *L'Écho*, www.lecho.be/entreprises/technologie/avec-son-million-d-utilisateurs-coronalert-devient-interessant/10257723.html; consultés en dernier lieu le 20 octobre 2020.

automatique ou manuel²⁵³, volontaire ou obligatoire, utilisant des données agrégées ou non. On soulignera le principe de minimisation des données collectées tant dans le contenu que s'agissant de la quantité des données collectées. Seules les données réellement nécessaires aux différentes finalités du traçage pourraient être collectées et traitées par les catégories de personnes en charge de la réalisation de ces finalités.

Ainsi, en matière de *tracing* automatique, le principe de minimisation exclut, selon le CEPD, les données de localisation. Le CEPD ajoute :

« In the context of a contact tracing application, careful consideration should be given to the principle of data minimisation and data protection by design and by default :

- contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used ;
- as contact tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification ;
- the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary ».

Sur la base de ce principe, l'application de *tracing* belge, CORONALERT, fonctionne sans identification directe de personnes. Seules les informations pertinentes et absolument nécessaires suivantes sont collectées :

- « – numéros de série temporaires non personnalisés (via jetons *Bluetooth*), indispensables pour alerter de manière anonyme les utilisateurs de l'appli qu'ils sont entrés en contact avec une personne infectée ;
- résultat test labo : indispensable pour initier ou non les actions nécessaires pour alerter les contacts des risques de contamination ;
- date probable de l'infection : indispensable pour estimer d'un point de vue médical pour quels contacts il existe un risque de contamination ;
- codes de test : indispensables pour éviter que de fausses notifications (malveillantes) soient envoyées en matière de risques d'infection ;
- séjour dans un pays d'Europe : indispensable pour envoyer une notification aux personnes avec lesquelles la personne infectée a été en contact en dehors de la Belgique »²⁵⁴.

²⁵³ Il est clair que le *tracing* manuel pose des problèmes certes différents mais tout aussi sérieux en matière de protection des données. Le fait que les données soient reçues et gérées par un personnel non qualifié même si placé sous la surveillance, en Wallonie, du personnel de l'AWIQ soulève des craintes légitimes. Actuellement, deux décrets et une ordonnance des Régions et Communautés sont venus préciser les modes de traitement dans le cadre de ce *tracing* manuel qui avait démarré sans règles. À cet égard, on rappellera, et ce n'est pas pour faciliter les décisions, que les questions de vie privée restent du ressort du fédéral, alors que la gestion ressort du niveau régional.

²⁵⁴ *Application de traçage des contacts – Belgique. Analyse d'impact relative à la protection des données (AIPD), op. cit.*

Enfin, l'application ne traite aucune donnée de localisation (GPS) des utilisateurs individuels pour mesurer la proximité entre personnes²⁵⁵ et le système ne stocke pas non plus les adresses IP des utilisateurs²⁵⁶.

- e. Principes de proportionnalité et de nécessité de la loi dans une société démocratique

61. Des exigences clés des textes en matière de droits de l'homme.

Ces deux exigences découlent d'une lecture combinée des principes de finalité et de minimisation des traitements. La nécessité et la proportionnalité du traitement au regard de l'objectif poursuivi doivent impérativement être assurées afin de ne pas entraîner son illégalité et la violation des droits fondamentaux de ses utilisateurs. La Cour de Strasbourg précise que la notion de « nécessité » au sens de l'article 8 impliquait une ingérence fondée sur un besoin social impérieux et, notamment, proportionnée au but légitime recherché. Si la Cour laisse aux autorités nationales une marge d'appréciation, celles-ci se devront de démontrer l'existence d'un besoin social impérieux qui justifie l'ingérence²⁵⁷. Le critère de nécessité et le besoin de justification se retrouvent dans nombre des documents publiés par les organes en charge de la protection des données. Ainsi, pour reprendre les termes de l'APD dans son avis n° 34/2020²⁵⁸ :

« Pour rappel, un traitement de données à caractère personnel est considéré comme étant nécessaire s'il constitue la mesure la moins attentatoire pour atteindre l'objectif (d'intérêt général) qu'il poursuit. Il faut donc, premièrement, que le traitement de données permette effectivement d'atteindre l'objectif poursuivi. Il faut donc démontrer, sur base d'éléments factuels et objectifs, l'efficacité du traitement de données à caractère personnel pour atteindre l'objectif recherché ; deuxièmement, que ce traitement de données à caractère personnel constitue la mesure la moins intrusive au regard du droit à la protection de la vie privée. Cela signifie que s'il est possible d'atteindre l'objectif recherché au moyen d'une mesure moins intrusive pour le droit au respect de la vie privée ou le droit à la protection des données à caractère personnel, le traitement de données initialement envisagé ne pourra pas être mis en place. Il faut, à cette fin, détailler et être en mesure de démontrer, à l'aide d'éléments de preuves factuels et objectifs, les raisons pour lesquelles les autres mesures moins intrusives ne sont pas suffisantes pour atteindre l'objectif recherché. Si la nécessité du traite-

²⁵⁵ « [L]e souci de réduire l'ingérence à ce qui est véritablement nécessaire et proportionné conduit à privilégier les systèmes enregistrant les données de proximité (s'appuyant sur la technologie *Bluetooth*) plutôt que les données de localisation (GPS). Les APD autrichienne, tchèque et italienne ont en général recommandé le traitement de données de localisation anonymisées. En revanche, selon l'APD néerlandaise, l'anonymisation des données de localisation n'est pas vraiment possible, car il est très probable que les individus puissent être réidentifiés » (Y. POULLET, « Pandémie, numérique et droits de l'homme – un étrange cocktail ! », *op. cit.*).

²⁵⁶ *Ibid.*

²⁵⁷ En ce sens, notamment, Cour eur. D.H., arrêt *Piechowicz c. Pologne*, 17 avril 2012, n° 20071/07, § 212. Sur la marge d'appréciation laissée aux États : Gde Ch., arrêt *Paradiso et Campanelli c. Italie*, 24 janvier 2017, n° 25358/12, §§ 179-184.

²⁵⁸ APD, avis 34/2020, du 28 avril 2020, *op. cit.*

ment de données à caractère personnel est démontrée, il faut encore démontrer que celui-ci est proportionné (au sens strict) à l'objectif qu'il poursuit, c'est-à-dire qu'il faut démontrer qu'il existe un juste équilibre entre les différents intérêts en présence, droits et libertés des personnes concernées. En d'autres termes, il faut qu'il y ait un équilibre entre l'ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel et l'objectif que poursuit – et permet effectivement d'atteindre – ce traitement. Les avantages qui découlent du traitement de données en question doivent donc être plus importants que les inconvénients qu'il génère pour les personnes concernées».

On retrouve la même préoccupation dans le «Statement» récemment publié par la présidente du Comité consultatif de la Convention n° 108 du Conseil de l'Europe et le DPO de la même institution²⁵⁹ :

«Although technological tools can play an important role in addressing the current challenge, the first – essential – question we have to ask ourselves before systematic and uncritical adoption of technology (not having assessed their effectiveness and proportionality) is: Are those “Apps” the solution? Considering the absence of evidence of their efficacy, are the promises worth the predictable societal and legal risks?»

On rappelle certes qu'il existe une marge de manœuvre des États dans l'appréciation de ce caractère nécessaire. La jurisprudence de la Cour de Strasbourg²⁶⁰ estime en particulier que cette marge est ample lorsque l'État doit ménager un équilibre entre des intérêts privés et des intérêts publics concurrents ou entre différents droits protégés par la Convention qui se trouvent en conflit (en l'occurrence, notamment le droit à la vie et le droit à la protection des données). La Cour de justice de Luxembourg suit une jurisprudence similaire tant sur l'exigence de vérifier le caractère nécessaire que sur la marge de manœuvre à reconnaître aux États :

«À cet égard, il convient de rappeler que le principe de proportionnalité exige, selon une jurisprudence constante de la Cour, que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs [...]. En ce qui concerne le contrôle juridictionnel du respect de ces conditions, dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre

²⁵⁹ *Statement* ou déclaration déjà citée à la note 8. Cf. dans le second texte du Conseil de l'Europe, l'insistance sur ce besoin d'évaluer la nécessité ou plus-value des applications envisagées : «Le traitement à grande échelle des données à caractère personnel ne peut être effectué que lorsque, sur la base de preuves scientifiques, les avantages potentiels pour la santé publique d'une telle surveillance numérique des épidémies (par exemple, le suivi des contacts), y compris leur exactitude, l'emportent sur les avantages d'autres solutions alternatives qui seraient moins intrusives», www.coe.int/fr/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter; consulté en dernier lieu le 20 octobre 2020

²⁶⁰ En particulier, les arrêts *Fretté c. France*, 26 février 2002, n° 36515/97, § 42 ; *Odièvre c. France*, 13 février 2003, n° 42326/98, §§ 44-49 ; (Gde Ch.) *Evans c. Royaume-Uni*, 10 avril 2007, n° 6339/05, § 77 ; *S.H. et autres c. Autriche*, 3 novembre 2011, n° 57813/00, § 94.

d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci (voy., par analogie, en ce qui concerne l'article 8 de la CEDH, arrêt Cour EDH, *S et Marper c. Royaume-Uni* [GC], n^{os} 30562/04 et 30566/04, § 102, CEDH 2008-V)²⁶¹.

62. Application aux *tracings*. Il s'ensuit qu'il est important de démontrer, tant que faire se peut, la plus-value et, au-delà, la nécessité des modalités de *tracing* mises en œuvre, renvoyant à diverses conceptions du bénéfice attendu du système technologique. Il importe de ne pas privilégier outre mesure l'un ou l'autre point de vue, du moins dans un premier temps, mais d'envisager la pluralité de ceux-ci avant toute décision. La plus-value se mesure, d'abord, en termes de santé publique et suppose la comparaison de diverses méthodes technologiques mais également non technologiques. Il importe de se méfier de ce que la CNIL appelle le « solutionnisme technologique »²⁶².

Cette plus-value s'apprécie aussi en termes économiques lorsqu'il s'agit des coûts liés directement ou indirectement à la mise en place et au fonctionnement du *tracing*, mais également lorsqu'on calcule l'impact sur l'activité économique de la persistance de la pandémie. Elle s'évalue également en termes de bien-être psychologique de la population. À cet égard, certains mettent en doute l'opportunité et la nécessité du traçage automatique sur base volontaire dans la mesure où seuls 20 % de la population suivraient la recommandation et se porteraient volontaires alors qu'une couverture de 60 % serait nécessaire²⁶³ pour l'efficacité du système. D'autres arguments sont évoqués à l'encontre du système. Ainsi, on avance que le retraçage des contacts grâce à la technologie *Bluetooth* présente quelques lacunes : on cite, premièrement, les faux négatifs, c'est-à-dire des contacts qui auraient dû être pris en compte et ne l'ont pas été par exemple du fait que le *Bluetooth* était désactivé, que la personne n'avait pas pris son GSM ou que la distance prise en considération par le *Bluetooth* (soit 1,50 m) est insuffisante en particulier dans les lieux où fonctionne un conditionnement d'air, etc. ; en deuxième lieu, les faux positifs, c'est-à-dire des contacts pris en compte alors qu'ils n'auraient pas dû l'être, plaisantins ou per-

²⁶¹ CJUE, 8 avril 2014, *Digital Rights c. Irlande*, aff. jtes C-293/12 et C-594/12.

²⁶² CNIL, « Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée "StopCovid" », disponible à l'adresse : www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid : « Dans son avis, la CNIL rappelle que l'utilisation d'applications de recherche des contacts doit s'inscrire dans une stratégie sanitaire globale et appelle, sur ce point, à une vigilance particulière contre la tentation du "solutionnisme technologique". Elle souligne que son efficacité dépendra, notamment, de sa disponibilité dans les magasins d'application (*appstore*, *playstore*...), d'une large adoption par le public et d'un paramétrage adéquat ».

²⁶³ Ceci est à nuancer. Selon Cédric O, reprenant les travaux d'épidémiologistes anglais dans une rubrique publiée sur le site <https://medium.com/@cedric.o/stopcovid-ou-encore-b5794d99bb12>, « Pour être plus précis, ce qu'avancent les travaux de Christophe Fraser, c'est qu'à elle seule et sans autre mesure, l'application permettrait de juguler l'épidémie à partir d'un taux d'adoption de 60 % ; à l'inverse, dans un bassin de population comme une ville, l'application commence à être efficace à partir de quelques pourcents, ce qui devrait être précisé dans les jours à venir » ; consulté en dernier lieu le 20 octobre 2020.

sonnes déclarant être affectées sans l'être réellement, présences prises en compte par le *Bluetooth* alors que les risques n'existent pas, par exemple : croisement de deux rames de métro. Tous ces défauts remettent-ils en question le choix du *tracing* automatique ?

On ajoute que « l'expérience montre à ce sujet que les pays précurseurs du recours aux moyens numériques pour lutter contre le coronavirus, comme la Chine, Taiwan ou la Corée du Sud, ne retirent quelque efficacité de l'usage des technologies qu'en inscrivant soigneusement ce dernier au sein d'une politique de gouvernance beaucoup plus globale et multidimensionnelle de la crise, où la participation sociale et politique des communautés et des corps intermédiaires, entre l'individu et l'État, permet un contrôle continu de l'efficacité de l'outil numérique et son adaptation aux besoins humains de la lutte contre la pandémie »²⁶⁴.

f. Principe de sécurité adéquate

63. Le principe. L'article 32 du RGPD stipule : « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- a) la pseudonymisation et le chiffrement des données à caractère personnel ;
- b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ».

64. L'application du principe. Il revient dès lors à l'autorité en charge de l'application d'assurer un niveau aussi important que possible de sécurité technique, mais également organisationnelle. En ce sens, le DPIA de l'application CORONALERT informe que l'application a été conçue, construite, et est

²⁶⁴ J.-L. DAVET, E. SALOBIR *et al.*, « Élaboration et gouvernance des solutions technologiques pour une sortie de crise sanitaire », Human technology Foundation, disponible à l'adresse : http://optictech-nology.org/images/Élaboration_et_gouvernance_des_solutions_technologiques_pour_une_sortie_de_crise_sanitaire_6-3.pdf. Cette étude belgo-franco-québécoise, à la rédaction de laquelle j'ai participé, esquisse, à partir de la description de quelques systèmes de *tracing*, quelques réflexions relatives à une gouvernance éthique des différentes méthodes susceptibles d'être utilisées dans le cadre du de confinement.

aujourd'hui hébergée et entretenue avec la sécurité comme une des principales priorités²⁶⁵. Parmi ces mesures, la pseudonimisation apparaît en bonne place et constitue une mesure de sécurité largement appuyée par le Règlement. Le choix d'un encryptage avec une double clé (double hachage) de lecture assure un niveau élevé de protection.

Ensuite, on notera que la mise en place de l'architecture de l'application se fonde sur le principe «security by design», et que «les serveurs sont établis en Europe, à Francfort, les “Data at rest” sont cryptées (AES-256), les “Data in transit” sont toujours cryptées (TLS), seules des données pseudonymisées sont stockées sur les systèmes *back-end*. Le code de 15 chiffres donnant accès aux résultats d'un test et permettant à la personne concernée de recevoir son résultat ne contient aucune donnée pouvant être ramenée à l'utilisateur ou à son téléphone, ce code de 15 chiffres est supprimé du *back-end* dès que l'utilisateur a reçu le résultat de son test, les informations sont supprimées des systèmes de *back-end* une fois qu'elles ne sont plus nécessaires (une fois que l'utilisateur a reçu ses résultats ou au plus tard 14 jours après la date probable de l'infection)»²⁶⁶.

Enfin, pour limiter au maximum les risques pour les personnes concernées, les données stockées dans la base de données centrale ne peuvent pas être corrélées ou accessibles aux autres bases de données et des audits sont programmés à propos du fonctionnement de l'application. On ajoute que la base des données résultant du *tracing* automatique est soigneusement cloisonnée par rapport aux autres bases de données.

g. Principe de rétention minimale

65. Rappel du principe – Deux questions. De la durée des bases de données, on distinguera la durée de conservation des données inscrites dans les bases de données. Même si la tentation de conserver les données récoltées par les systèmes technologiques mis en place afin de combattre l'urgence du moment est grande, et souvent justifiée par les besoins de suivi des patients et de recherche statistique ou scientifique, il n'empêche que les données ne peuvent être conservées au-delà des risques que présente le patient atteint ou suspecté de pouvoir être atteint soit pendant une durée limitée à quelques semaines; les données doivent ensuite être effacées ou anonymisées²⁶⁷.

Au-delà des limites de conservation des données se pose la question des bases de données elles-mêmes, sachant qu'elles ont été créées pour lutter contre la pandémie et n'ont pas vocation à devoir être maintenues au-delà. La durée des traitements est un point important et cette durée strictement limitée à la

²⁶⁵ Application de traçage des contacts – Belgique. Analyse d'impact relative à la protection des données (AIPD), *op. cit.*, p. 30.

²⁶⁶ *Ibid.*, pp. 28 et s.

²⁶⁷ CNIL, document cité, p. 7 et EDPB, *Guidelines*, points 31 et s.

période de lutte contre la pandémie (l'état d'urgence) est et doit être inscrite dans la « loi »²⁶⁸.

66. Application des principes. L'APD a rappelé, à l'occasion de son avis n° 64/2020, qu'aux termes de l'article 5, 1., e), du RGPD, les données à caractère personnel doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées »²⁶⁹. Modifiant les écueils rencontrés dans l'arrêté royal n° 44 et à la suite des recommandations de l'APD, le texte de l'accord de coopération²⁷⁰ s'inspire de la disposition française à laquelle le Conseil constitutionnel²⁷¹ avait donné son aval.

Néanmoins, la durée de traitement par les banques de données de Sciensano fait l'objet d'une disposition peu protectrice à notre sens :

« § 2. Les données à caractère personnel pseudonymisées telles que définies à l'article 10, § 3, qui sont transmises pour la finalité de traitement définie à l'article 3, § 1^{er}, 4^o, seront supprimées conformément au délai généralement accepté pour la conservation des dossiers concernant la santé et dans le cadre de la recherche scientifique en matière de santé, à savoir trente ans »²⁷².

²⁶⁸ APD, avis 64/2020, *op. cit.*

²⁶⁹ APD, avis 64/2020, *op. cit.*

²⁷⁰ *L'article 15 de l'accord de coopération* (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'inspections 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, M.B., 15 octobre 2020) détermine sur base de ce principe, les durées de conservation des données reprises dans les différentes bases de données créées en fin du *tracing*, comme suit : « § 1^{er}. Sous réserve des dispositions du paragraphe 2, les données à caractère personnel seront supprimées de la Base de données I au plus tard soixante jours après leur enregistrement. Les données à caractère personnel de la Base de données III sont supprimées quotidiennement. Après la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus Covid-19, les données à caractère personnel de la Base de données IV seront transférées aux entités fédérées compétentes pour l'exercice de leur compétence en matière de détection des maladies infectieuses, dans le cadre des compétences matérielles dans le domaine des soins de santé préventifs conformément au § 3 du présent article. Les données sauvegardées dans la Base de données V sont supprimées après trois semaines au plus tard, conformément aux dispositions de l'article 14, § 6; § 2. Les données à caractère personnel pseudonymisées telles que définies à l'article 10, § 3, qui sont transmises pour la finalité de traitement définie à l'article 3, § 1^{er}, 4^o, seront supprimées conformément au délai généralement accepté pour la conservation des dossiers concernant la santé et dans le cadre de la recherche scientifique en matière de santé, à savoir trente ans; § 3. À l'exception des données des Bases de données II et IV, les Bases de données et leur fonctionnement seront en tout cas désactivées, supprimées ou effacées par le responsable du traitement au plus tard cinq jours après le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus Covid-19. Conformément au § 1 du présent article, les données à caractère personnel dans la Base de données IV seront transférées aux entités fédérées au plus tard cinq jours après le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus Covid-19 ».

²⁷¹ Cour constitutionnelle française, décision n° 2020-800 DC du 11 mai 2020, n° 76, disponible à l'adresse : www.conseilconstitutionnel.fr/.

²⁷² Loi du 16 octobre 2009 accordant des pouvoirs au Roi en cas d'épidémie ou de pandémie de grippe, M.B., 21 octobre 2009, donc l'article 2 énonce ce qui suit : « Afin de permettre à la Belgique de se préparer et de

Le temps nous dira si notre crainte de voir les données et les bases de données conservées au-delà des exigences qu'impose le principe de proportionnalité était ou non fondée.

3. *De l'article 35 du RGPD à un «ethical assessment» du système préalable à sa mise en route*

67. L'article 35 du RGPD. En cas de traitements dits à haut risque²⁷³, l'article 35 du RGPD impose des obligations particulières d'évaluation, ce que le RGPD appelle «Analyse d'impact relative à la protection des données» (en anglais : «Privacy Impact Assessment» ci-après PIA). Parmi les traitements soumis à cette obligation, l'article 35, 3., b), inclut «le traitement à grande échelle de catégories particulières de données, visées à l'article 9, § 1, [...]». L'application de traçage utilisée par l'État, dans le cadre de la lutte contre le coronavirus, est à considérer comme une application à haut risque : elle est développée à grande échelle et concerne des données de santé²⁷⁴. En d'autres termes, que le *tracing* soit automatique ou manuel, ce PIA est dû. Le volontariat et la prohibition du traitement des données de géolocalisation étant retenus en matière de *tracing* automatique à la suite des insistance du CEPD et de l'APD, les risques diminuent d'autant. «Néanmoins, il s'agit d'établir, par la collecte de traces pseudonymes, la liste des personnes dont chaque porteur de l'application a été physiquement proche, pendant une durée circonscrite, parmi tous les porteurs de l'application. Une telle collecte, qui a vocation à s'appliquer à la plus grande partie de la population possible, doit être envisagée avec une grande prudence»²⁷⁵.

68. L'exécution de l'obligation de DPIA en Belgique et son élargissement du débat. À cet égard, la Belgique, à la demande de l'APD, en son avis n° 64/2020, n'a pas manqué de réaliser son DPIA et de le rendre public, et

réagir à une épidémie ou une pandémie de grippe qui présenterait un risque particulier et grave pour la santé publique, le Roi peut, par arrêté délibéré en Conseil des ministres, prendre les mesures visées à l'article 3 ».

L'habilitation a pris fin le 21 avril 2010, à l'expiration du délai de six mois prévu par le législateur, et ce, après la confirmation, par la loi du 23 mars 2010 de confirmation des arrêtés royaux pris en application des articles 2 et 3 de la loi du 16 octobre 2009 accordant des pouvoirs au Roi en cas d'épidémie ou de pandémie de grippe, M.B., 29 mars 2010.

²⁷³ Art. 35.1 du RGPD.

²⁷⁴ L'article 35.3, b), du RGPD considère leur traitement comme à haut risque, imposant une obligation de *privacy impact assesment*.

²⁷⁵ CNIL, «Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée "StopCovid" », *op. cit.* ; « Délibération n° 2020-051 du 8 mai 2020 portant avis sur un projet de décret relatif aux systèmes d'information mentionnés à l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire », disponible à l'adresse : www.cnil.fr/sites/default/files/atoms/files/2020-051-urgence-sanitaire.pdf. Le lecteur trouvera la liste complète et impressionnante des avis, opinions, déclarations, etc., des autorités de protection des données et autres organes nationaux et internationaux de protection des données sur le site : <https://globalprivacyassembly.org/covid-19/>. Cf. également le site très nourri de l'équipe de recherche LSTS de la VUB (Bruxelles) : « Data Protection Law and the Covid-19 outbreak », disponible à l'adresse : <https://lsts.research.vub.be/en/data-protection-law-and-the-covid-19-outbreak>.

ce, quinze jours avant la mise à disposition de l'application au grand public²⁷⁶. Suivant l'article 36, 1., du Règlement, cette analyse d'impact entraîne l'obligation de consultation de l'APD, si les mesures prises témoignent d'un risque élevé. Dans ce cas, l'APD réagira, le cas échéant, pour proposer des mesures complémentaires de réduction des risques. En l'occurrence, le DPIA de l'application n'a pas, selon les volontés des responsables et du gouvernement, nécessité de notification préalable à l'APD. Avec l'APD, nous le regrettons. Ajoutons que l'article 35, 9., du RGPD réclame, en outre, une évaluation participative, multidisciplinaire et si possible *multistakeholders* des risques²⁷⁷ et, ajoute l'article 36, « continue », afin de pouvoir à tout moment adapter le système aux évolutions de la pandémie et à sa réception par le public.

Par contre, il faut noter que la Belgique a procédé à une première consultation publique du 5 au 31 août et une seconde, suivant la publication de son DPIA²⁷⁸, du 25 septembre au 26 octobre²⁷⁹. L'article 35 ne concerne que l'évaluation de l'impact sur les libertés individuelles et la protection des données à caractère personnel. Cette application étant une application à haut risque, concernant des données de santé à caractère personnel, il est souhaitable d'élargir l'objet de l'évaluation dans la mesure où le choix du système a des implications bien plus étendues que celles portant sur la protection des données comme nous le notions déjà plus haut (*supra*, n° XX). Il y a lieu également de considérer les risques collectifs, prendre en considération des droits aussi fondamentaux que ceux liés à l'éducation, la non-discrimination, les droits des personnes âgées, le droit à la vie, etc.

Ces préoccupations débordent la question des libertés individuelles et touchent à l'intérêt général. L'évaluation des nécessités de l'intérêt général au regard de la mise en danger de nos libertés tant individuelles que collectives doit être inclusive et réunir les représentants de toutes les catégories de personnes intéressées. Il importe qu'une place soit laissée à la discussion publique au sein d'un forum réunissant toutes les parties prenantes : corps médical, représentants de la société civile (en particulier des groupes vulnérables), des entreprises, du milieu éducatif, etc. Il ne peut être question d'abandonner aux seuls experts, y compris ceux de la vie privée, la décision du choix d'un système plutôt que l'autre mais d'ouvrir à la discussion publique les choix et d'en imposer l'évaluation tant sur les plans techniques (*ethics by design*) que sur les autres plans (psychologique, socio-économique...).

²⁷⁶ Disponible à l'adresse : https://coronalert.be/wp-content/uploads/2020/09/20200915-DPIA_contactopsporingsapplicatie-Belgie-V.5_final_FR.pdf; consulté en dernier le 20 octobre 2020.

²⁷⁷ Sur cette ardente obligation du responsable d'ouvrir la consultation et la nécessité de motivation en cas de non-consultation, voy. les *Guidelines* du Groupe de l'article 29, WP 248, déjà citées, pp. 18 et 19 et surtout les Recommandations émises par la Commission belge de protection de la vie privée, n° 01/2018, pp. 31 et 32.

²⁷⁸ *Application de traçage des contacts – Belgique. Analyse d'impact relative à la protection des données (AIPD)*, *op. cit.*

²⁷⁹ Voy. www.esat.kuleuven.be/cosic/sites/corona-app/fr/; consulté en dernier lieu le 20 octobre 2020.

69. Vers un *ethical impact assesment*? Peut-être devrions-nous suivre le modèle de pays comme le Danemark, l'Allemagne²⁸⁰ ou le Royaume-Uni²⁸¹ et créer de manière générale un organe multidisciplinaire d'évaluation « éthique » des systèmes d'information présentant un haut risque, coordonnant les avis des divers organes en charge des intérêts mis en cause par ces systèmes (Autorité de protection des données, Centre d'égalité des chances, etc.). Le *eHealth Network* de la Commission européenne, mis en place récemment pour développer une médecine en ligne européenne²⁸² s'exprime également en ce sens à propos des processus de décision qui entourent la gestion de la crise, en ce compris les mesures de déconfinement²⁸³:

«The experience of several Member States that started introducing contact tracing apps shows that, in order to increase the acceptance, an integrated governance is needed to prepare and implement the measures, involving not only health, but also other authorities, as well as private sector, experts, academics, data protection authorities, etc. A wide communication model is needed, as well».

En toute clarté vis-à-vis de la population et afin d'obtenir sa confiance et la maintenir, l'autorité publique expliquera, sans paternalisme aucun, les raisons des choix posés et le contenu des décisions en ce compris les modèles utilisés y compris par les algorithmes d'intelligence augmentée éventuellement retenus, le cas échéant. À cet égard, nous ne pourrions admettre que les choix technologiques soient dictés par des acteurs qui n'opéreraient pas de manière transparente et avec le souci d'une évaluation éthique²⁸⁴. De manière spécifique à la gestion de la pandémie, les dispositions de l'article 11, VIII et IX, de la loi française sur l'évaluation, le processus à suivre et le rôle du Parlement méritent d'être prises en exemple :

«Il est instauré un Comité de contrôle et de liaison covid-19 chargé d'associer la société civile et le Parlement aux opérations de lutte contre la propagation de l'épidémie par suivi des contacts ainsi qu'au déploiement des systèmes d'information prévus à cet effet. Ce comité est chargé, par des audits réguliers :

²⁸⁰ La *Data Ethics Commission* fédérale a été mise en place le 5 septembre 2018. Elle est composée notamment de représentants de l'industrie, de représentants de l'autorité de contrôle, etc. Elle a publié récemment (octobre 2019) un rapport important sur le développement des systèmes d'intelligence artificielle, disponible à l'adresse: https://datenethikkommission.de/wp-content/uploads/191015_DEK_Gutachten_screen.pdf.

²⁸¹ À propos de la *Data Ethics and Innovation Authority* du Royaume-Uni, voy. le site de l'autorité: www.statisticsauthority.gov.uk/about-the-authority/committees/nsdec/data-ethics/.

²⁸² Décision d'exécution (UE) 2019/1765 de la Commission du 22 octobre 2019 arrêtant les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales chargées de la santé en ligne, et abrogeant la décision d'exécution 2011/890/UE, disponible à l'adresse: <https://eurlex.europa.eu/legalcontent/FR/TXT/HTML/?uri=CELEX:32019D1765&from=EN>.

²⁸³ Déclaration relative aux mesures de confinement suite à la pandémie disponible à l'adresse: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf; consulté en dernier lieu le 20 octobre 2020.

²⁸⁴ J.-L. DAVET, E. SALOIR et al., «Élaboration et gouvernance des solutions technologiques pour une sortie de crise sanitaire», *op. cit.*, p. 7. se retrouve sur le site de l'Académie royale de Belgique.

- 1° D'évaluer, grâce aux retours d'expérience des équipes sanitaires de terrain, l'apport réel des outils numériques à leur action, et de déterminer s'ils sont, ou pas, de nature à faire une différence significative dans le traitement de l'épidémie;
- 2° De vérifier tout au long de ces opérations le respect des garanties entourant le secret médical et la protection des données personnelles.

Sa composition, qui inclut deux députés et deux sénateurs désignés par les présidents de leurs assemblées respectives, et la mise en œuvre de ses missions sont fixées par décret. Les membres du comité exercent leurs fonctions à titre gratuit. [...]

Le Gouvernement adresse au Parlement un rapport détaillé de l'application de ces mesures tous les trois mois à compter de la promulgation de la présente loi et jusqu'à la disparition des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de covid-19. Ces rapports sont complétés par un avis public de la Commission nationale de l'informatique et des libertés ».

De telles solutions offrent l'avantage d'ouvrir au débat démocratique la gestion de la crise, concentrée parfois trop arbitrairement dans les mains des quelques-uns qui en ont la charge, au mépris des droits fondamentaux, de la démocratie et de l'État de droit.

Conclusion

70. Des besoins d'une solution procédurale générale pour régler les conflits entre libertés et intérêt général. La lutte contre le coronavirus Covid-19²⁸⁵ est souvent abordée comme réveillant l'antagonisme entre les intérêts publics et les droits fondamentaux. Dans un article paru dans le *Financial Times*²⁸⁶, Yuval Harari prétendait que liberté et sécurité ne devraient jamais s'exclure²⁸⁷, d'autant plus lorsqu'il s'agit de sécurité sanitaire. Nos libertés et droits fondamentaux doivent être et rester le cœur de nos démocraties et de l'État de droit, avec qui ils forment la « Sainte Trinité » énoncée à l'article 4 du TUE. Les dérogations ou limitations à nos libertés fondamentales imposées en vue de répondre à l'état d'urgence sanitaire nous forcent à reconnaître, les limites de notre « vieille » Constitution. N'est-il pas temps d'insérer un *corpus* cohérent et complet de règles de base destinées à encadrer les limitations et dérogations aux droits fondamentaux²⁸⁸ ? Le professeur Marc Verdussen le

²⁸⁵ Sur l'utilisation du masculin ou du féminin, voy. www.academie-francaise.fr/le-covid-19-ou-la-covid-19; consulté en dernier lieu le 20 octobre 2020.

²⁸⁶ Traduit en français et publié par *l'Express* le 26 mars; www.lexpress.fr/actualite/yuval-noah-harari-le-monde-dans-lequel-nous-vivons-apres-l-orage_2121963.html; consulté en dernier lieu le 20 octobre 2020.

²⁸⁷ EDPB, *Guidelines* 04/2020, *op. cit.*

²⁸⁸ La Constitution belge « a été révisée à de nombreuses reprises, spécialement à partir de la fin des années 60. Mais, si on y regarde de plus près, on constate que le pouvoir constituant est obnubilé par le fédéralisme. La plupart des modifications sont liées à la transformation de l'État belge en un État fédéral. Si d'autres changements sont intervenus, ils révèlent une dérive pointilliste dans l'exercice du pouvoir

demande : « N'est-il pas préférable d'entrouvrir cette porte, *in tempore non suspecto*, en posant des limites matérielles et procédurales à la mise en œuvre d'un régime dérogatoire ? »²⁸⁹.

Sans doute, l'absence de cadre constitutionnel aux dérogations²⁹⁰ à nos droits fondamentaux a poussé nos gouvernements à faire fi de toutes contraintes, mêmes conventionnelles, se cachant derrière la notion vague de « l'état d'urgence sanitaire ». De la sorte, ce n'est pas simplement les droits fondamentaux qui se trouvent en danger, mais bien l'État de droit et, par extension, notre démocratie libérale. Ainsi, il importe que ces restrictions, même ordonnées à la hâte, trouvent un fondement légal, soient motivées et proportionnées et surtout fassent l'objet d'un minimum de consensus au sein de la population.

71. Numérique, droit et éthique. La crise a également permis d'accélérer le développement du numérique dans notre quotidien. Cette accélération n'a pas manqué de cristalliser les tensions entre les droits fondamentaux lors de l'immixtion des gouvernements dans nos vies privées par le truchement des applications de *tracing*. Dans ce contexte, le numérique est-il la panacée²⁹¹ assurant une sortie de crise, ou à tout le moins un confinement, pérenne ? Rien n'est moins certain. Notre propos n'est certes pas de condamner l'utilisation des technologies ni de la privilégier mais de réclamer que nos autorités opèrent un juste équilibre entre les libertés individuelles, d'une part, et l'intérêt général et celui d'autrui, de l'autre. Sans doute serait-il utile que le gouvernement, à l'issue d'un débat ouvert, opère une balance à l'aune des circonstances actuelles et des risques particuliers et majeurs liés, d'une part, à la pandémie et, d'autre part, aux mesures diverses tant de nature que de portée, qu'elles soient purement sanitaires, sociales ou qu'elles utilisent les ressources du numérique²⁹².

constituant, ne répondant qu'à des besoins ponctuels et limités. [...], les révisions au coup par coup trahissent dans le chef du Constituant un triste manque d'ambition. Combien de choix fondamentaux ne sont-ils pas omis, reportés ou évités ? », in M. VERDUSSEN, *Réenchâter la Constitution*, Bruxelles, Académie royale de Belgique, 2019, p. 15.

²⁸⁹ M. VERDUSSEN, « Démocratie, État de droit et droits fondamentaux face à la pandémie de Covid-19 : perspectives croisées. La situation en Belgique », note de travail pour l'Unité mixte de recherche (UMR) « DICE – Droits International, Comparé et Européen », 15 avril 2020, p. 2, disponible à l'adresse : https://dice.univ-amu.fr/sites/dice.univ-amu.fr/files/public/m._verdussen-note_de_travail_ndeg_1-15_avril_2020.pdf?fbclid=IwAR2_eRAZRKInvMhmMZfzIR-vW0qei-AP0ecaHmurErJCaBpD74mylz-qgbo ; consulté en dernier lieu le 20 octobre 2020.

²⁹⁰ R. ERGEC et S. WATTHÉE, « Les dérogations aux droits constitutionnels », in M. VERDUSSEN et N. BONBLED (dir.), *Les droits constitutionnels en Belgique – Les enseignements jurisprudentiels de la Cour constitutionnelle, du Conseil d'État et de la Cour de cassation*, vol. 1, Bruxelles, Bruylant, 2011, p. 396.

²⁹¹ À cet égard, l'expérience passée de la lutte contre l'Ebola, une pandémie africaine, a bien montré que les outils numériques mis en place non seulement ont eu peu de succès mais surtout ont contribué à limiter les libertés individuelles dans des États à tendance autoritaire. Sur ce point, voy. l'article de S. M. McDONALD, « Ebola : A Big Data Disaster – Privacy, Property, and the Law of Disaster Experimentation », *CIS Papers*, 2016.01, mars 2016, disponible à l'adresse : <http://cis-india.org/papers/ebola-a-big-data-disaster>.

²⁹² Conseil de l'Europe, *Joint statement on the right to data protection in the context of the Covid-19 pandemic*, 30 mars 2020, disponible à l'adresse : www.coe.int/dataprotection ; consulté en dernier lieu le 20 octobre 2020.

Comme l'écrit le Comité consultatif national d'éthique consulté par le gouvernement français²⁹³ : « L'un des enjeux éthiques majeurs dans cette situation, avec le passage à la dimension épidémique et collective, est d'engager la société tout entière dans une véritable démarche de responsabilité et de solidarité, parce que la lutte contre une épidémie doit être l'affaire de tous et pas seulement l'affaire des experts et des professionnels de santé ». La maladie nous embarque tous dans une aventure commune, et nous contraint aujourd'hui à sortir de notre zone de confort et à questionner le monde, questionner nos pratiques, questionner le droit. Le droit, en particulier les droits de l'homme et les modalités de leurs limitations et dérogations, est justement là pour nous rappeler certaines préoccupations éthiques et les rappeler à nos dirigeants. Cette épreuve semble encourager à repenser tout ce qui jusqu'à présent semblait acquis.

Le déploiement du numérique, force également à l'approfondissement des différents droits de l'homme et, peut-être à la reconnaissance de nouveaux droits subjectifs, comme de droit à la vie privée a pu aboutir, du fait des risques nouveaux créés par le numérique à des législations de protection des données et par là à la création de droits subjectifs nouveaux ; droit d'accès, droit à ne pas être soumis à une décision automatisée, etc. Autre exemple, la liberté d'expression oblige, dans nos sociétés modernes à la reconnaissance d'un droit d'accès à la toile²⁹⁴ ou encore le secret des correspondances s'entend bien du secret des communications électroniques²⁹⁵. Il faut néanmoins rester prudent et ne pas succomber à la tentation de l'efflorescence de nouveaux droits de l'homme liés au numérique, tant en matière de liberté d'expression que de protection de la vie privée (droit à l'anonymat, droit à l'oubli, droit à la portabilité...) ²⁹⁶, au risque d'un affaiblissement du caractère fondamental de ces droits et libertés propres à l'homme.

72. La pandémie nous oblige-t-elle à revoir la liste des droits fondamentaux ? Il ne paraît pas utile d'envisager une modification de la liste des droits de l'homme, en y consacrant de nouveaux droits, car « lorsque tout devient fondamental, rien ne l'est plus vraiment »²⁹⁷. Au contraire, dans la droite ligne du principe d'interprétation évolutive et dynamique des droits de l'homme²⁹⁸ par le juge strasbourgeois, consacré à l'article 32 de la CEDH, lais-

²⁹³ Contribution du Comité consultatif national d'éthique, *Enjeux éthiques face à une pandémie*, 13 mars 2020, disponible à l'adresse : www.ccne-ethique.fr/sites/default/files/reponse_ccne_-_covid-19_def.pdf.

²⁹⁴ Cour eur. D.H., arrêt *Ahmet Yildirim c. Turquie*, 18 décembre 2012, n° 3111/10.

²⁹⁵ Cour eur. D.H., arrêt *Copland c. Royaume-Uni*, 3 avril 2007, n° 62617/00.

²⁹⁶ En ce sens, Y. POULLET, « Quelques réflexions d'avant-propos », in *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, pp. 7-37.

²⁹⁷ *Ibid.*, p. 11.

²⁹⁸ L'article 32 de la CEDH traduit ce lien essentiel entre interprétation et application du droit, en stipulant que « La compétence de la Cour s'étend à toutes les questions concernant l'interprétation et l'application de la Convention et de ses protocoles » ; en ce sens, selon l'expression du professeur François Rigaux, le juge strasbourgeois est qualifié de « Ministre du sens » (Fr. RIGAUX, *La loi des juges*, Paris, Éd. Odile Jacob, 1997, p. 233).

ser les juges faire œuvre créatrice. C'est à l'aune de ce principe que la Cour a consacré le droit à la santé et le droit à un environnement sain, par une lecture dynamique du droit à la vie (art. 2 CEDH), mais aussi et particulièrement du droit au respect de la vie privée et familiale (art. 8 CEDH).

Elle a introduit également le principe de précaution dans la mise en œuvre de ces droits à coloration environnementale ou sanitaire. Suivant ce principe, la Cour consacre l'idée selon laquelle « l'absence de certitude compte tenu des connaissances scientifiques et techniques du moment ne saurait justifier que l'État retarde l'adoption de mesures effectives et proportionnées »²⁹⁹. La Cour a en outre noté la nécessité pour les autorités d'assurer l'accès du public aux conclusions des études et enquêtes, rappelant l'obligation de l'État de garantir le droit de la population à participer au processus décisionnel en matière d'environnement. Le principe de précaution constitue ainsi une inversion de la charge de la preuve en matière de responsabilité dans le chef des États, lors de la mise en œuvre des droits conventionnels. Hasardons-nous à espérer que la crise sanitaire contribue à intégrer ce changement de paradigme dans la notion de responsabilité au bénéfice de la notion de « responsabilité sociale » (le concept américain d'« accountability », introduit par le RGPD). À l'instar des modifications apportées à la protection des données, ce changement permettrait de contrer les dérives des États mais également les entités non étatiques à l'occasion de la réalisation des droits fondamentaux, surtout lorsqu'il s'agit de les mettre en exergue avec d'autres droits et intérêts, tels que les intérêts économiques ou de santé publique.

Gageons que cette crise contribue à définir cette nouvelle génération des droits de l'homme³⁰⁰ avec en ligne de mire la préservation de l'individu dans son intégrité et son altérité.

Parce que, par-delà le droit, il y a l'humain !

²⁹⁹ Cour eur. D.H., arrêt *Tatar c. Roumanie*, 27 janvier 2009, n° 67021/01

³⁰⁰ Pour une réflexion plus générale sur les catégories juridiques, dont la valeur logique et scientifique reste discutable, voy. notamment M. TROPER, « Les classifications en droit constitutionnel », *R.D.P.*, 1989, pp. 945-956 ; J.L. BERGEL, *Théorie générale du droit*, coll. Méthodes du droit, 4^e éd., Paris, Dalloz, 2003, spéc. n°s 180 à 207, pp. 209-232. Sur les droits dits de la « troisième génération », également appelés « droits-solidarité », que l'on oppose aux droits-attributs de la personne humaine (première génération) et aux droits-créances (deuxième génération), voy. K. VASAK, « Les différentes typologies des droits de l'homme », in E. BRIBOSIA et L. HENNEBEL (dir.), *Classer les droits de l'homme*, coll. Penser le droit, Bruxelles, Bruylant, 2004, p. 19, et, du même auteur, « Revisiter la troisième génération des droits de l'homme avant leur codification », in *Liber Amicorum Hector Gros Espiell*, Bruxelles, Bruylant, 1997, pp. 1649-1679. Cette troisième génération comprend notamment le droit à la paix, au développement et à un environnement sain. Sur les droits dits de la « quatrième génération », à savoir ceux qui doivent protéger la dignité humaine de certains abus de la science, et qui incluent « les droits bioéthiques et de la génétique » et « les droits relatifs aux communications », voy. S. MARCUS HELMONS, « La quatrième génération des droits de l'homme », in *Les droits de l'homme au seuil du troisième millénaire. Mélanges en hommage à Pierre Lambert*, Bruxelles, Bruylant, 2000, pp. 549-559, spéc. p. 551.