Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Le Covid face au droit de la protection des données, bien au-delà de la protection de la vie privée

Parsa, Saba; Van Gyseghem, Jean-Marc

Published in:
La pandémie de Covid-19 face au droit

Publication date:
2022

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Parsa, S & Van Gyseghem, J-M 2022, Le Covid face au droit de la protection des données, bien au-delà de la protection de la vie privée. Dans S Parsa & M Uyttendaele (eds), *La pandémie de Covid-19 face au droit: volume 2 : analyse et perspective d'une crise et de ses lendemains.* Anthemis, Limal, p. 297-358.

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.

Download date: 18. Apr. 2024

Le Covid face au droit de la protection des données, bien au-delà de la protection de la vie privée

Saba Parsa

Avocate au barreau du Brabant wallon
Assistante en droit à l'Université Saint-Louis – Bruxelles
Première vice-présidente du Conseil supérieur de l'audiovisuel
Rédactrice en chef de la revue *DPO News*

Jean-Marc Van Gyseghem[1]

Avocat au barreau de Bruxelles
Directeur de recherche au Centre de recherche information, droit et société de l'Université de Namur

> « Il faut se réserver une arrière-boutique toute nôtre, toute franche, en laquelle nous établissons notre vraie liberté et principale retraite et solitude. » (Montaigne)

Introduction

Dans la lutte contre la pandémie du Covid-19, le traitement de données à caractère personnel par des acteurs privés et publics a occupé une place centrale notamment en vue d'assurer la phase de déconfinement. De l'obligation pour les exploitants de cafés et restaurants de collecter les données destinées au *tracing* de leurs clients, de celle des écoles à l'égard de leurs élèves et étudiants, en passant par la lecture et la collecte des données depuis le « *Passenger Location Form* » (ou PLF) ou la lecture des données depuis l'application Covid Safe Ticket, et enfin le traitement des données des laboratoires et les centres de dépistage, les exemples sont nombreux. Les États ont mobilisé les ressources privées et publiques afin de rassembler les données de santé de citoyens dans de gigantesques bases. Pire encore, l'accès aux données des patients paraît même avoir été un outil de négociation clé dans les accords bilatéraux passés par un État ou l'autre pour l'achat des doses de vaccin, comme semble le démontrer le cas israélien[2].

---

1 *This work has been done with the financial support from the European Union's Horizon 2020 general MGA program under Grant Agreements n° 830892 (SPARTA).* La publication ne reflète que l'opinion de l'auteur et la Commission européenne ne peut être tenue responsable de l'usage qui en serait fait.

2 AFP, « Quand Israël offre ses données médicales à Pfizer », *L'Express*, 18 janvier 2021 ; disponible à l'adresse : https://www.lexpress.fr/actualites/1/actualite/quand-israel-offre-ses-donnees-medicales-a-pfizer_2142936.html ; consulté en dernier lieu le 20 décembre 2020.

Ces traitements massifs sont rendus possibles grâce à l'évolution des technologies de l'information et du numérique, soulevant d'importantes questions juridiques et éthiques relatives à la conception du droit au respect de la vie privée et de la protection des données. Dans ce contexte, force est de constater que l'entrée en vigueur du Règlement général relatif à la protection des données à caractère personnel[3] (ci-après, « RGPD » ou « Règlement »), en mai 2018, semble avoir sensibilisé les individus à la protection de leurs données à caractère personnel, devenue un sujet 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 publics des autorités de contrôle au travers de toute l'Europe, et ce, dès les premiers jours de la crise, publiant 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 »)[4]; au niveau européen, du Comité européen de protection des données (ci-après, le « CEPD » ou « EDPB » en anglais)[5] et du Conseil de l'Europe[6].

Cela dit, il convient de ne pas sacraliser la protection de la vie privée par le truchement de la protection des données, ni même de sanctuariser la protection des données au titre d'un droit autonome de l'homme, au risque d'en dénaturer la portée. En ce sens, la Convention 108+[7] *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* énonce des normes élevées pour la protection des données personnelles qui restent compatibles et conciliables avec d'autres droits fondamentaux et l'intérêt public[8]. Le

3 Règlement (UE) n° 2016/679 du Parlement et du Conseil européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données, ci-après, le « RGPD » ou « Règlement »).

4 APD, avis relatifs au Covid-19, disponibles à l'adresse: https://www.autoriteprotectiondonnees.be/professionnel/avis-relatifs-au-covid-19; consulté en dernier lieu le 20 décembre 2021.

5 « 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 décembre 2021.

6 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-pierucciand-jean-philippe-walter. Cette déclaration a été complétée par les mêmes personnes, au vu des questions nouvelles soulevées par le déconfinement; disponible sur le site www.coe.int/en/web/data-protection/contact-tracingapps, consulté en dernier lieu le 20 décembre 2021.

7 *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 28 janvier 1981, entrée en vigueur le 1er octobre 1985, telle que modifiée par le Conseil de l'Europe, Comité des ministres, *Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, STCE 223, adopté le 18 mai 2018*, et ouvert à signature depuis le 25 juin 2018, ci-après, « Convention n° 108 + ».

8 Conseil de l'Europe, « Déclaration conjointe sur le droit à la protection des données dans le contexte de la pandémie à COVID-19 », par Alessandra Pierucci, présidente du Comité de la Convention n° 108, Jean-Philippe Walter, Commissaire à la protection des données du Conseil de l'Europe, 30 mars 2020, Strasbourg, p. 2.

droit à la protection des données ne peut être un dogme et ne peut en aucun cas être un obstacle à sauver des vies humaines.

De son côté, 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[9], sans que ni l'un ni l'autre de ces droits ne puissent être qualifiés d'absolus.

Dès lors, si, à l'occasion de la contribution réalisée dans la première édition du présent ouvrage[10], l'impact de la gestion de la pandémie sur le droit à la vie privée et de la protection des données a été appréhendé, *a contrario* la présente contribution vise à examiner l'impact de la législation relative à la protection des données à caractère personnel sur les mesures prises par l'État en vue de contenir la propagation de la maladie.

Ainsi, dans un premier temps (Section 1) le cadre juridique des traitements des données nécessaires à la gestion de la pandémie sera défini. Ensuite sera exposée l'application en Belgique de ce cadre (Section 2), qui aura permis d'éviter parfois une dérive autoritaire au profit du pragmatisme qui a guidé le gouvernement dans la gestion de la crise.

Section 1
Cadre juridique du traitement des données à caractère personnel applicable à la gestion d'une pandémie

Dans le cadre de la gestion de la pandémie, certains États, dont la Belgique[11], ont utilisé des instruments d'observation des pratiques collectives de mobilité et de confinement, tels que la cartographie des déplacements de populations[12],

9 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 ».

10 S. Parsa et Y. Poulet, « Les droits fondamentaux à l'épreuve du confinement et du déconfinement: le *tracing* », *in* S. Parsa et M. Uyttendael, *La pandémie de Covid-19 face au droit*, vol. 1, Limal, Anthemis, 2020, pp. 137-217.

11 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 plates-formes 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. À noter que ce projet a été accompagné par un « comité éthique » se réunissant une fois par semaine afin d'évaluer les aspects tant juridiques, en matière de protection de la vie privée, qu'éthiques.

12 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,

l'identification des sujets « contacts » 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.

L'objectif de veille sanitaire assigné à ces instruments est légitime à condition que les moyens mis à disposition de cet objectif (légitime) respectent les lois en vigueur, notamment celles relatives à la protection des données, et restent proportionnés.

En effet, 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 de porter atteinte au bon fonctionnement de la démocratie[13]. 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[14].

Ces traitements ne peuvent avoir lieu hors du cadre précis des dispositions du RGPD, de l'article 8 de la Convention européenne des droits de l'homme, et de la Convention n° 108+ qui succède à la Convention n° 108 en 2018[15]. Le RGPD et la Convention n° 108+ étant assez similaires, il sera examiné ci-après les principes généraux et les obligations qui découlent du Règlement et qui s'imposent à toute organisation, publique ou privée, de manière directe qu'elle agisse en qualité de responsable du traitement ou du sous-traitant, y compris bien évidemment dans le cadre des traitements intervenant dans la limitation de la propagation du coronavirus.

Dans un premier temps seront examinés les principes généraux et obligations découlant du RGPD (§ 1), pour pouvoir appréhender ensuite les spécificités des traitements de données liés à la gestion de la pandémie (§ 2).

numérique et droits de l'homme – un étrange cocktail !», *op. cit.*, p. 248. En Belgique, un tel système impliquant des caméras avec reconnaissance faciale ou non ou des capteurs GPS n'a pas été utilisé. Seuls les signaux GSM l'ont été mais de telle manière qu'aucune identification n'était possible.

13 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.*

14 S. Parsa et Y. Poulet, « Les droits fondamentaux à l'épreuve du confinement et du déconfinement : le tracing », *in* S. Parsa et M. Uyttendael (dir.), *La pandémie de Covid-19 face au droit*, vol. 1, Limal, Anthemis, 2020, p. 137.

15 *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 28 janvier 1981, entrée en vigueur le 1er octobre 1985, telle que modifiée par le Conseil de l'Europe, Comité des ministres, *Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, STCE 223, adopté le 18 mai 2018*, et ouvert à signature depuis le 25 juin 2018, ci-après, « Convention n° 108 + ».

§ 1. Principes généraux et obligations découlant du RGPD

Les principes généraux applicables aux traitements des données à caractère personnel sont énoncés notamment 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 ces principes généraux comme 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, § 1er, 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*) ».

Ces principes occupent une place importante dans la garantie du droit fondamental à la protection des données et le respect de la vie privée. Ils font l'objet

d'une attention rigoureuse des autorités de contrôle nationales[16]. En témoignent les avis, recommandations, sanctions que les Autorités de contrôle émettent au gré de leurs activités[17] régulatoires.

Ainsi, il est rappelé les dispositions de l'article 36, § 4, du RGPD, qui énoncent ce qui suit :

- « Les États membres consultent 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. »

Les États membres sont ainsi tenus de consulter leur Autorité sur l'ensemble des textes normatifs se rapportant à des traitements de données à caractère personnel. Cet article est complété par l'article 23 de la loi du 3 décembre 2017 portant création de l'Autorité[18] de protection des données, qui énonce ce qui suit :

- « *Art. 23.* § 1er. Le centre de connaissances émet soit d'initiative, soit sur demande du gouvernement, des Chambres législatives, des Gouvernements de communauté ou de région, des Parlements de communauté ou de région, du Collège réuni ou de l'Assemblée réunie visés à l'article 60 de la loi spéciale du 12 janvier 1989 relative aux institutions bruxelloises :
  1° des avis sur toute question relative aux traitements de données à caractère personnel ;
  2° des recommandations relatives aux développements sociaux, économiques et technologiques qui peuvent avoir une incidence sur les traitements de données à caractère personnel.
  § 2. Dans ses avis et recommandations, le centre de connaissances tient compte des mesures de sécurité techniques et organisationnelles nécessaires. »

En Belgique, c'est donc le centre des connaissances de l'APD qui examine et donne un avis sur toutes les questions relatives aux traitements de données à caractère personnel dans les textes normatifs.

À l'occasion de cet examen concernant le projet de loi relative à l'urgence épidémique[19], le centre des connaissances a émis un avis assassin. Revenant sur les principes généraux du RGPD, l'APD constatait l'absence de conformité de la loi, notamment pour les raisons suivantes[20] :

- l'avant-projet ne constitue pas une base légale valable pour les traitements de données qui pourraient être effectués dans le cadre de la mise en place des mesures de police. Il donne lieu à une violation des principes de légalité et de prévisibilité ;
- l'avant-projet ne définit pas les catégories de personnes dont les données pourront être traitées ;
- l'absence de démonstration de la nécessité des traitements de données et la violation des principes de minimisation et proportionnalité ;
- la contrariété de l'avant-projet au principe de transparence.

Ceci explique, sans doute, pourquoi, dans sa dernière version du projet de loi relative à l'urgence épidémique, le législateur a purement et simplement fait abstraction des mesures relatives aux traitements des données, pourtant nécessaires à la gestion d'une crise sanitaire. Nous analyserons cet aspect de la loi relative à l'urgence épidémique plus loin.

Pour mieux appréhender l'étendue de ces principes, il sera premièrement examiné les principes de finalité, de licéité, de loyauté et de transparence en un seul tenant, ainsi que les obligations qui en découlent (A). Deuxièmement seront abordés les principes de minimalisation et de sécurité, d'intégrité et confidentialité (B).

A. Principes de finalité, de licéité, de loyauté et de transparence

Parmi ces principes, l'article 5, a) et b), du RGPD retient les principes de licéité[21] et de finalité[22] (1), de transparence et de loyauté du traitement (2).

1. Les principes de finalité et licéité

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 précise[23], assurant ainsi le principe de transparence et de loyauté des traitements. Enfin, les traitements doivent être licites, à savoir reposer sur une des *bases de légitimité* mentionnées à l'article 6, § 1er, du RGPD, pour être légaux[24]. 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 ;

16 Art. 51 et s. RGPD.
17 Art. 57 RGPD.
18 Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018.
19 Art. 6, § 10, du projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, *Doc. parl.*, 2020-2021, n° 1951/001, https://www.lachambre.be/FLWB/PDF/55/1951/55K1951001.pdf (dernière consultation le 6 janvier 2022).
20 APD, avis n° 24/2021 du 2 mars 2021 sur l'avant-projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique (CO-A-2021-044), pp. 3-10.
21 Art. 5.2 de la Convention n° 108+.
22 Art. 5.4.b) de la Convention n° 108+.
23 Art. 13 et 14 RGPD.
24 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.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1 ; consulté en dernier lieu le 20 octobre 2020.

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. »

Dans le cadre de la gestion de la pandémie, 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 elles sont investies en qualité de responsables du traitement[25]. La mission d'intérêt public est généralement reconnue par une loi ou une autre règle de droit[26]. « Le principe de légalité qui gouverne l'administration impose effectivement que les missions confiées aux entités du secteur public aient une base légale »[27].

En outre, lorsque le traitement de données porte sur des catégories particulières de données[28], telles que les données relatives à l'état de santé des personnes[29], ce

25 *Ibid.* ; art. 6, § 1er, e), RGPD.

26 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 ; consulté en dernier lieu le 20 décembre 2021.

27 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.

28 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 [...] ».

29 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.

qui est bien évidemment le cas dans les hypothèses qui nous occupent, les responsables du 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 données[30] :

– « 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[s], 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 [...] ;
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 [...] »[31].

Cumulant les articles 6 et 9, la CNIL conclut que :

– « [l]e 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 ;

30 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. 255-284. À noter que cette règle de cumul des articles 6 et 9 du RGPD ne fait pas l'unanimité. Nous aborderons cette question plus loin.

31 Nous soulignons.

- une des exceptions mentionnées à l'article 9 du règlement est applicable au traitement concerné »[32].

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 principalement leur base de licéité à l'article 6, § 1er, point e), lu conjointement avec l'article 9, § 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, les données relatives à l'état de santé peuvent également être utilisées, 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 du *tracing* ou du CST, selon l'article 9, est soumis à la surveillance d'un professionnel de la santé en vue de répondre aux exigences du paragraphe 2 de l'article 9 du RGPD. Ce point est important, car peu importe le système d'alerte mis en place, 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.

Enfin, dans le cadre de gestion de crise sanitaire, les données de santé ont également été traitées à des fins de recherche scientifique. À cet égard, dans ses lignes directrices[33], le CEPD rappelle la base de licéité mobilisable dans le cadre des traitements nécessaires à la recherche scientifique. Selon le CEPD[34], l'article 6, § 1er, point e) ou f), du RGPD lu en combinaison avec les dérogations adoptées en vertu de l'article 9, § 2, point j) ou i), du RGPD, peut constituer la base juridique du traitement de données à caractère personnel relative à l'état de santé à des fins de recherche scientifique. Néanmoins et en tout état de cause, un projet de recherche doit respecter les règles posées par l'article 89, § 1er, du RGPD comme suit :

– « est soumis [...] à des garanties appropriées » et que ces « garanties garantissent la mise en place de mesures techniques et organisationnelles, en

32 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-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd ; consulté en dernier lieu le 20 octobre 2020.

33 CEPD, Lignes directrices 03/2020 du 21 avril 2020 sur le traitement de données concernant la santé à des fins de recherche scientifique dans le contexte de la pandémie de COVID-19, disponible à l'adresse : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_fr.pdf, consulté en dernier lieu le 20 décembre 2021.

34 *Ibid.*, p. 6, § 23.

particulier pour assurer le respect du principe de minimisation des données. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière ».

Cet article met en évidence l'importance du principe de minimisation[35] des données et le principe d'intégrité et de confidentialité[36], ainsi que le principe de protection des données dès la conception et par défaut[37], en matière de recherche également[38].

Dans la pratique, les principes de finalité et de licéité n'ont pas été mis en œuvre sans heurts.

À titre exemplatif, en Grèce et en France, l'utilisation de drones a suscité de telles inquiétudes et entraîné des actions en justice, faute de base de licéité notamment. En Grèce, une ONG a souligné que le déploiement de drones était fondé sur une loi qui ne comportait aucune garantie spécifique en matière de protection des données et ne faisait aucune référence explicite à la législation sur la protection des données[39]. En France, deux ONG ont déposé un recours devant le Conseil d'État, signalant l'absence d'un cadre juridique explicite pour l'utilisation de drones au-dessus de Paris afin de surveiller les déplacements des personnes pendant et après la période de confinement. Le Conseil d'État a ordonné au gouvernement de cesser immédiatement cette surveillance[40].

S'agissant plus particulièrement des traitements initiés par les entreprises, c'est essentiellement dans le cadre de la gestion des ressources humaines s'agissant de la mise en œuvre des mesures imposées pour endiguer la pandémie que des difficultés sont rencontrées.

À titre d'exemple, le port d'Anvers a commencé à utiliser des bracelets Bluetooth pour appliquer des règles de distanciation sociale sur le lieu de travail. Ces dispositifs portables émettent des signaux avertissant les travailleurs qui s'approchent trop près les uns des autres. Sur son site internet, l'APD[41] confirme que des bracelets de suivi numérique totalement anonymes peuvent être utilisés sur le lieu de travail et avertit explicitement qu'ils ne peuvent pas l'être si les

35 Art. 5, § 1er, c), RGPD.

36 Art. 5, § 1er, e), et 32 RGPD.

37 Art. 25 RGPD.

38 Voy. *infra*, B., 1.

39 Pandémie de coronavirus dans l'UE - Conséquences pour les droits fondamentaux - Bulletin 2, Agence européenne des droits fondamentaux, 28 mai 2020, p. 56 (en anglais), disponible sur le site : https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1, consulté en dernier lieu le 20 décembre 2020.

40 Conseil d'État (FR), arrêté du 18 mai 2020, n° 440442, 440445, disponible sur le site : https://conseil-État.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-État-18-mai-2020-surveillance-par-drones, consulté en dernier lieu le 20 décembre 2020.

41 APD, « La covid-19 sur le lieu de travail », 14 septembre 2020, disponible sur le site : https://gegevensbeschermingsautoriteit.be/burger/thema-s/covid-19/covid-19-op-de-werkvloer, consulté en dernier lieu le 20 décembre 2020.

données de localisation de personnes identifiables sont utilisées et stockées. Ce traitement n'est autorisé que sur la base du consentement explicite de l'employé, ce qui est préoccupant compte tenu du déséquilibre des pouvoirs entre les employés et les employeurs[42] et de la difficulté d'utiliser le consentement comme base de licéité dans le cadre de la relation de travail.

Les scanners thermiques sont également largement utilisés pour surveiller l'accès aux locaux publics et privés et, de plus en plus également, dans les aéroports. L'utilisation de thermomètres à infrarouge a déclenché les réactions de plusieurs autorités de protection des données. Les autorités néerlandaise[43], lituanienne[44] et portugaise[45] ont déclaré illégale l'utilisation de scanners thermiques par les employeurs, tandis que d'autres, comme l'APD en Belgique[46], ont mis en doute la base juridique de leur utilisation dans les aéroports, mais non pas par l'employeur, sous réserve de ne pas compiler ces données dans des bases ou des listings de données des personnes atteintes du Covid et de les renvoyer vers un praticien de soins de santé. Enfin, il est également rappelé que faute de base de licéité et particulièrement à défaut de rencontrer une des conditions de l'article 9, § 2, s'agissant du traitement de données de santé, l'APD a interdit les questionnaires des employeurs portant sur l'état de santé. Les différences de positions adoptées par les autorités nationales, et les sanctions ou recommandations émises par ces dernières, témoignent de la difficulté en pratique de déterminer la bonne base de licéité, notamment dès lors qu'il s'agit de traiter des données sensibles, en l'occurrence relatives à l'état de santé. Deux causes sans doute à cette difficulté : d'une part, l'articulation des dispositions des articles 6 et 9 du RGPD n'est pas toujours commode ; d'autre part, la marge d'interprétation de la directive reste en ces matières encore importante.

42 *Ibid.*

43 Déclaration de l'autorité de surveillance néerlandaise sur les analyses thermiques, 24 avril 2020, disponible sur le site : https://autoriteitpersoonsgevens.nl/nl/nieuws/ap-temperatuur-meten-mag-niet-zomaar, consulté en dernier lieu le 20 décembre 2020.

44 Déclaration de l'autorité lituanienne de protection des données sur la protection des données à caractère personnel et le Covid-19, 16 mars 2020, disponible sur le site : https://vdai.lrv.lt/fr/news/personal-data-protection-and-coronavirus-covid-19, consulté en dernier lieu le 20 décembre 2020.

45 Déclaration de l'autorité de surveillance portugaise sur l'illégalité de l'utilisation des scanners thermiques par les employeurs, 23 avril 2020, disponible sur le site : https://cnpd.pt/home/orientacoes/Orientacoes_recolha_dados_saude_trabalhadores.pdf, consulté en dernier lieu le 20 décembre 2020.

46 APD, « L'APD impose une amende pour traitement illégitime d'images de caméras de surveillance », communiqué de presse, 25 novembre 2020, disponible sur le site : https://www.gegevensbeschermingsautoriteit.be/citoyen/lapd-impose-une-amende-pour-traitement-illegitime-dimages-de-cameras-de-surveillance, consulté en dernier lieu le 20 décembre 2020 ; voy. également APD, 17 juin 2020, https://autoriteprotectiondonnees.be/citoyen/controles-de-temperature-lapd-prend-contact-avec-brussels-airport.

2. Principe de transparence et de loyauté

S'agissant de l'obligation de transparence et de loyauté, l'article 5, § 1er, 1°, a), du RGPD doit être lu conjointement avec les articles 12, 13 et 14 du RGPD[47]. En effet, le principe de transparence induit simultanément un droit à l'information et son corollaire, un droit d'accès aux données dans le chef des personnes dont les données sont traitées. En vue de comprendre ces obligations seront examinés ci-dessous le contenu de cette information (a), les modalités de la réalisation de cette communication (b) et, enfin, les exceptions à cette obligation (c).

a. Contenu de l'information

Le principe de transparence énoncé à l'article 5, § 1er, 1°, du RGPD est précisé dans son contenu, entre autres, aux articles 12, 13 et 14 du Règlement. En substance, les dispositions de ces articles consacrent l'obligation pour un responsable du traitement d'informer les personnes concernées tant lorsqu'il collecte directement leurs données auprès de celles-ci que lorsqu'il les obtient indirectement, par l'entremise d'un tiers. À titre exemplatif, tant le Gouvernement Fédéral, les entités fédérées, l'AVIQ, Sciensano que les entreprises privées, telles que des compagnies aériennes, les restaurateurs, les écoles, notamment dans le cadre de l'utilisation des applications digitales de gestion de la situation sanitaire, ou le *tracing* doivent informer les personnes concernées du traitement de leurs données.

Les mentions minimales d'une telle communication sont définies aux articles 13 et 14 du RGPD, on y retrouve notamment les mentions suivantes :

- l'identité et les coordonnées du responsable du traitement ;
- les finalités et les bases juridiques des traitements ;
- les destinataires ou catégories de destinataires des données[48] ;
- la durée de conservation ;
- les transferts hors UE et les modalités de ces transferts ;
- les droits des personnes concernées ;
- le cas échéant, l'existence d'une prise de décision automatisée.

b. La forme de l'information

Ces informations doivent être fournies au plus tard au moment de la collecte des données, lorsque cette collecte est directe[49]. *À défaut*, ces informations

47 Voy. également art. 8 de la Convention n° 108+.

48 Le terme « destinataire » est défini à l'article 4, 9), du RGPD, comme signifiant « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ».

49 Art. 13, § 1er, RGPD.

doivent être remises dans un délai raisonnable et au plus tard au moment de la première communication avec la personne concernée[50].

S'agissant de la forme d'une telle communication, l'article 12 du RGPD impose les règles suivantes :

(i) les informations doivent être concises, transparentes, compréhensibles et aisément accessibles ;
(ii) des termes clairs et simples doivent être employés, en particulier vis-à-vis des enfants ;
(iii) les informations sont fournies par écrit ou par d'autres moyens ; et
(iv) elles sont généralement fournies gratuitement.

À cet effet et dans la pratique, les responsables des traitements procèdent à la rédaction et la publication d'un document déclaratif de type : charte de protection des données ou politique de confidentialité ou encore formulaire de collecte. Ces documents reprennent, sous diverses formes et divers supports (FAQ, en liste, menu déroulant en HTLM, PDF, format papier…), les mentions obligatoires ci-avant énoncées.

Il n'est cependant pas exclu de procéder par d'autres voies. Des vidéos, des infographies ou d'autres types de supports peuvent venir agrémenter cette documentation. Le RGPD n'impose aucune forme ou média, mais uniquement l'obligation d'information.

À titre exemplatif, l'application CST fournit cette information, notamment sur la page d'accueil de son site et de son application, via un onglet dénommé : « confidentialité ».

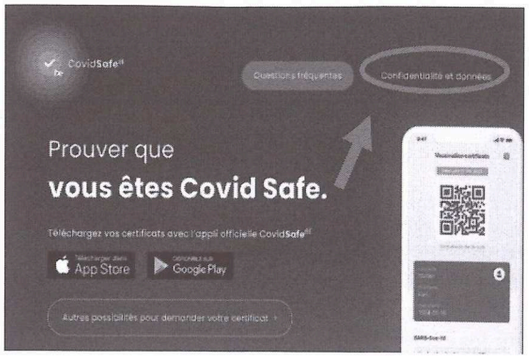
On y apprend par exemple que l'application est offerte à l'utilisateur par la plate-forme eHealth.

L'objectif de l'application est la récupération du certificat Covid numérique instauré par l'Union européenne[51] et garantissant la libre circulation des Européens dans l'Union sur pied de deux règlements :

– règlement (UE) n° 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats Covid-19 interopérables de vaccination, de test et de rétablissement (certificat Covid numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de Covid-19 ;
– règlement (UE) n° 2021/954 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat Covid numérique de l'UE) destinés aux ressortissants de pays tiers séjournant ou résidant légalement sur le territoire des États membres pendant la pandémie de Covid-19.

50 Art. 14 RGPD ; le G29 (devenu CEPD) dans ses Lignes directrices Transparence, énonçait qu'en tout état de cause, le délai maximal pendant lequel les informations doivent être fournies à une personne concernée est d'un mois.

51 Règlement (UE) n° 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats Covid-19 interopérables de vaccination, de test et de rétablissement (certificat Covid numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de Covid-19 et règlement (UE) n° 2021/954 du Parlement européen et du Conseil du 14 juin 2021, relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats Covid-19 interopérables de vaccination, de test et de rétablissement (certificat Covid numérique de l'UE) destinés aux ressortissants de pays tiers séjournant ou résidant légalement sur le territoire des États membres pendant la pandémie de Covid-19.



Ce cadre juridique européen fait suite à la Recommandation 2020/1475[52] relative à une approche coordonnée de la restriction de la libre circulation en réaction à la pandémie de Covid-19, afin de faciliter la circulation des personnes au sein de l'Union, notamment en précisant si ces dernières sont vaccinées, négatives à la suite d'un test ou rétablies.

Cependant, la réglementation autorise les États membres à utiliser ce certificat européen pour des mesures plus précises comme des concerts ou des festivals, dans le cadre de leur droit national, dans le respect du RGPD, notamment. En ce sens, la police de confidentialité précise :

– « Le certificat vous permettra de prouver que vous êtes vacciné contre la Covid-19, que vous avez obtenu un résultat de test négatif ou que vous êtes rétabli de la Covid-19. Le certificat peut être utilisé dans tous les États membres de l'UE, ainsi qu'en Islande, au Liechtenstein et en Norvège. Des discussions sont en cours avec la Suisse de sorte que le certificat puisse également être utilisé dans ce pays »[53].

52 Recommandation (UE) n° 2020/1475 du 13 octobre 2020 relative à une approche coordonnée de la restriction de la libre circulation en réaction à la pandémie de Covid-19.

53 Politique de confidentialité de l'application Covid Safe ticket, sous la mention « finalité », disponible à l'adresse : https://covidsafe.be/fr/confidentialite-et-donnees, consulté en dernier lieu le 20 décembre 2021.

L'utilisation de cette application est tout à fait libre. Les certificats de vaccination sont fournis par les entités fédérées, à savoir la Vlaams Agentschap Zorg en Gezondheid, l'Agence wallonne pour une vie de qualité, l'Office de la naissance et de l'enfance, la Commission communautaire française, le Ministerium der Deutschsprachigen Gemeinschaft. Les certificats de test et de rétablissement Covid numériques de l'UE sont, eux, délivrés par Sciensano, s'agissant d'une compétence fédérale.

Ce morcellement des acteurs est la conséquence du morcellement des compétences en matière de santé en Belgique. En effet, conformément aux dispositions de l'article 128 de la Constitution, les Communautés règlent par décret, chacune en ce qui les concerne les matières personnalisables qui comprennent, d'une part, la politique de santé (médecine préventive et curative) et, d'autre part, l'aide aux personnes (la protection de la jeunesse, l'aide sociale, l'aide aux familles, l'accueil des immigrés…), ainsi que le précise la loi spéciale du 8 août 1980 de réformes institutionnelles[54]. Pour le surplus, c'est l'État fédéral qui reste encore compétent, de sorte que l'utilisation des données dans le cadre des applications digitales fait l'objet d'un accord de coopération du 14 juillet, ayant reçu l'assentiment des parlements[55].

Par ailleurs, s'agissant de la transparence, certains pays ont rendu le code source de leurs applications ouvert, à savoir disponible en open source, pour plus de transparence et afin de renforcer la confiance du grand public. L'organisation Free Software Foundation Europe assure le suivi des applications. Selon une étude de l'Université allemande de Göttingen sur l'acceptation d'applications de suivi prototypes, les bénéfices pour la société de l'utilisation d'applications font partie des arguments les plus attrayants, même pour les personnes les plus sceptiques et indécises[56].

54 Art. 5, § 1er, I, al. 1er, 8o, de la loi spéciale du 8 août 1980 de réformes institutionnelles, *M.B.*, 15 août 1980.

55 Décret portant assentiment à l›accord de coopération du 14 juillet 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement des données liées au certificat COVID numérique de l'UE et au COVID Safe Ticket, le PLF et le traitement des données à caractère personnel des travailleurs salariés et des travailleurs indépendants vivant ou résidant à l'étranger qui effectuent des activités en Belgique.

56 S. Trang *et al.*, « One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps », *European Journal of Information Systems*, 2020, disponible sur le site: www.tandfonline.com/doi/full/10.1080/0960085X.2020.1784046, consulté en dernier lieu le 20 décembre 2020.

Tableau de quelques pays qui publient le code source des applications[57]

Pays	Nom de l'application	URL Open Source
Belgique	COVID Safe Ticket	https://github.com/covid-be-app
Pays-Bas	Coronamelder	https://github.com/minvws
Irlande	Covid Tracker	https://github.com/HSEIreland/
France	STOPCOVID	https://github.com/ct-report/FR
Danemark eRouška	eRouška "eFaceMask"	https://github.com/covid19cz?q=erouska
Suisse	SwissCovid	https://github.com/ct-report/CH
Maroc	Wiqaytna	https://github.com/Wiqaytna-app
Finlande	Ketju	https://github.com/ct-report/FI

c. Les exceptions à l'obligation d'information

Si l'information est la règle en ce qu'elle est une des mises en œuvre du principe de transparence, le RGPD énonce, en ses articles 13, § 4, et 14, § 5, les exceptions à cette obligation comme suit:

- «Art. 13. § 4. Les paragraphes 1, 2 et 3 ne s'appliquent pas lorsque, et dans la mesure où, *la personne concernée dispose déjà de ces informations*[58].»
- «Art. 14. § 5. Les paragraphes 1 à 4 ne s'appliquent pas lorsque et dans la mesure où:
  a. la personne concernée *dispose déjà de ces informations*;
  b. la fourniture de telles informations *se révèle impossible* ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve des conditions et garanties visées à l'article 89, § 1er, ou dans la mesure où l'obligation visée au paragraphe 1er du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles;

57 À partir du tableau, mis à jour, du Conseil de l'Europe, *in* « Solutions numériques pour lutter contre la covid-19: rapport sur la protection des données 2020 », Conseil de l'Europe, octobre 2020, p. 37.

58 Nous soulignons.

c. *l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée*; ou

d. *les données à caractère personnel doivent rester confidentielles* en vertu d'une obligation de *secret professionnel* réglementée par le droit de l'Union ou le droit des États membre[s], y compris une obligation légale de secret professionnel.»

Il découle des dispositions de ces articles qu'il peut être dérogé à l'obligation d'informer les personnes concernées, notamment lorsque la personne concernée dispose déjà de cette information ou lorsque la communication des données à caractère personnel est expressément prévue par la loi. La question n'est pas sans intérêt, notamment s'agissant des traitements des données opérés par des entreprises privées, telles que les restaurateurs, les écoles, les laboratoires.

À titre exemplatif, le «registre des clients de l'horeca» ou le *listing tracing* des clients de l'Horeca n'a pas manqué de faire parler de lui[59]. Ce registre fut rendu obligatoire par arrêté royal le 23 juillet 2020[60], à la suite du Conseil national de sécurité pour être *in fine* abandonné au profit du CST et du *Covid safe scan*.

En France, la CNIL, l'autorité de protection des données, a néanmoins veillé à adresser aux restaurateurs ses recommandations[61]. Elle y précise que les clients doivent être informés de l'objet de la collecte et des droits dont ils disposent concernant leurs données, et ce, au moment de la collecte, comme énoncé ci-avant. Cette communication doit se faire sous un format facilement accessible (p. ex., une mention d'information intégrée sur le formulaire papier à compléter par le client, un panneau d'affichage visible à l'entrée de l'établissement, etc.).

Elle rappela en outre que cette communication doit être claire, précise et simple, et comprendre (i) l'identité et les coordonnées de l'établissement, (ii) l'objectif de la collecte des données, à savoir faciliter le traçage des «cas contacts» par les autorités sanitaires, (iii) la durée de conservation des données de quinze jours maximum, (iv) les droits dont dispose la personne concernée, notamment le droit d'accès et de rectification, et (v) les éventuels destinataires, et en particulier à quelles autorités sanitaires pourraient être transmises ces données au cas où une infection au Covid-19 serait détectée.

À cet effet, elle partage un projet de communication à l'adresse des clients des restaurateurs.

59 Ph. Laloux, «Les registres dans l'horeca, c'était de l'amateurisme», *Le Soir*, mars 2021.

60 Arrêté royal du 23 juillet 2021 relatif à ...

61 CNIL, «COVID-19: les recommandations de la CNIL pour le cahier de rappel papier», 8 juin 2021, disponible sur le site: https://www.cnil.fr/fr/covid-19-les-recommandations-de-la-cnil-pour-les-cahiers-de-rappel-papier, consulté en dernier lieu le 20 décembre 2020.

Exemple de formulaire à utiliser pour les bars, restaurants et salles de sport

Établissements soumis au protocole sanitaire renforcé imposant la tenue d'un cahier de rappel

COVID-19 : vos coordonnées pour faciliter la recherche des « cas contacts »

Notre établissement est soumis au respect d'un protocole sanitaire spécifique, qui prévoit le recueil d'informations vous concernant, dans le cadre de la lutte contre l'épidémie de COVID-19.

Date et heure d'arrivée[1]:.....

Chaque client doit compléter les informations suivantes.

Nom :.....

Prénom :.....

Numéro de téléphone :.....

***

Les informations recueillies sur ce formulaire sont enregistrées et utilisées uniquement par notre établissement[2] : .....

.....

Conformément au protocole sanitaire applicable aux[3] ....., **vos données seront uniquement utilisées pour faciliter la recherche des « cas contacts » par les autorités sanitaires, et ne seront pas réutilisées à d'autres fins.**

En cas de contamination de l'un des clients au moment de votre présence, ces informations pourront être communiquées aux autorités sanitaires compétentes (agents des CPAM, de l'assurance maladie et/ou de l'agence régionale de santé), afin de vous contacter et de vous indiquer le protocole sanitaire à suivre.

Vos données seront conservées pendant 15 jours à compter de leur collecte, et seront supprimées à l'issue de ce délai.

Vous pouvez accéder aux données vous concernant, les rectifier ou exercer votre droit à la limitation du traitement de vos données.

Pour exercer ces droits ou pour toute question sur le traitement de vos données, vous pouvez contacter[4].....

.....

.....

Si vous estimez, après nous avoir contactés, que vos droits sur vos données ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL.

[1] A compléter par l'établissement

[2] A compléter par l'établissement : identité et coordonnées

[3] A compléter par l'établissement : type d'établissement

[4] A compléter par l'établissement : coordonnées téléphonique, postales ou électroniques pour contacter la personne de votre établissement qui sera chargée de répondre à la demande

Il s'ensuit que, même mobilisées par les autorités publiques dans la lutte contre le Covid-19, il semble que les entreprises privées soient tenues tant que faire se peut d'assurer leur obligation de communication. Ces recommandations sont d'application en France.

Cela étant dit, il n'est pas certain qu'en Belgique, ces traitements ne soient pas couverts par les exceptions relatives à l'obligation de communication et énoncées aux articles 13 et 14 du RGPD, à deux égards. Premièrement, étant institués par des dispositifs normatifs (règlement, loi, décret, ordonnance), ces traitements font déjà l'objet d'une belle publicité. Deuxièmement, les entités fédérées et l'État fédéral assurent une communication très large des modalités des traitements sur ces outils, de sorte qu'il est impossible pour un citoyen de ne pas trouver l'information aisément. Néanmoins, et en toutes circonstances, si l'absence d'une telle communication dans le chef des écoles ou restaurateurs nous semble difficilement être sanctionnable, réaliser cette obligation participe activement à la réalisation de l'obligation d'*accountability* ou de responsabilisation énoncée dans le RGPD en son article 5, § 2[62], à condition de communiquer de manière cohérente.

B. *Principe de minimalisation et de sécurité*

Ces premières étapes réalisées, il y a lieu de vérifier si les principes de minimisation et proportionnalité, ainsi que de sécurité et d'intégrité, sont également respectés.

1. Principe de minimisation

Le principe de minimisation et de proportionnalité consacré par l'article 5, 1., c)[63], consiste, d'une part, à s'interroger sur la nécessité de traiter des données à caractère personnel pour atteindre les finalités recherchées par le traitement et, d'autre part, à limiter le traitement des données au minimum, en ce qui concerne[64] :

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

62 Suivant cet article, un responsable du traitement est capable de démontrer à tout moment le respect des principes et obligations découlant du Règlement.

63 Art. 5.c) de la Convention n° 108+.

64 En ce sens, la décision de l'APD: Gegevensbeschermingsautoritait (GBA), Geschillenkamer, « Betreft: Klacht wegens gebruik van de elektronische identiteitskaart voor de aanmaak van een klantenkaart », Beslissing ten gronde 06/2019 du 17 septembre 2019, disponible à l'adresse: www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/BETG062019_web.pdf#overlay-context=nieuws/de-gegevensbeschermingsautoriteit- berispt-de-fod-volksgezondheid, consulté en dernier lieu le 20 décembre 2021.

Dès lors, il y a lieu d'évaluer :

- la pertinence du traitement, à savoir si le traitement permet de réaliser la finalité (test de pertinence) ;
- l'adéquation ou la nécessité au sens strict du traitement en vue de la réalisation de la finalité (test de nécessité ou subsidiarité) ;
- la proportionnalité, à savoir s'il y a un juste équilibre entre les intérêts, droits et libertés en présence (test de proportionnalité)

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'urgence[65].

À titre d'exemple, il semble opportun de s'attarder sur l'application de ce principe au CST, en examinant notamment l'appréciation récente de l'APD en son avis n° 232/2021. L'APD, dans un premier temps, revient sur la nécessité du CST comme suit :

- « Le droit au respect de la vie privée et [celui] à la protection des données à caractère personnel ne sont toutefois pas absolus et peuvent être limités si cela s'avère nécessaire dans une société démocratique pour atteindre un objectif d'intérêt général, c'est-à-dire qu'il faut démontrer que le recours au CST est une mesure pertinente (c'est-à-dire efficace pour atteindre l'objectif légitime qui est poursuivi), nécessaire (c'est-à-dire qu'il n'y a pas de mesure alternative moins attentatoire aux droits et libertés qui permettent d'atteindre cet objectif) et proportionnée à l'objectif qui est poursuivi (c'est-à-dire qu'il y a un juste équilibre entre les intérêts, droits et libertés en présence) »[66].

Ensuite, elle énonce la finalité de l'application, comme suit :

- « [c]omme l'Autorité l'a relevé dans ses avis précédents, le CST *vise à limiter la circulation du virus dans la population*, en créant des lieux plus sûrs et à moindre risque de transmission du virus, afin d'éviter une saturation du système hospitalier, tout en évitant de nouvelles fermetures de sec-

65 Art. 5, § 1er, d), RGPD.

66 APD, avis n° 232/2021 du 15 décembre 2021 concernant un projet d'accord de coopération visant à la modification de l'accord de coopération du 14 juillet 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement des données liées au certificat COVID numérique de l'UE et au COVID Safe Ticket, le PLF et le traitement des données à caractère personnel des travailleurs salariés et des travailleurs indépendants vivant ou résidant à l'étranger qui effectuent des activités en Belgique et un projet d'accord de coopération d'exécution visant à la modification de l'accord de coopération d'exécution du 15 octobre 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement des données liées au certificat COVID numérique de l'UE et au COVID Safe Ticket, le PLF et le traitement des données à caractère personnel des travailleurs salariés et des travailleurs indépendants vivant ou résidant à l'étranger qui effectuent des activités en Belgique (CO-A-2021-257 & CO-A-2021-258),

teurs déterminés. Comme l'Autorité a déjà eu l'occasion de le souligner dans ses avis précédents, un tel objectif est légitime »[67].

Une fois la finalité établie, à l'aide d'éléments concrets et factuels, l'APD examine les critères de pertinence (i), de nécessité (ii) et de proportionnalité (iii) du recours au CST, rappelant qu'il s'agit d'un dispositif particulièrement attentatoire à la vie privée de l'ensemble de la population.

Ces éléments doivent prendre en compte l'état des connaissances au moment de l'élaboration du projet de norme. Ainsi, l'APD revient sur les déclarations du directeur de l'OMS fin novembre 2021, qui a déclaré que le variant Delta, très contagieux, avait réduit à 40 % l'efficacité des vaccins contre la transmission de la maladie[68].

Dans ce contexte, l'APD précise que, par ailleurs, « le CST n'avait pas réussi à diminuer la circulation du virus[3] et qu'il pouvait, au contraire, donner un faux sentiment de sécurité »[69]. Partant, le rapport du GEMS du 14 novembre 2021 propose même aux autorités d'abandonner les termes de « Covid Safe Ticket » et de les remplacer par « Covid pass »[70].

Enfin, elle ne manque d'expliquer en guise de rappel ce qui suit :

– « le CST n'était pas un moyen efficace pour atteindre cet objectif, l'ingérence dans le droit au respect de la vie privée qu'il génère ne serait pas justifiée »[71]. L'Autorité soulignait déjà, dans son avis n° 163/2021, « que plusieurs études scientifiques récentes, réalisées notamment par des instituts de santé publique, tendent à montrer que le vaccin limite fortement, mais n'empêche pas, que les personnes vaccinées puissent être infectées et transmettre le SARS-Cov-2 (en particulier le variant Delta qui est particulièrement contagieux). De même, la réalisation d'un test permet de déterminer si, au moment du prélèvement, la personne était ou non infectée par le SARS-Cov-2. Mais il n'est pas exclu que cette personne puisse néanmoins être infectée dans les 48 h qui suivent la réalisation de ce test. En outre, même si la fiabilité des tests est très élevée, elle n'est pas absolue. De plus, bien qu'il apparaisse qu'une infection récente réduise les risques de réinfection, elle ne l'empêche pas totalement. Au vu de ces éléments, l'Autorité relève que l'usage du CST pourrait entraîner un faux sentiment de sécurité puisque les personnes vaccinées, testées négatives ou rétablies disposent d'un CST leur permettant d'accéder aux "évènements de masse" et autres lieux "où la transmission et/ou la super propagation sont les plus probables" alors qu'il n'est pas exclu qu'elles puissent être infectées et transmettre le virus ; ce qui pourrait s'avérer contre-productif au regard de l'objectif poursuivi ».

67 *Ibid.*, p. 3.

68 AFP, « Avec le variant Delta, les vaccins ne sont efficaces qu'à 40 % contre la transmission du coronavirus, prévient l'OMS », *RTBF Info*, 24 novembre 2021 ; disponible sur le site : https://www.rtbf.be/info/societe/detail_avec-le-variant-delta-les-vaccins-ne-sont-efficaces-qu-a-40-contre-la-transmission-du-coronavirus-previent-l-oms?id=10885137, consulté en dernier lieu le 20 décembre 2021 ; voy. également H. Angot, « Le CST encore vraiment bénéfique ? Marius Gilbert ne semble pas vraiment convaincu... », *RTBF Info*, 30 novembre 2021, disponible sur le site : https://www.rtbf.be/info/belgique/detail_le-cst-encore-vraiment-benefique-marius-gilbert-ne-semble-pas-vraiment-convaincu?id=10888992, consulté en dernier lieu le 20 décembre 2021

69 https://www.levif.be/actualite/sante/yves-van-laethem-sur-la-3e-dose-saint-nicolas-apporte-des-cadeaux-avant-l-heure-il-faut-les-prendre/article-normal-1488915.html, consulté en dernier lieu de 20 décembre 2021 ; voy., en ce sens, le rapport du GEMS du 25 novembre 2021 dans lequel il indique que : « *The use of the CST alone creates a false sense of security.* »

70 « *It creates the false impression that a "Covid Safe Ticket" allows one to have close contacts, hug each other and shake hands* », *in* GEMS, Rapport du 14 novembre 2021.

71 APD, *ibid.*, p. 6

On ne peut que lui donner raison. La question de la proportionnalité de l'utilisation du CST mérite à tout le moins un examen régulier des autorités, et notamment des parlements, au risque d'habituer la population à ce suivi permanent, alors que le Covid-19 semble établir ses quartiers pour un certain temps. C'est également l'avis de la cour d'appel de Liège qui rappelle, en son arrêt du 7 janvier 2021, que, si le CST peut apparaître comme une restriction proportionnée de liberté, ce n'est qu'en raison de son caractère temporaire, son prolongement nécessitant un examen réel de la situation scientifique[72].

Hautement intrusif dans la vie privée des gens, la permanence d'un tel contrôle n'est ni nécessaire ni souhaitable.

2. Principe de sécurité et intégrité

À la « minimisation », on ajoutera le principe de sécurité affirmé entre autres aux articles 5 et 32 du RGPD. Selon ce principe, les mesures de sécurité nécessaires et adéquates doivent également être prises en vue de protéger les données à caractère personnel[73], particulièrement quand il s'agit de données sensibles telles que les données de santé nécessaires à la gestion d'une pandémie. Cette obligation à charge du responsable du traitement de sécuriser de manière adéquate les données à caractère personnel qu'il traite sous-tend l'ensemble des obligations en matière de protection des données à caractère personnel[74].

Ces mesures doivent assurer un niveau de sécurité approprié, eu égard à 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[75]. Le RGPD énonce en son article 32 à titre exemplatif un certain nombre de mesures techniques et organisationnelles appropriées :

1. la pseudonymisation et le chiffrement des données à caractère personnel ;

72 Liège (12e ch. A), 7 janvier 2022, R.G. n° 2021/RF/24, pp. 33-34, inédit.

73 Art. 32 RGPD.

74 Voy., en ce sens, art. 25, 28, 26, 32 à 35.

75 Art. 32 RGPD.

2. des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité/accessibilité et la résilience constante des systèmes et des services de traitement. À titre d'exemple, le responsable du traitement et le sous-traitant devront prendre des mesures afin de garantir que les personnes physiques agissant sous leur autorité et ayant accès aux données à caractère personnel ne les traitent que sur leur instruction et dans le respect des procédures mises en place[76]. Peuvent y contribuer la traçabilité des accès et une politique de gestion des mots de passe dynamiques;
3. 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, à l'instar des plans de continuation, de reprise d'activité ou de secours informatique avec une politique de sauvegarde appropriée des données;
4. une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles mises en place pour assurer la sécurité du traitement.

En toute hypothèse, le choix d'une mesure au détriment d'une autre doit se fonder sur l'analyse des risques attachés à chaque utilisation du point de vue des libertés individuelles. Ces risques peuvent s'apparenter à ce que le RGPD définit sous le vocable «violation des données»[77], entendu comme la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral à l'égard de la personne concernée. En toutes circonstances, la survenance d'un des risques ci-avant énoncés nécessite une notification de la violation, notamment à l'APD, conformément aux dispositions de l'article 72 du RGPD.

Enfin, en vue d'éviter ces risques, en cas de traitements dits à haut risque[78], l'article 35 du RGPD impose une obligation particulière d'évaluation, connue sous le nom d'«Analyse d'impact relative à la protection des données» (ou 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, [...]», à savoir notamment les données de santé.

Il s'ensuit que les applications utilisées par l'État dans le cadre de la lutte contre le coronavirus doivent être considérées comme des applications à haut risque.

76 Art. 28 et 29 RGPD.

77 Sur cette obligation du responsable d'ouvrir la consultation et la nécessité de motivation en cas de non-consultation: voy. not. les lignes directrices du Groupe de l'article 29, *WP 248*, pp. 18-19, et surtout les Recommandations émises par la Commission belge de la protection de la vie privée, n° 01/2018, pp. 31-32.

78 Art. 35.1 RGPD.

Elles sont toutes développées à grande échelle et concernent des données de santé[79]. Ajoutons que l'article 35, 9., du RGPD réclame, en outre, une évaluation participative, multidisciplinaire et, si possible, multistakeholders des risques[80] et, ajoute l'article 36, «continue», afin de pouvoir à tout moment adapter le système aux évolutions de la pandémie. Au terme de cette procédure, si les mesures prises témoignent d'un risque élevé, conformément à l'article 36, 1., du Règlement, cette analyse d'impact entraîne l'obligation de consultation de l'APD. Dans ce cas, l'APD réagira, le cas échéant, pour proposer des mesures complémentaires de réduction des risques.

Dans ce contexte, il est regrettable et surprenant d'apprendre par la presse qu'une faille de sécurité a été découverte sur l'application CST, affectant les données de plus de 39.000 personnes. Pratiquement, le CST doit être lu et validé grâce à l'application *CovidScan* qui, dans le cas des personnes vaccinées, vérifie avant validation du ticket si la personne n'a pas récemment été soumise à un test PCR qui se serait révélé positif. Cette vérification se ferait à l'aide d'une liste chiffrée. C'est à cette étape du processus de scan que le CST présente une faille de sécurité observée par un citoyen. Ainsi, la presse relaye ce qui suit:

– «Le "bug" avait été découvert par Guillaume Derval, chercheur en science informatique de l'UCLouvain. En résumé: pour vérifier si le CST est valide, l'application doit vérifier que le QR Code de la personne n'est pas repris dans une liste reprenant toutes les personnes vaccinées, mais dont un test Covid s'est révélé positif. L'ingénieur s'est étonné de voir cette liste, remise à jour régulièrement, être accessible sur le Web. Pour l'ouvrir, il faut néanmoins disposer d'une "clé" de cryptage. Or, celle-ci, hébergée directement dans l'application, peut être très facilement dénichée. Un niveau de Bac 3 en informatique suffit. Aucun piratage, donc, puisque l'on donne la clé qui permet d'ouvrir le fichier circulant sur le Web... Dans un communiqué, l'APD confirme avoir "pris connaissance d'une potentielle faille de sécurité relative à la validation et la lecture des Covid Safe Tickets via l'application CovidScan"»[81].

Le 21 octobre 2021, l'Autorité de protection des données confirme bien une «fuite de données» à caractère sensible à la suite de la faille de sécurité découverte par un chercheur de l'UCLouvain. Les données traitées dans le cadre du CST étant très sensibles, l'APD prend cette potentielle violation de données très au sérieux[82].

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

80 274.

81 Ph. Laloux, «Vie privée: les failles du Covid Safe Ticket débusquées», *Le Soir*, 13 octobre 2021.

82 APD, «L'APD se penche sur une potentielle faille de sécurité de l'application CovidScan», 13 octobre 2021, complété le 21 octobre 2021, disponible sur le lien: https://www.gegevensbeschermingsautoriteit.

Cet incident rappelle l'importance de prendre en compte d'autres valeurs dans l'examen des mesures à mettre en place dans le cadre de la gestion de la crise sanitaire. Trois valeurs éthiques nous paraissent incontournables : l'autonomie, l'égalité et la non-discrimination, guidant la justice sociale et la dignité que la Charte européenne des droits fondamentaux et la Convention européenne des droits de l'homme obligent à prendre en compte[83]. La justice sociale nous oblige à veiller à ce que les mesures prises n'excluent personne, et la dignité des personnes[84] bannit la surveillance de tous les instants des personnes concernées et leur manipulation.

Force est de constater qu'à l'ère du numérique, le droit à la protection des données semble s'autonomiser de sa grande sœur, le respect de la vie privée, en faveur d'une corrélation encore plus importante avec ses droits fondamentaux cousins, tels que l'égalité, la non-discrimination et la dignité.

Section 2
Les spécificités des traitements liés à la gestion de la pandémie

Ce cadre légal posé, il est opportun de vérifier les spécificités des traitements propres à la pandémie, en s'attardant sur, d'une part (§ 1), les traitements des données relatives à la santé, notamment en faveur de la recherche et, d'autre part (§ 2), les traitements numériques des données à grande échelle, particulièrement s'agissant de la surveillance massive et de l'utilisation de l'intelligence artificielle dans la gestion de la crise.

§ 1. Traitement des données relatives à la santé dans la recherche scientifique

La pandémie et la découverte progressive du virus et de ses variants amènent une volonté, bien légitime, de recherche scientifique. Qui dit recherche en matière médicale dit traitement de données relatives à la santé qui bénéficient d'un régime de protection particulier dans le RGPD.

Le Comité européen de la protection des données (ci-après « EDPB ») a très rapidement travaillé sur cette question et a rendu des recommandations adoptées le 21 avril 2020 afin de « mettre en lumière les plus urgentes de ces [questions juridiques relatives à l'utilisation de données concernant la santé au sens

be/citoyen/lapd-se-penche-sur-la-potentielle-faille-de-securite-de-lapplication-covidscan, consulté en dernier lieu le 20 décembre 2021.

83 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.

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

de l'article 4, point 15), du RGPD] telles que la base juridique, la mise en place de garanties adéquates pour ce traitement de données concernant la santé et l'exercice des droits des personnes concernées »[85].

En guise de préambule et afin de couper court à toute tentative de rendre le RGPD coupable de restreindre la recherche, l'EDPB a précisé que le RGPD « n'entrave pas les mesures prises dans le cadre de la lutte contre la pandémie de COVID-19 »[86] et qu'il est « un vaste texte législatif qui prévoit plusieurs dispositions permettant de gérer le traitement de données à caractère personnel aux fins de la recherche scientifique liée à la pandémie de COVID-19 dans le respect des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel »[87].

La *première question juridique* qui se pose porte sur la base juridique du traitement de données effectué. Pour cela, l'EDPB va travailler sur les articles 6 et 9 du RGPD. Avant d'aller plus avant, l'on peut s'étonner que l'EDPB mentionne l'article 6 du RGPD alors que les données relatives à la santé sont visées à l'article 9 du même Règlement. Il nous semble qu'effectuer une application cumulative des articles 6 et 9 du RGPD est illogique et ne correspond pas à l'économie du RGPD. S'il est vrai que le RGPD n'est pas clair à ce propos en termes de titre de chapitre ou de section, il n'en demeure pas moins qu'il opère une différenciation entre, d'une part, les données appartenant à des catégories particulières de données à caractère personnel appelées sensibles dans la directive 95/46 et, d'autre part, les autres catégories de données. En effet, les premières sont traitées dans l'article 9, tandis que les secondes le sont dans l'article 6. De plus, lorsqu'on lit les considérants relatifs à ces deux articles, l'on observe tout autant cette différenciation. Par ailleurs, la méthode d'analyse imposant de trouver une base de licéité dans l'article 6 puis, en cas de données sensibles, en chercher une seconde dans l'article 9 est un non-sens, d'autant plus que, finalement, c'est la finalité trouvée à l'article 9 qui sera utilisée. Le RGPD est déjà suffisamment complexe sans le complexifier davantage par des règles cumulatives entre les articles 6 et 9. Un autre élément allant dans le sens d'une application exclusive des deux articles tient également au fait que le RGPD n'a pas modifié les principes fondamentaux de protection des données à caractère personnel figurant dans la directive 95/46. Or cette dernière n'imposait pas cette application cumulative et rien dans le RGPD n'indique que le législateur européen a modifié ce principe. Il nous semble donc que l'EDPB commet une

85 EDPB, Lignes directrices 03/2020 sur le traitement de données concernant la santé à des fins de recherche scientifique dans le contexte de la pandémie de COVID-19, 21 avril 2020, p. 4, point 2. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_fr.pdf.

86 EDPB, *idem*, p. 4, point 4 ; voy. également la déclaration du Comité européen de la protection des données du 19 mars 2020 sur le traitement des données à caractère personnel dans le contexte de l'épidémie de Covid-19, https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context- covid-19-outbreak_fr.

87 EDPB, *ibid.*

erreur de méthodologie dans la recherche des bases de licéité lorsque le traitement porte sur des données sensibles ; erreur qui complexifie inutilement et illogiquement le travail des responsables du traitement. Cependant, et nous ne pouvons le nier, certaines exceptions permettant au responsable du traitement de déroger à certains droits des personnes concernées ne s'appliquent qu'à l'article 6 et non 9 comme ils auraient dû. Il s'agit manifestement d'erreurs matérielles du législateur européen que l'EDPB tente de pallier en procédant à un cumul entre les articles 6 et 9 du RGPD. Mais est-ce vraiment son rôle ou ne conviendrait-il pas qu'il alerte le législateur sur ces erreurs ? Ce serait plus indiqué, mais en a-t-il le courage ?

Sur cette question de base de licéité, l'EDPD a identifié le consentement, mais également d'autres bases qui seraient exploitées par les États membres, telles que l'intérêt public ou la recherche scientifique conjointement avec l'article 89 du RGPD. Précisons qu'au niveau belge, le législateur a réglé la question de recherche scientifique au titre 4 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Une *deuxième question juridique* soulevée par l'application du RGPD à la recherche scientifique impliquant des traitements de données à caractère personnel concerne l'information de la personne concernée. Si, dans de nombreux cas, la recherche porte sur des données qui n'ont pas été obtenues directement auprès des personnes concernées, il n'en demeure pas moins que le responsable du traitement doit procéder à une information à moins qu'il se trouve dans une des exceptions visées à l'article 14 du RGPD. Ainsi en va-t-il lorsque l'information se révèle impossible, impliquerait des efforts disproportionnés, compromettrait gravement la réalisation des objectifs ou que l'obtention ou la communication des données à caractère personnel sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis. Toutes ces exceptions pourraient être mobilisées par un responsable du traitement dans le cadre de projets de recherche. L'on attire cependant l'attention sur une application restrictive de ces exceptions[88].

Une *troisième question juridique* soulevée est la compatibilité des finalités de recherche avec les finalités initiales. L'article 5, § 1er, point b), du RGPD établit que « le traitement ultérieur à des fins [...] de recherche scientifique [...] n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales ». Cependant et comme le rappelle l'EDPB :

> *44. L'article 89, paragraphe 1, du RGPD dispose que le traitement de données à des fins de recherche « est soumis[...] à des garanties appropriées » et que ces « garanties garantissent la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière ».*
>
> *45. Les exigences posées par l'article 89, paragraphe 1, du RGPD mettent en évidence l'importance du principe de minimisation des données et le principe d'intégrité et de confidentialité, ainsi que le principe de protection des données dès la conception et par défaut (voir ci-dessous)[16]. En conséquence, compte tenu de la nature sensible des données concernant la santé et des risques inhérents à la réutilisation de ces données à des fins de recherche scientifique, des mesures fortes doivent être prises afin de garantir un niveau de sécurité approprié tel qu'exigé par l'article 32, paragraphe 1, du RGPD*[89].

À noter que la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel fixe des règles en matière de recherche scientifique dont le respect permet de considérer que le traitement ultérieur est compatible avec le traitement initial.

La *quatrième question juridique* porte sur la mise en œuvre du principe de minimisation imposant au responsable du traitement « de préciser les questions de recherche et d'évaluer le type et le volume des données nécessaires pour répondre de manière appropriée à ces questions »[90]. Et l'EDPB de préciser que « les données nécessaires dépendent de la finalité de la recherche même lorsque celle-ci est de nature exploratoire, et elles devraient toujours respecter le principe de limitation des finalités énoncé à l'article 5, paragraphe 1, point b), du RGPD »[91] et qu'« il convient de noter que les données doivent être anonymisées lorsqu'il est possible d'effectuer la recherche scientifique avec des données anonymisées »[92]. Ce principe de minimisation implique également une évaluation de la durée de conservation des données à caractère personnel. Si le RGPD donne quelque latitude en matière de recherche, il n'en demeure pas moins que le responsable du traitement devra mettre en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée. Afin de rencontrer les exigences du RGPD en matière de conservation des données, l'EDPB précise qu'« afin de définir les durées de conservation (délais), des critères tels que la durée et l'objet de la recherche devraient être pris en compte. Il convient de noter que des dispositions nationales peuvent également établir des règles relatives à la durée de conservation »[93].

Au niveau des droits de la personne concernée, le RGPD offre la possibilité pour le responsable du traitement de les restreindre dans le respect de la légis-

88 Voy. Groupe de travail de l'article 29, Lignes directrices sur la transparence au sens du règlement (UE) n° 2016/679, 11 avril 2018, *WP 260*, rév.01, 17/FR, p. 34 (approuvées par le Comité européen de la protection des données), https://ec.europa.eu/newsroom/article29/item- detail.cfm?item_id=622227.

89 CEPD, Lignes directrices 03/2020 sur le traitement de données concernant la santé à des fins de recherche scientifique dans le contexte de la pandémie de Covid-19, 21 avril 2020, p. 11, points 44-45, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_fr.pdf.

90 CEPD, *ibid.*, p. 11, point 46.

91 CEPD, *ibid.*

92 CEPD, *ibid.*

93 CEPD, *ibid.*, p. 11, point 48.

lation applicable, telle la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Au regard de ces divers développements, l'on constate que la recherche scientifique dans le cadre de la pandémie est possible et peut voir certains articles ne pas s'appliquer, mais se doit de respecter les garde-fous mis en place par le RGPD. Il n'en demeure pas moins qu'il est difficile d'échapper à un devoir d'information qui s'applique également aux autorités publiques, en ce compris le gouvernement qui semble l'oublier de manière chronique.

§ 2. Traitement numérique des données à grande échelle : de la surveillance massive à l'intelligence artificielle (IA)

À l'ère dite du « Big Data », l'utilisation des données de santé par les applications de gestion de la pandémie renvoie autant aux masses de données numériques qu'à l'ensemble des techniques logicielles d'analyse de ces données, au rang desquelles se retrouvent le *data mining*[94], *machine learning*[95], *social network analysis*, ou encore le *predictive analytics*[96]. Les applications permettent au détour d'un algorithme ou l'autre de collecter sans précaution une quantité massive de données et de faire des corrélations avec ces dernières. Dans ce contexte, la quantité de données collectées par le gouvernement en vue d'endiguer le Covid-19 n'est pas sans risque et nécessite un détour par de la récente jurisprudence de la Cour européenne des droits de l'homme (ci-après, « Cour EDH »), en matière de surveillance de masse à savoir les arrêts *Centrum för Rättvisa c. Royaume de Suède* (ci-après, « l'arrêt *Centrum* ») et *Big Brother Watch et autres c. Royaume-Uni* (ci-après, « l'arrêt *Big Brother* ») (A), rendus tous deux le 25 mai 2021, ainsi qu'un examen des garde-fous existant dans la mise en œuvre de l'intelligence artificielle (B).

A. *La surveillance de masse dans le cadre de la gestion de la pandémie*

La surveillance des citoyens par leur État n'est pas un phénomène nouveau ou lié à la pandémie. Néanmoins, il est, de plus en plus, fait appel à de l'IA et notamment pendant cette gestion de crise. On retrouve une première forme organisée de service secret de surveillance sous l'Antiquité, au I^er^ siècle avant notre ère, sous l'autorité de l'empereur Auguste : le *cursus publicus*[97]. Il s'agissait d'un service postal destiné en réalité à être un service de renseignement[98] afin

94 Le *data mining* peut se définir comme étant de l'exploration de données, du forage de données, de la prospection de données ou encore de l'extraction de connaissance à partir de données.

95 Il s'agit d'une science moderne permettant de découvrir des *patterns* et d'effectuer des prédictions à partir de données en se basant sur des statistiques, sur du forage de données, sur la reconnaissance de *patterns* et sur les analyses prédictives.

96 Considéré comme un type d'exploration de données, c'est un domaine de l'analyse statistique qui extrait l'information à partir des données pour prédire les tendances futures et les motifs de comportement.

97 H.-G. Pflaum, « Essai sur le *cursus publicus* dans le Haut-Empire », mémoires présentés par divers savants étrangers à l'Académie, 1940, p. 189, consulté en dernier lieu le 20 octobre 2021 sur le site : https://www.persee.fr/doc/mesav_0398-3587_1940_num_14_1_1120.

98 *Ibid.*, p. 213.

de prédire les rébellions. La sortie de l'ère de la surveillance « traditionnelle » pour entrer dans l'ère de la surveillance « automatisée » n'est pas là simplement inscrite dans l'utilisation de nouvelles technologies. Dès les années 1980, la surveillance devenue plus massive grâce aux nouveaux moyens techniques de communication se trouve dans les mains de nouveaux acteurs. Aujourd'hui, chaque clic, chaque courriel générant des données et des métadonnées devient une source de revenus[99]. La surveillance de masse est la combinaison de plusieurs caractéristiques[100]. Premièrement, l'attention est désormais portée tant sur les métadonnées que sur la donnée elle-même[101]. Deuxièmement, cette nouvelle surveillance opère sur un principe de « collecte en masse, accès en détail »[102], grâce à l'utilisation d'un ensemble de technologies appelé les « Big Data », dont la notion n'est pas définie de manière unanime[103].

C'est dans ce contexte que la Cour EDH doit assurer la protection des droits fondamentaux lors des traitements des données et métadonnées par les États, par le biais de son article 8, mais également de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[104], devenue la Convention n° 108 +. En effet, attentif à une protection internationale poussée des données à caractère personnel, le Conseil de l'Europe[105] a adopté, le 18 mai 2018[106], un Protocole d'amendement[107] qui

99 Voy. en ce sens : S. Myers West, « Data capitalism : Redefining the logics of surveillance and privacy », *Business & Society*, vol. 58, n° 2, p. 25 ; A. Mondoux et M. Ménard, « Big Data et société. Industrialisation des médiations symboliques », *PUQ*, Études de communication, 52 | 2019.

100 P. Bernal, « Data gathering, surveillance and human rights: recasting the debate », *J Cyber Policy*, 1/2, 2019, p. 246.

101 Les métadonnées sont les données à propos des données, elles décrivent ou définissent une autre donnée et sont souvent générées automatiquement.

102 P. Bernal, « Data gathering, surveillance and human rights: recasting the debate », *op. cit.*, p. 246.

103 La CNIL, l'autorité française de protection des données, évoque un concept « encore flou et difficile à synthétiser », *in Les cahiers IP, Innovation et prospective*, n° 1, Vie privée à l'horizon 2020, Paroles d'expert, CNIL, Direction des Études, de l'Innovation et de la Prospective, 2012, p. 18. Elle pourrait néanmoins être analysée comme « un ensemble de technologies et de méthodes consistant à analyser, à des fins généralement prédictives, le flot de données produites par les entreprises, les organisations et les individus, mais aussi les objets s'ils sont connectés, dans des volumes et à une vitesse sans précédent ; [...], et qui engloberait les mails, SMS, photos, vidéos, commentaires ou changements de statuts sur les réseaux sociaux, sessions de connexion, relevés d'étiquettes ou de capteurs électroniques, signaux de géolocalisation, envoyés à foison chaque minute partout dans le monde ». Définition proposée par D. Cuny, *in* « Big Data is Big Business vraiment », *in La tribune*, le 3 avril 2013, consulté en dernier lieu le 20 octobre 2021, URL : http://www.latribune.fr/technos-medias/internet/20130403trib000757290/-big-data-is-big-business.-vraiment-.html.

104 Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg le 28 janvier 1981, approuvée par la loi du 17 juin 1991, *M.B.*, 30 décembre 1993, p. 29023, ci-après, « Convention n° 108 ».

105 Pour l'évolution des travaux législatifs, voy. également : Conseil de l'Europe, CAHDATA, 3^e^ réunion, Document de travail : Convention n° 108 avec son Protocole additionnel et propositions de modernisation, 9 avril 2014.

106 Art. 1^er^ de la Convention n° 108 : « Le but de la présente Convention est de protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère personnel, contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment du droit à la vie privée. »

107 Eu égard à l'évolution des technologies de l'information, de la vidéosurveillance, au recours en hausse aux identifiants biométriques, le Comité conventionnel de la Convention n° 108 avait lancé, en 2010,

modernise la Convention n° 108[108] pour donner naissance à la Convention n° 108+[109]. Il existe néanmoins une divergence majeure d'approche qu'il revient ici de souligner entre des garanties offertes, d'une part, par l'article 8 de la CEDH et, d'autre part, par la Convention n° 108. En effet, cette dernière, dès son intitulé, met au centre la protection de la personne concernée par le traitement et ses droits, de sorte que, dans un contexte de marchandisation des données à caractère personnel, l'individu et son intégrité physique et morale sont au centre du discours juridique[110].

La Cour EDH, sollicitée de manière régulière sur la question relative à la conformité des mesures de surveillance avec la CEDH, a développé une jurisprudence importante au départ de l'affaire *Klass e.a. c. Allemagne* en 1978[111]. De manière générale, lors de l'examen de la conformité à la CEDH des traitements de données à caractère personnel par une autorité publique, le contrôle de la Cour EDH se concentre en trois phases différentes. Premièrement, elle vérifie si la requête tombe dans le champ des droits protégés par l'article 8, § 1er, et établit la qualité de « victime » dans le chef des requérants. Deuxièmement, elle vérifie si l'État assume une obligation positive concernant les droits garantis, et enfin, troisièmement, si par ailleurs il s'en acquitte valablement. Une fois l'ingérence vérifiée et la qualité de « victime » établie, la Cour procède à l'analyse de facteurs autorisant les restrictions à l'article 8 de la CEDH, à savoir le critère de légalité, de légitimité et de nécessité (ou de proportionnalité), comme suit.

1. Critère de la légitimité

La Cour accorde une large marge d'appréciation aux États dans l'établissement du critère de légitimité[112]. Partant, de manière constante depuis 1978, la Cour accorde au législateur national un certain pouvoir discrétionnaire qui n'est toutefois pas illimité, examinant dès lors l'existence de garanties adéquates et suffisantes contre les abus et l'existence de recours adéquats.

2. Critère de légalité et nécessité des mesures de surveillance

Pour que ce critère soit garanti, l'ingérence doit être prévue par une loi s'agissant des mesures générales de surveillance, ce qui suppose l'adoption de la

une étude recensant les déficiences de la Convention, suivie d'une consultation publique en 2011, afin d'élaborer les pistes d'amélioration les plus adaptées possible, aboutissant ainsi à la dernière version de la Convention n° 108 adoptée en 2018 (STCE n° 223).

108 Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signé à Elseneur (Danemark) le 18 mai 2018. Entre la version originelle et le protocole d'amendement qui est actuellement à l'étape de ratification.

109 Afin d'assurer une facilité de lecture, les Conventions nos 108 et 108+ sont reprises sous les termes de Convention n° 108.

110 F. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *Rev. trim. dr. h.*, n° 108/2016, Bruxelles, Anthemis, 2016.

111 Cour eur. D.H., *Klass e.a. c. Allemagne*, 6 septembre 1978.

112 *Ibid.*, § 49.

mesure par un parlement. Pour ce qui est des mesures individuelles de surveillance, elles doivent se conformer aux conditions et procédures rigoureuses fixées par la législation elle-même. En outre, dans sa jurisprudence, ce critère est étroitement corrélé à celui de nécessité, élément essentiel dans la légalité de toute ingérence. La Cour a ainsi jugé que :

– « [...] la question de la légalité de l'ingérence est étroitement liée à celle de savoir si le régime institu[é] par la [loi] satisfait au critère de la "nécessité", raison pour laquelle la Cour doit examiner conjointement les critères de la "prévisibilité au regard de la loi" et de la "nécessité" »[113].

Dès lors, la Cour EDH vérifie simultanément si la mesure était « prévue par la loi » et si elle est « nécessaire », et évalue ainsi la proportionnalité du régime de surveillance au regard des buts légitimes poursuivis[114]. La surveillance dénoncée doit, dès lors, dans une société démocratique, être « nécessaire à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales ». La Cour vérifiera en deux étapes « si les moyens prévus par la législation en cause pour atteindre ce but restent à tous égards à l'intérieur des bornes de ce qui est nécessaire dans une société démocratique »[115]. Il y a lieu « d'évaluer la proportionnalité de la mesure de surveillance dans sa nature, compte tenu de sa portée et de ses caractéristiques technologiques »[116]. En outre, dès lors que la surveillance devient massive (non ciblée), l'État devra être à même de justifier en quoi une telle méthode est nécessaire à la préservation de l'objectif légitime défini, ce qui implique de pouvoir démontrer que seule une collecte massive de données permet d'assurer une protection contre les menaces soulevées (test de nécessité au sens strict)[117]. Deuxièmement, elle vérifie si le choix de la surveillance massive se justifie pour recueillir des informations essentielles à la préservation de l'intérêt légitime poursuivi, notamment la sécurité nationale, à l'exclusion de voies alternatives moins intrusives (test de subsidiarité).

3. Les garanties procédurales de « bout en bout »

Enfin, le dernier élément pertinent de l'examen opéré par la Cour consiste en un examen *in concreto* des procédures et mécanismes de contrôle *a priori* ou *a posteriori* à disposition des individus[118]. Dans sa jurisprudence *Big Brother*, elle

113 Cour eur. D.H., *Kennedy c. Royaume-Uni*, *op. cit.*, § 155.

114 F. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *Rev. trim. dr. h.*, n° 108/2016, Bruxelles, Anthemis, 2016, *op. cit.*, p. 863.

115 *Ibid.*

116 F. Dubuisson, « La Cour européenne des droits de l'homme et la surveillance de masse », *Rev. trim. dr. h.*, n° 108/2016, Bruxelles, Anthemis, 2016, p. 282.

117 Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, préc., § 52.

118 R. Angrisani, « Données personnelles et surveillance massive : quelle protection face aux ingérences des autorités publiques ? », *Revue québécoise de droit international*, 2020, § 1er.

introduit une nouveauté. La Cour y considère qu'afin de réduire autant que possible le risque d'abus, la surveillance de masse doit être encadrée par des « garanties de bout en bout »[119], de sorte que la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus. En outre, elle distingue la protection à octroyer à la surveillance ciblée de celle à octroyer à la surveillance de masse[120].

Enfin, la Cour établit les critères spécifiquement applicables à l'examen de conformité des mesures de surveillance de masse[121] afin d'assurer les garanties de « bout en bout ». Elle examine dès lors si le cadre juridique national définit clairement les éléments suivants :

> « 1. Les motifs pour lesquels l'interception en masse peut être autorisée ;
> 2. Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;
> 3. La procédure d'octroi d'une autorisation ;
> 4. Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;
> 5. Les précautions à prendre pour la communication de ces éléments à d'autres parties ;
> 6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;
> 7. Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ;
> 8. Les procédures de contrôle indépendant *a posteriori* du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement »[122].

In fine, dans l'arrêt *Big Brother Watch c. Royaume-Uni*, la grande chambre a jugé à l'unanimité que le régime d'interception massive des données violait l'article 8 de la CEDH. En effet, elle a estimé que le régime britannique souffrait de diverses lacunes. Premièrement, les mandats d'interception en masse n'étaient pas soumis à une autorisation indépendante. Les interceptions en masse étaient en effet autorisées par un ministre, et non par un organe indépendant de l'exécutif. Deuxièmement, les catégories de termes de recherche n'étaient pas mentionnées dans les demandes de mandat d'interception. Troisièmement, les termes de recherche liés à un individu, c'est-à-dire des « identifieurs » spécifiques tels que des adresses de courriels, n'étaient pas soumis à une autorisation interne préalable.

119 Cour eur. D.H. (gr. ch.), *Big Brother Watch et autres c. Royaume-Uni*, 25 mai 2021, § 350.

120 *Ibid.*, § 342.

121 La Cour fait référence au rapport de la Commission de Venise, selon lequel deux des garanties majeures dans un régime d'interception en masse sont l'autorisation et le contrôle du processus ; Cour eur. D.H., *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*, § 197.

122 Cour eur. D.H., *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*, § 361.

En conclusion, la Cour EDH opère ainsi un nouveau tournant dans sa jurisprudence en matière de surveillance de masse, en soulignant le développement d'obligations procédurales positives. Ces dernières visent notamment à garantir la transparence des traitements de données et l'accès à un recours effectif à charge des États, sous l'impulsion des obligations découlant du droit à la protection des données. Cette évolution jurisprudentielle témoigne d'un développement autonome du droit fondamental à la protection des données à caractère personnel. Elle semble tendre vers une logique plus managériale visant essentiellement à encadrer de manière optimale l'usage d'informations personnelles[14]. Cependant, paradoxalement, cette approche du risque d'abus pourrait être effectuée au détriment de l'article 8 de la CEDH, en ce qu'elle présente un risque significatif de perte de sens du droit à la vie privée au profit d'une approche managériale. Ainsi, au nom de la « lutte contre la pandémie », des atteintes toujours plus larges à la vie privée des personnes pourraient être admises, voire même *a fortiori* normalisées, au motif de l'existence de garanties procédurales adéquates.

B. *L'intelligence artificielle dans le cadre de la gestion de la pandémie*

Il n'aura pas fallu attendre la crise sanitaire du Covid-19 pour voir mobiliser les experts dans la rédaction de nouvelles lignes directrices et d'une législation encadrant l'intelligence artificielle en général. Ainsi, en avril 2019, un groupe d'experts indépendants a élaboré des lignes directrices éthiques pour l'intelligence artificielle[123] sous la supervision de la Commission. Par intelligence artificielle (ci-après, « IA »), il y a lieu d'entendre la branche de l'informatique qui vise à permettre aux ordinateurs et aux machines électroniques de reproduire un comportement intelligent, notamment en utilisant de grandes quantités de données[124].

Ces chercheurs plaident en faveur d'une utilisation de l'IA au service de l'humanité et de l'intérêt public afin d'améliorer le bien-être et la liberté de l'homme[125]. Tout au long de leur cycle de vie, les systèmes d'IA doivent toujours respecter les lois applicables, adhérer aux principes et valeurs éthiques et promouvoir la robustesse technique et sociétale[126], en se fondant sur une base sûre, sécurisée et fiable. Toutes les précautions doivent être prises pour éviter les

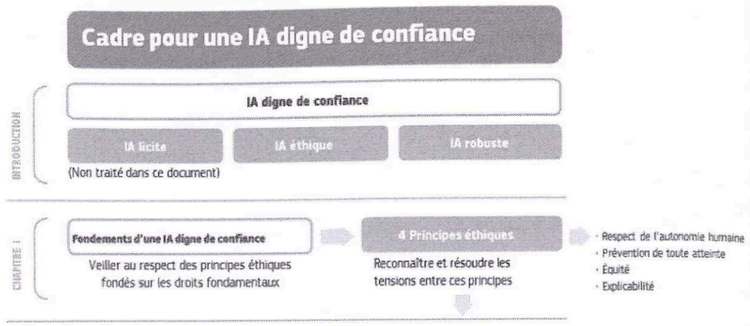
123 Groupe d'experts de haut niveau sur l'intelligence artificielle, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, Commission européenne, 8 avril 2019, 48 p.

124 European Commission, *Artificial Intelligence for Europe*, Brussels, 25 April 2018, COM(2018) 237 final, p. 1.

125 *Ibid.*, p. 8.

126 *Ibid.* ; voy. également : K. Karoe, A. Miyata-Sturm et E. Henden, « How to achieve trustworthy artificial intelligence for health », *Bull World Health Organ*, 2020, p. 98, disponible sur le site : https://www.who.int/bulletin/online_first/BLT.19.237289.pdf, consulté en dernier lieu le 20 décembre 2021.

conséquences négatives involontaires. Ces lignes directrices peuvent être résumées comme suit[127] :



En matière de gestion de pandémie, l'expérience de la gestion d'épidémies passées, comme Ebola, a montré que l'analyse des données de télécommunications par des systèmes d'intelligence artificielle permet de prévoir et d'anticiper la propagation des épidémies sur diverses zones géographiques et d'identifier les populations les plus à risque[128].

Actuellement, l'intelligence artificielle est utilisée pour venir porter appui à la lutte contre le Covid dans le monde entier. Il sera important que les systèmes d'IA utilisés pour lutter contre le Covid-19 ne conduisent pas à une perte de confiance du public[129]. Cela peut être le cas si l'on autorise la réaffectation de données personnelles identifiables traitées à d'autres fins non liées, ou si la justification de l'utilisation des données est mal communiquée, de sorte que cette technologie arrive en appui de mesures liberticides. À titre d'exemple, la Chine, premier épicentre de la maladie et réputée pour son avancée technologique en la matière, a tenté d'en tirer un avantage déterminant. Ses usages semblent néanmoins concerner tant l'appui à des mesures restrictives de circulation des populations que les prévisions d'évolution des foyers de la maladie ou la recherche pour l'élaboration d'un vaccin ou d'un traitement. Ainsi, l'IA semble avoir été employée pour accélérer le séquençage du génome, effectuer des diagnostics plus rapides, réaliser des analyses par scanner ou, plus ponctuellement, recourir à des robots de maintenance et de livraison[130].

127 Tableau du Groupe d'experts de haut niveau sur l'intelligence artificielle dans ses Lignes directrices en matière d'éthique pour une IA digne de confiance, p. 9, § 30.

128 World Economic Forum, Big Data, Big Impact: New Possibilities for International Development, 2012, p. 5, voy. http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf, consulté en dernier lieu le 20 décembre 2021

129 Voy. en ce sens: S. Callens et G. Pomes, «Artificial intelligence in healthcare and the impact of COVID-19 », *in* J. Herveg (éd.), *Deep Diving into Data Protection*, 1re éd., Bruxelles, Larcier, 2021, p. 392.

130 A. Chun, «In a time of coronavirus, China's investment in AI is paying off in a big way», *South China Morning Post*, 18 mars 2020.

L'expérience de l'utilisation de l'IA dans le cadre la gestion du Covid permet de tirer deux enseignements. Premièrement, en Europe, ni le RGPD ni la Convention n° 108 + ne devraient être modifiés en vue de l'utilisation de l'IA afin de lutter contre le Covid-19. Les obligations et principes généraux énoncés ci-avant, à savoir les principes généraux et les obligations en matière de protection des données, doivent pouvoir continuer à s'appliquer pleinement en toutes circonstances, notamment lors de l'utilisation de données biométriques, de la géolocalisation, de la reconnaissance faciale et de l'exploitation de données de santé. Le déploiement même en situation d'urgence doit s'effectuer en concertation avec les autorités de protection des données[131] et dans le respect de la dignité et de la vie privée des utilisateurs et des risques de discriminations[132].

Le second enseignement est qu'une approche européenne est nécessaire en la matière. À cet égard, il y a lieu de féliciter l'initiative de la Commission qui, afin d'éviter la fragmentation du marché intérieur, a publié, le 8 avril 2020, une recommandation pour l'établissement d'une boîte à outils commune de l'Union pour l'utilisation de la technologie et des données afin de combattre et de sortir de la crise du Covid-19, en particulier en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées[133]. La Commission promeut une approche européenne pour les applications mobiles Covid-19 et pour l'utilisation des données de mobilité pour la modélisation et la prédiction de l'évolution du virus[134]. La Commission indique que l'utilisation des applications mobiles d'alerte et de prévention du Covid-19 devrait respecter plusieurs principes, tels que (i) les garanties assurant le respect des droits fondamentaux et la prévention de la stigmatisation, en particulier les règles applicables en matière de protection des données à caractère personnel et de confidentialité des communications, (ii) la préférence pour les mesures les moins intrusives mais efficaces, y compris l'utilisation des données de proximité et l'évitement du traitement des données relatives à la localisation ou aux mouvements des personnes, et l'utilisation de données anonymes et agrégées lorsque cela est possible, (iii) l'expiration des mesures prises et l'effacement des données à caractère personnel obtenues par le biais de ces mesures lorsque la pandémie est déclarée maîtrisée, au plus tard, et (iv) le téléchargement des don-

131 En France, en Belgique, aux Pays-Bas et en Italie notamment, les autorités de protection des données ont été consultées avant le développement d'une application de suivi des contacts, ce qui a parfois entraîné des modifications importantes de la conception de l'application; voy. en ce sens: «Pandémie de coronavirus dans l'UE – Conséquences pour les droits fondamentaux» - Bulletin 2, Agence européenne des droits fondamentaux, 28 mai 2020, p. 47; disponible sur le site https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1, consulté en dernier lieu le 20 décembre 2020.

132 A.F. Cahn et J. Veiszlemlein, « COVID-19 tracking data and surveillance risks are more dangerous than their rewards », *NBC News*, 19 mars 2020.

133 Commission européenne, *8 avril 2020, on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*, C(2020) 2296 final, p. 8.

134 *Ibid.*

nées de proximité en cas d'infection confirmée et des méthodes appropriées pour avertir les personnes qui ont été en contact étroit avec la personne infectée, qui restent anonymes[135].

Ainsi, aujourd'hui, à défaut d'un cadre juridique spécifique dans le droit positif permettant d'encadrer le déploiement de l'IA, force est de constater que, s'agissant de la protection des droits fondamentaux, tant le RGPD que la Convention n° 180 ont fait œuvre utile.

Section 3
Application spécifique en droit belge

Le Covid-19 a lancé, dès mars 2020, la valse des arrêtés royaux de pouvoirs spéciaux pris sur la base de la loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus COVID-19. Certains de ces arrêtés royaux ont ensuite été confirmés par la loi du 24 décembre 2020 portant confirmation des arrêtés royaux pris en application de la loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus COVID-19[136]. Il s'agissait, pour le gouvernement fédéral, d'agir, dans un premier temps, dans l'urgence face à une pandémie dont il ne connaissait pas les effets. Des mesures similaires ont été prises au niveau des entités fédérées.

Il va sans dire que ces mesures ont généré des réactions diverses et variées avec l'apparition, entre autres, de positions quelque peu dogmatiques en matière, par exemple, de protection de la vie privée. En effet, certains n'ont pas hésité à élever ce droit fondamental au statut de droit absolu alors que l'article 8 de la CEDH prévoit des exceptions à ce droit.

Il est donc utile de se reporter à cet article 8 en vertu duquel :

> « 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. »

135 CEPD, Déclaration sur le traitement des données à caractère personnel dans le contexte de l'épidémie de Covid-19, adoptée le 19 mars 2020, p. 3 ; disponible sur le lien : https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_art_23gdpr_20200602_fr_1.pdf, consulté en dernier lieu le 20 décembre 2020.

136 http://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=21-01-15&numac=2021200012 (dernière consultation le 6 janvier 2022).

Si le premier alinéa assure la protection de la vie privée et, par extension, des données à caractère personnel, le second alinéa prévoit un pouvoir d'ingérence par les 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 8[137]. Et, parmi les buts légitimes, nous retrouvons celui de la protection de la santé. Une des exceptions à la protection de la vie privée réside donc dans la protection de la santé.

La Cour européenne des droits de l'homme a eu l'occasion de rappeler que, « si le droit à la santé ne fait pas partie en tant que tel des droits garantis par la Convention, les États ont l'obligation positive de prendre les mesures nécessaires à la protection de la vie des personnes relevant de leur juridiction et de protéger leur intégrité physique, y compris dans le domaine de la santé publique (*Lopes de Sousa Fernandes c. Portugal* [GC], n° 56080/13, § 165, 19 décembre 2017, *Vasileva c. Bulgarie*, n° 23796/10, §§ 63-69, 17 mars 2016) »[138].

Le Conseil d'État en a tiré la conclusion que « la protection de la santé en cas de situation d'urgence épidémique constitue par conséquent une obligation positive dans le chef des autorités publiques, et non un simple objectif légitime qu'il leur serait loisible de poursuivre »[139]. Elle tempère cependant cette conclusion en précisant que « cette obligation positive, à charge des autorités publiques en matière de protection de la santé, doit cependant être mise en balance avec d'autres obligations positives »[140] telles que le droit à l'enseignement, le droit au travail et au libre exercice d'une activité professionnelle, le droit à l'épanouissement culturel et social, la liberté de réunion et d'association, le droit de circuler librement, le droit au respect de la vie privée et familiale.

Nous retrouvons ainsi les ingrédients juridiques présents dans la crise du Covid-19. En vulgarisant le concept, la vie privée peut donc se voir limitée si la santé le requiert avec, bien entendu, des garde-fous.

En effet, il ne suffit pas que l'ingérence soit légitime, encore faut-il qu'elle soit, d'une part, prévue par la loi et, d'autre part, nécessaire dans une société démocratique incluant, comme le précise le Conseil d'État, la mise en balance avec d'autres libertés fondamentales. La jurisprudence de la Cour EDH considère que, pour que l'ingérence soit acceptable, il faut que 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

137 Cour eur. D.H. (gr. ch.), *Dubská et Krejzová c. République tchèque*, req. n^{os} 28859/11 et 28473/12, 15 novembre 2016, n° 166.

138 Cour eur. D.H. (5^{e} sect.), *Le Mailloux c. France*, req. n° 18108/20, 5 novembre 2020.

139 Projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 59.

140 Projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 59.

même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé (*A, B et C c. Irlande*, précité, § 220, avec d'autres références)»[141]. Il nous paraît pertinent de relever que le législateur, ou l'exécutif en cas de pouvoirs spéciaux tels que nous les avons connus entre mars et juillet 2020, pense une loi en termes d'efficacité, mais aussi de lisibilité. À force de vouloir mélanger les objectifs, les rédacteurs manquent de clarté dans leur pensée ou, à tout le moins, dans le contenu des textes.

En termes de nécessité, ou de proportionnalité, l'on ne peut pas oublier le principe selon lequel le législateur doit choisir la voie qui crée le moins d'ingérence dans la vie privée des justiciables. Il est bien évident que, dans le cadre de notre contribution, la discussion se portera à ce niveau.

À noter qu'en Belgique, la protection de la vie privée se voit consacrée dans l'article 22 de la constitution belge. Ainsi, «chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi». Cet article donne à la vie privée une protection très forte, mais pas absolue. Pour en analyser la portée, il y a lieu de porter notre attention vers d'autres textes.

Ainsi, la Cour constitutionnelle a considéré, dans un arrêt du 18 mars 2010, que «la Cour peut examiner si le législateur a respecté les obligations internationales qui découlent des dispositions invoquées de la directive précitée [ndr : directive 95/46/CE remplacée par le RGPD depuis] et de la convention n° 108 [du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel] auxquelles la Loi précitée du 8 décembre 1992 [ndr : relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel remplacée par le RGPD depuis] et ses modifications ultérieures donnent exécution. Ces obligations forment un ensemble indissociable des garanties qui sont reproduites à l'article 22 de la Constitution»[142].

Ainsi, la Cour réaffirme la filiation de l'article 22 de la Constitution avec les normes internationales qui sous-tendent le droit à la protection de la vie privée. Cela donne également une clé d'analyse de cet article 22 dès lors que les interprétations de l'article 8 de la CEDH rendues par la Cour européenne des droits de l'homme de Strasbourg lui sont applicables.

Cela a été confirmé une nouvelle fois, en d'autres termes, par la Cour qui a considéré qu'«il ressort des travaux préparatoires de [l']article [22] que le Constituant [a] cherché à mettre le plus possible la proposition en concordance avec l'article 8 de la Convention européenne de sauvegarde des droits de

141 Cour eur. D.H. (gr. ch.), *Dubská et Krejzová c. République tchèque*, req. n^{os} 28859/11 et 28473/12, 15 novembre 2016, n° 167.

142 C. const., 18 mars 2010, n° 29/2010, www.const-court.be ; nous soulignons.

l'homme et des libertés fondamentales (CEDH), afin d'éviter toute contestation sur le contenu respectif de l'article de la Constitution et de l'article 8 de la CEDH (*Doc. parl.*, Chambre, 1993-1994, n° 997/5, p. 2)»[143].

§ 1. La loi pandémie et la protection des données

Devant la diversité des bases légales nécessaires pour prendre des actes administratifs dans le cadre de la crise du Covid-19, le gouvernement a, le 27 avril 2021, déposé devant le Parlement un projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique. Il justifiait donc cette initiative par le fait que, «dans le cadre de la lutte contre la pandémie de COVID-19, les bourgmestres, les gouverneurs, le ministre-président bruxellois et le ministre de l'Intérieur ont été amenés à prendre des mesures de police administrative. Ces mesures ont été adoptées, selon le cas, sur la base de la nouvelle loi communale, de la loi provinciale, de la loi sur la fonction de police, de la loi du 31 décembre 1963 sur la protection civile et de la loi du 15 mai 2007 relative à la sécurité civile. Si ces différentes lois constituent une base légale adéquate, comme le Conseil d'État l'a jugé à titre provisoire à l'occasion de nombreux recours, il est cependant souhaitable de prévoir un ensemble de règles de police administrative spéciale, spécifiques aux situations d'urgence épidémiques. Cet ensemble de règles peut être appliqué à la pandémie de COVID-19 (dans la mesure où c'est encore nécessaire), ainsi qu'à d'éventuelles situations épidémiques futures»[144].

La spécificité du texte tel que présenté par le gouvernement fédéral est que «le pouvoir d'adopter des mesures de police administrative est attribué au Roi et, dans des situations extrêmement urgentes, au ministre de l'Intérieur. Lorsque les circonstances locales l'exigent, les gouverneurs et bourgmestres prennent des mesures renforcées, conformément aux éventuelles instructions du ministre de l'Intérieur»[145]. Le texte ne devrait cependant pas être un obstacle à l'«adoption éventuelle de mesures de police administrative générale dans le cadre de la législation existante, si la nécessité devait s'en faire sentir»[146].

Conscient que des règles supranationales s'appliquent aux matières visées par ce projet de loi, le gouvernement a précisé que :

> «les mesures de police administrative doivent toujours être strictement nécessaires, limitées dans le temps et proportionnées à l'objectif visé, en particulier

143 C. const., 10 novembre, n° 166/2011, www.const-court.be, B16.6. Voy. également C. const., 7 juillet 2011, n° 122/2011, www.const-court.be, B.3.

144 Projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 3.

145 Projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 3.

146 Projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 3.

> la protection de la santé publique et le droit à la vie». À ce sujet et après une analyse du projet de loi, le Conseil d'État a considéré que «l'article 5, § 1er, a) à g) [fixant les mesures de police administrative pouvant être prises par les autorités compétentes], de l'avant-projet de loi, combiné avec les autres dispositions de l'avant-projet de loi, répond d'une manière satisfaisante au principe de légalité tant formelle que matérielle»[147] dès lors que «l'avant-projet détermine de manière suffisante les "éléments essentiels" des mesures de police administrative à prendre par le pouvoir exécutif et, partant, également des éventuelles incriminations: d'une part, il contient en effet une liste limitative de mesures qui sont définies de manière suffisamment précise; d'autre part, l'avant-projet indique également de manière suffisante les circonstances dans lesquelles ces mesures peuvent être prises, à savoir dans une "situation d'urgence épidémique" dont l'existence doit être confirmée par le législateur et lorsqu'il existe des données scientifiques justifiant les mesures. L'exposé des motifs indique à ce sujet que "les mesures doivent être basées sur les connaissances scientifiques les plus récentes et doivent reposer sur des motifs matériels valables, dont l'existence factuelle peut être supposée et peut être prise en compte en justice pour justifier la décision". Enfin, les mesures pourront être attaquées en justice, aussi bien devant le Conseil d'État, section du contentieux administratif, que, par voie incidente, sur la base de l'article 159 de la Constitution»[148].

Dans le cadre de la présente contribution ne sera pas plus développé cet aspect de la loi.

Constatant que le projet de loi impliquait un traitement de données à caractère personnel au sens de l'article 4, 1., du RGPD, le gouvernement avait, initialement, rédigé un article 6 relatif au traitement de données à caractère personnel long de dix paragraphes; article qui a attiré les critiques de l'Autorité de protection des données, mais également du Conseil d'État, de députés et de juristes.

Un *premier axe* de cet article concernait le traitement de données dans le cadre de la surveillance des personnes par rapport aux mesures de police prises par les autorités compétentes telles que:

- la limitation de l'entrée au ou de la sortie du territoire belge;
- la fermeture de ou la limitation d'accès à une ou plusieurs catégories d'établissements ou parties des établissements recevant du public ainsi que des lieux de réunion;
- la limitation ou l'interdiction de la vente et/ou de l'utilisation de certains biens et services;

147 Projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 98.

148 Projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 99.

- l'interdiction ou la limitation des rassemblements;
- l'interdiction ou la limitation des déplacements;
- la fixation de conditions d'organisation du travail;
- la détermination des commerces, entreprises et services des secteurs privés et publics nécessaires à la protection des intérêts vitaux de la nation ou aux besoins essentiels de la population, qui doivent;
- la détermination des mesures physiques ou sanitaires.

Un *deuxième axe* concernait la «création de bases de données, les modalités de la mise en place et de la gestion de la banque de données»[149]. Le projet de loi laissait cependant au Roi, c'est-à-dire au gouvernement, la charge de déterminer les données à caractère personnel visées, les personnes concernées ainsi que la transmission de ces données à des tiers «après avis de l'autorité de contrôle de la protection des données compétente sur la création d'une banque de données ainsi que sur les modalités qui l'accompagnent et la gestion»[150]. Il est utile de noter que le projet de loi mentionnait «l'autorité de contrôle de la protection des données compétente», sous-entendant que plusieurs autorités seraient compétentes en matière de protection des données alors que la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après, «APD») précise, en son article 4, que «l'Autorité de protection des données exerce cette mission [de contrôle du respect des principes fondamentaux de la protection des données à caractère personnel, dans le cadre de la présente loi et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel], indépendamment du droit national applicable au traitement concerné, sur l'ensemble du territoire du Royaume»[151] et qu'elle «est l'autorité de contrôle compétente lorsqu'aucune autre loi n'en dispose autrement»[152]...

L'APD a rendu un avis très critique par rapport à ce texte mettant, entre autres éléments, l'accent sur de nombreuses lacunes et de trop grandes libertés laissées au gouvernement en matière de protection des données; libertés contraires à l'article 8 de la CEDH et du RGPD.

Ainsi, elle rappelle 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 objec-

149 Projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 36.

150 Projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 36.

151 Art. 4, § 1er, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

152 Art. 4, § 2, al. 2, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

tifs) qu'elle poursuit et qu'elle est *encadrée par une norme suffisamment claire et précise et dont l'application est prévisible* pour les personnes concernées.
En vertu de l'article 6.3 du RGPD, lu conjointement avec l'article 22 de la Constitution et l'article 8 de la CEDH, *il doit s'agir d'une norme légale formelle (loi, décret ou ordonnance,* ci-après, aussi appelée "la loi") définissant les éléments essentiels du traitement accompagnant l'ingérence publique. Dans la mesure où les traitements de données à caractère personnel accompagnant l'ingérence publique représentent une *ingérence importante* dans les droits et libertés des personnes concernées, ce qui semble pouvoir être supposé en l'espèce malgré l'absence de description des traitements de données envisagés), *la loi doit décrire clairement et précisément les éléments essentiels suivants*:
1. les finalités déterminées, explicites et légitimes des traitements de données à caractère personnel (voir chapitre IV);
2. le ou les responsables de chaque traitement de données à caractère personnel (voir chapitre III);
3. les (catégories de) données à caractère personnel qui seront traitées (et qui doivent être pertinentes et non excessives) (voir chapitre II);
4. les catégories de personnes concernées dont les données à caractère personnel seront traitées (voir chapitre I);
5. les catégories de destinataires des données à caractère personnel (ainsi que les raisons pour lesquelles ils recevront les données et les usages qu'ils en feront) (voir chapitre V);
6. le délai de conservation maximal des données à caractère personnel enregistrées.
Dans la mesure où la loi définit ces éléments essentiels, *les détails et modalités de ces traitements de données peuvent être précisés par le Roi* via arrêté royal, moyennant une délégation claire et précise en ce sens effectuée par la loi.»[153]

Sur la base de ce rappel, l'APD juge que «le pouvoir exécutif ne peut être habilité à définir les modalités d'un traitement de données que dans le cadre et en vue de l'exécution de mesures dont les éléments essentiels ont été définis préalablement par le législateur. Or l'avant-projet de loi ne définit pas les éléments essentiels et délègue à l'exécutif la tâche de définir ces éléments»[154]. Il est vrai qu'en déléguant la définition des éléments essentiels au gouvernement, le législateur enlève à la loi ses caractères de clarté, de précision et de prévisibilité. Ainsi que le rappelle l'APD, un arrêté royal doit être limité à préciser des modalités d'éléments prévus par la loi avec précision, clarté et permettant aux justiciable d'en prévoir les conséquences. À défaut, la base légale permettant l'ingérence dans la vie privée des individus manque. Nous devons cependant relever, ainsi que le Conseil d'État l'a précisé dans son avis, que, «même dans des matières réservées à la loi, des délégations de compétence plus étendues

153 APD, avis n° 24/2021 du 2 mars 2021, pp. 2-3; les soulignements sont de l'APD.
154 APD, avis n° 24/2021 du 2 mars 2021, pp. 2-3.

portant sur des "éléments essentiels" peuvent toutefois être accordées au pouvoir exécutif, mais sous des conditions strictes[155]»[156].

Afin de pallier ce problème, les auteurs du projet de loi avaient prévu une confirmation ou infirmation par la loi dans un délai de quinze jours à partir de leur entrée en vigueur, à défaut de quoi ils cessent de sortir leurs effets[157]. Cette formulation a cependant été critiquée par le Conseil d'état qui a jugé qu'«un tel mécanisme [de délégation à l'exécutif] ne peut toutefois être admis au regard des conditions strictes qui régissent la matière» et qu'afin de «respecter le principe de légalité inhérent à l'article 22 de la Constitution, lorsque les arrêtés n'ont pas été confirmés par le législateur dans le délai prévu, ils doivent être "réputés n'avoir jamais produit d'effets" (et non pas "cesser de produire leurs effets")». Cette modification a tout son sens dès lors que le fait de considérer que les arrêtés royaux sont réputés n'avoir jamais produit d'effet implique que les traitements de données effectués sur la base desdits arrêtés royaux devront être purement et simplement supprimés.

De plus, nous pourrions considérer que le délai de quinze jours pour une confirmation ou infirmation par le législateur était trop long dès lors que, même si les arrêtés royaux n'étaient pas confirmés par le législateur, ils auraient produit leurs effets durant quinze jours sans aucune légitimité au sens de la jurisprudence de la Cour EDH.

Outre ces problèmes de légalité, l'APD avait relevé des infractions à plusieurs principes du RGPD tels que ceux de minimisation, de traitement ultérieur compatible à la finalité initiale, etc.

En termes de traitement ultérieur, le projet de loi prévoyait, en son article 6, § 3, alinéa 2, que «des données à caractère personnel de banques de données existantes soient utilisées pour les finalités visées au § 2, alinéa 1er, 1° à 3°, ou nécessitent qu'une banque de données existante soit alimentée avec d'autres catégories de données, une telle utilisation ou un tel élargissement est consi-

155 « Dont, notamment: 1°) le fait qu'une telle délégation de compétences ne peut avoir lieu que dans des circonstances exceptionnelles dûment justifiées; 2°) l'exigence que la loi d'habilitation doit être formulée dans des termes aussi précis que possible; 3°) le fait que des garanties procédurales précises soient prévues au niveau de l'adoption des arrêtés soumis à confirmation (voir l'avis du Conseil d'État 68.309/1-3 donné le 24 novembre 2020 sur un avant-projet devenu la loi du 20 décembre 2020 portant des mesures de soutien temporaires à la suite de la pandémie COVID-19, p. 12); 4°) l'exigence d'une confirmation dans un bref délai; 5°) le fait de prévoir dans la loi d'habilitation que les arrêtés adoptés en vertu de celle-ci doivent être réputés n'avoir jamais produit d'effets lorsqu'ils n'ont pas été confirmés dans le délai imparti par la loi d'habilitation (voy. en ce sens: C. const., 1er décembre 2004, n° 195/2004, considérant B.16.3)» (voy. art. 6, § 10, du projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 120, note infrapaginale 180).
156 Art. 6, § 10, du projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 120.
157 Art. 6, § 10, du projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 39.

déré comme un traitement ultérieur compatible nécessaire à l'exécution d'une mission d'intérêt public au sens des réglementations relatives à la protection des traitements de données à caractère personnel». L'APD a été très critique à l'égard de ce traitement ultérieur, d'autant plus que le projet de loi l'érigeait en traitement ultérieur compatible sans autre contrôle. Ainsi, l'APD a relevé que «l'avant-projet semble en outre vouloir opérer une extension d'office et en bloc des possibilités d'utilisation de données contenues dans toutes les banques de données en possession de toutes les autorités publiques belges, donc de toutes les données détenues et utilisées par toutes ces institutions dans le cadre de l'exécution de leurs missions (données fiscales, médicales, sociales, pénales, etc.). Et ce, en édictant arbitrairement que les finalités de surveillance et de contrôle sont considérées comme "compatibles" avec les finalités pour lesquelles ces données ont été collectées et utilisées initialement»[158]. Le Conseil d'État a abondé dans son sens en considérant que «l'avant-projet à l'examen ne démontre pas en quoi cette réutilisation serait nécessaire et proportionnée dans une société démocratique pour garantir un ou plusieurs des objectifs d'intérêt général énumérés à l'article 23, paragraphe 1, du RGPD. La proportionnalité pourrait d'ailleurs difficilement être démontrée, dans la mesure où les données à caractère personnel pouvant être réutilisées ne sont, à ce stade, pas encore clairement identifiées. L'article 6, § 3, alinéa 4, délègue en effet au Roi le soin de déterminer notamment les données à caractère personnel visées, les personnes concernées ainsi que la transmission de ces données à des tiers»[159].

En termes de proportionnalité ou de minimisation, le Conseil d'État n'a guère été plus tendre en jugeant que, «eu égard aux nombreuses délégations contenues dans l'article 6 et à la définition trop vague de certains éléments essentiels, il est impossible de se prononcer, à ce stade, quant à la proportionnalité des traitements envisagés par l'avant-projet à l'examen»[160]. Cela revient à dire à l'auteur du projet de loi qu'il doit revoir sa copie; copie qu'il a préféré effacer plutôt que de la retravailler afin de pouvoir la rendre compatible avec les règles applicables en matière de protection des données.

En effet et face à ces critiques, mais également à celles venant de divers milieux tant politiques que scientifiques[161] tout autant que la pression mise par le jugement rendu le 12 avril 2021 par le président du tribunal de première instance

158 APD, avis n° 24/2021 du 2 mars 2021, p. 7.

159 Art. 6, § 10, du projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 124.

160 Art. 6, § 10, du projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, préc., p. 124.

161 Voy., entre autres, C. Fallon et E. Paul, «Carte blanche: la loi "pandémie" ne permettra pas de sortir de la "sidération politique"», *Le Soir*, 3 mai 2021, https://www.lesoir.be/369802/article/2021-05-03/carte-blanche-la-loi-pandemie-ne-permettra-pas-de-sortir-de-la-sideration (dernière consultation le 16 janvier 2022).

francophone de Bruxelles siégeant en référé[162], le gouvernement a purement et simplement retiré l'article 6 du projet de loi. Cela implique que les règles relatives au traitement des données à caractère personnel devront être prévues pour chaque arrêté royal pris sur la base de la loi «pandémie». Si cette suppression a permis l'adoption de la loi, cela laisse beaucoup de zones d'ombre sur le sort réservé aux données à caractère personnel. Il s'agit d'une réelle occasion manquée et, encore et toujours, d'une absence de volonté de prendre à bras-le-corps cette question de protection des données à caractère personnel dans le contexte pandémique que nous connaissons.

Certains pourront également se poser la question sur l'avantage démocratique d'une telle loi par rapport au régime d'arrêtés de pouvoirs spéciaux qui a été utilisé depuis le mois de mars 2020 jusqu'en septembre 2021. Il nous semble que le fait que chaque arrêté royal pris sur la base de la loi «pandémie» doit passer par le Parlement donne à nouveau un certain contrôle parlementaire, même si nous pouvons nous poser la question de la réalité d'un débat démocratique lorsque les députés suivent les instructions des partis politiques lors des votes.

§ 2. Les bases de données et outils mis en place dans la gestion de crise et la protection des données en période de Covid: analyse des accords de coopération

Dans le cadre du présent paragraphe, nous allons nous attacher à deux accords de coopération impactant la vie privée en ce compris la protection des données, à savoir l'accord de coopération du 12 mars 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre le Covid-19 (ci-après, «accord vaccination») et l'accord de coopération du 14 juillet 2021 tel que modifié le 27 septembre 2021 et le 28 octobre 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement des données liées au certificat Covid numérique de l'UE et au Covid Safe Ticket, le PLF et le traitement des données à caractère personnel des travailleurs salariés et des travailleurs indépendants vivant ou résidant à l'étranger qui effectuent des activités en Belgique (ci-après, «accord CST»).

162 Le président du tribunal de première instance francophone de Bruxelles avait jugé que les arrêtés ministériels mettant en place des mesures de confinement étaient illégaux et avait prononcé des astreintes à l'encontre de l'État belge. On peut se demander si l'action des demandeurs ayant donné lieu à une telle décision a réellement servi la cause. En effet, la pression mise par ce jugement a, à notre avis, réduit le débat parlementaire par rapport à la loi «pandémie» à peau de chagrin alors qu'une telle loi méritait mieux que cela...

A. *L'accord vaccination*

Les entités fédérale et fédérées ont conclu, le 12 avril 2021, un accord de coopération concernant le traitement de données relatives aux vaccinations contre le Covid-19 qui, en réalité, reprend les éléments figurant dans l'arrêté royal du 24 décembre 2020 concernant l'enregistrement et le traitement de données relatives aux vaccinations. Cet arrêté royal avait donné lieu à un avis du 18 décembre 2020 de l'APD[163] auquel nous ferons référence ici.

1. Minimisation des traitements

Nous devons rappeler, tel que l'a fait l'APD, qu'en application de l'article 5, 1.b), du RGPD, « les données personnelles doivent être traitées pour des finalités déterminées, explicites et justifiées »[164]. En effet, ce principe de finalité qui est lié à celui de minimisation est essentiel pour la personne concernée dès lors qu'il lui permet de pouvoir exercer ses droits de contrôle sur le traitement et vérifier si le responsable du traitement traite les données conformément à ce qui est annoncé.

La professeure de Terwangne précise, à ce sujet, que « [t]out traitement de données doit poursuivre une ou des finalité(s) déterminée(s). Il s'agit de savoir, dès le démarrage d'un traitement de données, quel(s) objectif(s) ce traitement est appelé à servir. La finalité ne peut être inexistante ("on ne sait pas encore à quoi vont servir ces données, mais comme on a l'occasion de les collecter, collectons-les toujours") ni floue. La spécification de la finalité est fondamentale, car c'est elle qui va déterminer le traitement de données à caractère personnel (le traitement "gestion de clientèle", "gestion du contentieux", "contrôle sur le lieu de travail", "lutte contre la fraude", "relations publiques", "sécurité des biens et des personnes"…) et permettre à la personne concernée de contrôler le sort réservé aux données la concernant »[165].

Elle complète cela en précisant que « cette précision permettra également au responsable du traitement de déterminer les données qui devront être collectées et traitées. En effet, comme on le verra plus loin, les données traitées doivent être pertinentes au regard de la finalité. Une finalité qui ne serait pas suffisamment précise et serait donc énoncée de manière trop large permettrait de traiter un ensemble bien trop vaste de données, toutes pouvant passer pour pertinentes par rapport à la finalité annoncée. Le Groupe de l'article 29 a

163 APD, *advies nr 138/2020 van 18 december 2020.*

164 APD, *ibid.*, p. 11, n° 31 (traduction libre).

165 C. DE TERWANGNE, « Les principes relatifs au traitement des données à caractère personnel », *Le Règlement général sur la protection des données*, Collection du CRIDS, 2018, p. 92. Voy. aussi : Groupe de travail 29, « Opinion 03/2013 on purpose limitation », *WP 203*, 2 avril 2013, pp. 15-16. M.-H. BOULANGER *et al.*, « La protection des données à caractère personnel en droit communautaire », *J.D.E.*, 1997, p. 377 ; M. VAN OVERSTRAETEN et S. DEPRÉ, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, pp. 685-686.

signalé que, au risque de manquer de précision, la définition de la finalité des traitements ne peut se faire par la simple référence aux activités du responsable du traitement ou à ses missions légales[40]. La doctrine[41] a aussi pointé comme ne répondant pas au critère de spécificité les finalités trop vagues indiquées par Facebook, telles "Provide, Improve and Develop Services", "Promote Safety and Security" et "Show and Measure Ads and Services" »[166].

L'APD a considéré que certaines finalités sont si larges et imprécises qu'elles ne répondent pas à l'exigence d'être « spécifiques et explicites » comme cela est requis par l'article 5, 3, b), du RGPD, car elles ne permettent pas aux personnes concernées de comprendre ce qui va leur arriver et pourquoi.

Ainsi, l'article 4 de l'accord vaccination détermine les finalités pour lesquelles les données à caractère personnel sont traitées. Si le paragraphe 1er ne soulève pas d'observations particulières, il n'en va pas de même pour le second. En effet, les finalités qui y sont énoncées sont trop imprécises ainsi que l'Autorité de protection des données l'a également relevé[167] :

1. « *prestation de soins de santé et de traitements visée à l'article 9, 2, h, du RGPD* ». Pour rappel, cette base de licéité vise « le traitement [qui] 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 ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé […] ». Or la base de licéité adéquate est, en réalité, l'article 9, 2, i, du RGPD qui précise que le traitement de données relatives à la santé est autorisé si « 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, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel »[168]. La base de

166 C. DE TERWANGNE, « Les principes relatifs au traitement des données à caractère personnel », *Le Règlement général sur la protection des données*, Collection du CRIDS, 2018, p. 93.

167 APD, *ibid.*, p. 11, n° 33 (traduction libre).

168 Le considérant 54 précise que « [l]e traitement des catégories particulières de données à caractère personnel peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. Un tel traitement devrait faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques. Dans ce contexte, la notion de "santé publique" devrait s'interpréter selon la définition contenue dans le règlement (CE) n° 1338/2008 du Parlement européen et du Conseil (1), à savoir tous les éléments relatifs à la santé, à savoir l'état de santé, morbidité et handicap inclus, les déterminants ayant un effet sur cet état de santé, les besoins en matière de soins de santé, les ressources consacrées aux soins de santé, la fourniture de

licéité choisie n'est donc pas valable et, partant, il y a une irrégularité par rapport au RGPD ;

2. « *la pharmacovigilance des vaccins contre la COVID-19, conformément à l'article 12sexies de la loi du 25 mars 1964 sur les médicaments et aux lignes directrices détaillées publiées par la Commission européenne dans le "Module VI – Collecte, gestion et transmission des notifications d'effets indésirables présumés des médicaments (GVP)", telles qu'elles figurent dans la dernière version disponible, et visées à l'article 4, paragraphe 1, 3°, de la loi du 20 juillet 2006 relative à la création et au fonctionnement de l'Agence fédérale des médicaments et des produits de santé ainsi que la traçabilité des vaccins contre la COVID-19 afin d'assurer le suivi des "rapid alerts de vigilance" et "rapid alerts de qualité" visées à l'article 4, paragraphe 1, 3e alinéa, 3°, e, et 4°, j, de la loi du 20 juillet 2006 relative à la création et au fonctionnement de l'Agence fédérale des médicaments et des produits de santé* ». On comprend mal la nécessité d'un tel traitement de données qui est manifestement redondant par rapport à celui effectué par l'Agence fédérale des médicaments et des produits de santé tel que prévu à l'article 4, § 1er, alinéa 3, 3°, e, et 4°, j, de la loi du 20 juillet 2006 relative à la création et au fonctionnement de l'Agence. En effet, le Centre belge de pharmacovigilance pour les médicaments à usage humain (CBPH)[169] qui est une entité de l'Agence fédérale des médicaments et des produits de santé est chargé de la coordination des différentes tâches relatives à la pharmacovigilance et collecte ainsi des données de pharmacovigilance tant sur la base de rapports individuels que de compilations de données concernant les effets indésirables des médicaments. Il appert donc que l'Agence fédérale des médicaments et des produits de santé effectue la pharmacovigilance, de sorte que le traitement des données des personnes vaccinées (ou qui administrent le vaccin) dans le cadre de cette finalité constitue à nouveau une infraction au RGPD et, plus particulièrement, à son principe de minimisation dès lors que le traitement n'est pas nécessaire ;

3. « *l'organisation logistique de la vaccination contre la COVID-19, après anonymisation des données ou à tout le moins pseudonymisation des données dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser l'organisation logistique* ». Ainsi que l'a très justement relevé l'Autorité de protection des données, la lecture de cette finalité ne permet pas de comprendre si l'utilisation de données relatives aux vaccinés et vaccinateurs (et desquelles) est envisagée à des fins de commande des doses de vaccins à temps[170]. Il n'est donc

soins de santé, l'accès universel à ces soins, les dépenses de santé et leur financement, ainsi que les causes de mortalité. De tels traitements de données concernant la santé pour des motifs d'intérêt public ne devraient pas aboutir à ce que des données à caractère personnel soient traitées à d'autres fins par des tiers, tels que les employeurs ou les compagnies d'assurance et les banques ».

169 https://www.afmps.be/fr/humain/medicaments/medicaments/pharmacovigilance/cbph (dernière consultation le 10 janvier 2021).

170 APD, *ibid.*, p. 11, note infrapaginale 19 (traduction libre).

pas possible, pour la personne concernée, de comprendre la finalité prévue par l'accord vaccination ;

4. « *l'organisation du suivi des contacts en exécution de l'Accord de coopération du 25 août 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact 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* ». L'accord vaccination ne précise pas, et il est impossible de deviner de quelle manière, le suivi de la vaccination pourrait aider l'accomplissement des opérations de tracing prévues dans cet accord de coopération. Y a-t-il un croisement de base de données entre deux bases de données dans le cadre d'un traitement ultérieur qui ne paraît cependant pas compatible *prima facie* ? Il est certain que cette finalité est obscure pour la personne concernée qui ne peut évaluer sa pertinence. Elle ne répond donc pas au prescrit de l'article 5, 1.b), du RGPD en vertu duquel « les données personnelles doivent être traitées pour des finalités déterminées, explicites et justifiées » ;

5. « *l'exécution du suivi et de la surveillance post-autorisation conformément aux bonnes pratiques recommandées par l'Organisation mondiale de la Santé, après anonymisation des données ou à tout le moins pseudonymisation des données dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser le suivi et la surveillance post-autorisation* ». Cela signifie-t-il que les données seraient traitées afin d'organiser un contrôle et une surveillance après la délivrance de l'autorisation du vaccin ? Dans quelle mesure cette finalité diffère-t-elle de la finalité dite de « pharmacovigilance », puisqu'il est apparemment possible de contrôler et de surveiller les effets des vaccins sur la base de données anonymes ou au moins pseudonymisées[171] ;

6. « *l'exécution d'études scientifiques ou statistiques après anonymisation, ou à tout le moins pseudonymisation dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser l'étude scientifique ou statistique* ». Ainsi que l'Autorité de protection des données l'avait très justement relevé, l'indication de cette finalité n'est d'aucune pertinence, dès lors que l'utilisation de données à des fins de recherche scientifique est prévue et réglementée par l'article 89 du RGPD[172]. À noter que la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel prévoit également cette situation en son titre 4. En d'autres termes, une telle finalité n'est pas nécessaire en l'espèce et, de

171 APD, *ibid.*, p. 11, note infrapaginale 20 (traduction libre).

172 APD, *ibid.*, p. 11, note infrapaginale 21 (traduction libre).

plus, cela constitue une infraction au principe d'interdiction de retranscription du RGPD.

Au regard de ces divers éléments, l'on ne peut que constater que l'accord vaccination viole le principe de minimisation, mais également celui de prévisibilité de la norme. Cela ne peut évidemment pas être accepté d'autant plus lorsque ce sont des données appartenant à des catégories particulières qui sont traitées, à savoir des données relatives à la santé. Or l'on réserve à ces données une protection plus élevée qu'à celles visées à l'article 6 du RGPD à cause des risques accrus de porter préjudice aux individus sur la base du traitement de ces données. C'est principalement le risque de discriminations illégitimes ou arbitraires qui est lié à ces données qui justifie le traitement différencié qui leur est accordé[173]. De telles données présentent, en outre, un risque d'affecter la sphère la plus intime des sujets ainsi qu'un risque sérieux de dommage, en cas d'abus, pour la personne concernée. Cette protection accrue est mise en œuvre par l'article 9 du RGPD qui fixe un régime général d'interdiction de traitement assorti d'exceptions pour lesquelles le législateur européen a effectué une balance d'intérêts. On doit rappeler le principe général selon lequel toute exception doit être interprétée de manière restrictive et, à tout le moins, dans les intérêts de la personne protégée qui est, dans le cadre du RGPD, la personne concernée. Or le contenu de l'accord de vaccination laisse à penser que ses rédacteurs ont oublié ce principe, ce que nous pouvons réellement déplorer.

2. Minimisation des données

Le RGPD précise, en son considérant 39, que « les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées »[174]. Le principe de minimisation des données est ainsi posé et traduit dans l'article 5 du RGPD. À ce sujet, la professeure de Terwangne précise que « les données à caractère personnel faisant l'objet d'un traitement doivent, comme auparavant, être adéquates et pertinentes au regard des finalités du traitement. Pour être jugées pertinentes, les données doivent présenter un lien nécessaire et suffisant avec les finalités poursuivies »[175] et que « plutôt que de devoir être en outre "non excessives", comme dans les textes de la Convention 108 et de la directive, les données à caractère personnel doivent désormais être "limitées à ce qui est nécessaire" au regard des

173 Voy. J. Ringelheim, « Recueil des données personnelles et lutte contre les discriminations. Une tension nécessaire entre non-discrimination et vie privée », *in Les nouvelles lois luttant contre la discrimination*, Bruges, la Charte, 2008, pp. 91 et s.

174 Cons. 39 RGPD.

175 C. de Terwangne, « Les Principes relatifs au traitement des données à caractère personnel et à sa licéité », *Le Règlement général sur la protection des données (RGPD/GDPR), Analyse approfondie*, Collection du CRIDS, 2018, pp. 107-108. Voy. également M.-H. Boulanger *et al.*, « La protection des données à caractère personnel en droit communautaire », *J.T.-dr. eur.*, 1997, p. 146.

finalités pour lesquelles elles sont traitées[176]. Il est à noter que le critère de nécessité s'exprime tant au niveau de la quantité des données que de leur qualité. Ainsi, s'il est clair qu'on ne peut traiter un nombre excessif de données [...] on ne peut davantage se lancer dans le traitement d'une seule donnée qui, même pertinente au vu de la finalité, porterait excessivement atteinte aux droits et intérêts de la personne concernée par rapport à l'intérêt qu'elle présente pour la personne qui souhaite la traiter [...] »[177]. Elle conclut qu'« il faut comprendre que les deux formulations "limitées à ce qui est nécessaire" et "données non excessives" se rejoignent en ce qu'elles sont toutes deux l'expression du principe de proportionnalité »[178].

On constate que cette notion de proportionnalité oblige le législateur à procéder à une analyse complète de ses besoins en termes de données, mais également de la forme sous laquelle il les traitera. Ainsi, il devra, par exemple, vérifier si le traitement envisagé peut se satisfaire de données anonymes[179] qui permettraient au traitement de sortir du champ d'application du RGPD. Si le traitement ne permet pas d'atteindre la finalité déterminée, le responsable du traitement pourra alors traiter des données pseudonymisées[180]. Si, et seulement si, le traitement de telles données ne permet pas d'atteindre la finalité déterminée, le responsable du traitement pourra alors traiter des données à caractère personnel non pseudonymisées. Il s'agit d'une réelle cascade induite par le RGPD qui devra être appliquée pour chaque traitement déterminé par le responsable du traitement. Cela entre dans la méthode de travail visée par la notion de protection des données dès la conception[181].

Au niveau des données traitées lors de la vaccination, l'article 3, § 2, de l'accord vaccination précise :

176 La professeure de Terwangne note également que la directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, a, quant à elle, gardé la formulation initiale et son article 4, § 1er, c), établit que les données à caractère personnel doivent être « non excessives au regard des finalités pour lesquelles elles sont traitées ».

177 C. de Terwangne, « Les Principes relatifs au traitement des données à caractère personnel et à sa licéité », *op. cit.*, p. 108.

178 *Ibid.*, p. 108.

179 Par donnée anonyme, nous devons entendre une donnée dont le lien est définitivement coupé avec la personne physique à laquelle elle se rapportait. À noter que le caractère anonyme d'une donnée peut se révéler difficile à maintenir avec l'avènement du *Big Data* et de l'intelligence artificielle.

180 Le RGPD définit la pseudonymisation comme « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable » (art. 4, 5). Il n'en demeure pas moins que des données rendues pseudonymes restent des données à caractère personnel. Dans la législation belge antérieure au RGPD, nous avions la notion de donnée codée.

181 Les termes de *privacy by design* sont également largement utilisés.

> « Pour chaque vaccination visée à l'article 2, §2 les catégories de données suivantes sont enregistrées dans Vaccinnet :
> 1° des données d'identité de la personne à laquelle le vaccin a été administré, notamment le numéro d'identification visé à l'article 8 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, le nom, le prénom, le sexe, le lieu et la date de naissance, le lieu de résidence principale et, le cas échéant, la date de décès. Ces données sont collectées, pour autant qu'elles soient disponibles, auprès du registre national et des registres Banque-Carrefour visés à l'article 4 de la loi précitée du 15 janvier 1990, sur la base du numéro d'identification mentionné ;
> 2° des données d'identité de la personne qui a administré le vaccin, notamment le numéro d'identification visé à l'article 8 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale ou le numéro INAMI ;
> 3° des données relatives au vaccin, notamment la marque, le numéro de lot et le numéro d'identification du vaccin ;
> 4° des données relatives au moment et au lieu d'administration du vaccin ;
> 5° des données relatives au schéma de vaccinations contre la COVID-19 de la personne à laquelle est administré le vaccin ;
> 6° des données relatives aux effets indésirables de la vaccination, dont la personne qui a administré le vaccin ou son délégué a ou devrait avoir connaissance »[182].

Or il s'avère que certaines de ces données ne sont pas nécessaires à l'accomplissement des finalités prévues par l'accord vaccination ou que la nécessité de leur traitement n'est pas précise. Ainsi, par exemple :

1. le numéro de registre national : ce numéro est un identifiant personnel faisant l'objet d'une protection toute particulière, de sorte que son traitement est strictement réglementé par la loi du 8 août 1983 organisant un registre national des personnes physiques. Tout traitement de ce numéro doit être effectué pour une finalité précise. L'on suppose que ce numéro est utilisé pour permettre une identification univoque de la personne vaccinée. Il eût été pertinent de le préciser afin que la personne concernée puisse connaître les raisons du traitement d'une telle donnée ;
2. ainsi que cela a déjà été mentionné ci-dessus, les données relatives aux effets indésirables font déjà l'objet d'un traitement par l'Agence fédérale des médicaments et des produits de santé de sorte que leur traitement par d'autres entités – que l'accord vaccination ne détermine par ailleurs pas – ne s'avère donc pas nécessaire et constitue un doublon par rapport à la base de données gérée par l'Agence fédérale des médicaments et des produits de santé. Cette absence de nécessité est donc contraire au principe de minimisation mis en place par le RGPD.

182 Art. 3, § 2, de l'accord vaccination.

3. Transparence

La transparence est un des éléments essentiels du RGPD. L'on pourrait même considérer qu'il s'agit d'une pierre angulaire en matière de protection des données. Thomas Tombal a clairement expliqué ce principe en précisant qu'« avant de nous plonger dans l'étude de ce droit, pour la personne concernée, d'être informée du traitement dont elle fait l'objet, il convient de souligner une particularité organisationnelle dans la rédaction du RGPD. Ainsi, bien que les articles 12 à 14 soient contenus dans le chapitre du RGPD relatif aux droits de la personne concernée 15, ces articles sont formulés en termes d'obligations imposées au responsable de traitement. Certes, il s'agit là de deux revers d'une seule et même médaille, mais l'on peut se demander s'il n'e[û]t pas été plus cohérent de formuler ces dispositions en termes de droits accordés à la personne concernée »[183].

Au niveau du contenu de la loi, il y a lieu de relever l'arrêt *Rotaru c. Roumanie* de la Cour EDH dans lequel la Cour a rappelé que l'ingérence dans la vie privée d'individus ne peut avoir lieu que via une loi qui doit préciser le genre d'informations pouvant être consignées, les catégories de personnes susceptibles de faire l'objet des mesures de surveillance, mais également *les personnes autorisées à consulter les dossiers, la nature de ces derniers*, la procédure à suivre et l'usage qui peut être donné aux informations ainsi obtenues. De même, la loi doit fixer la durée de leur conservation[184].

Le RGPD confirme cela en imposant au législateur, en toutes circonstances, de préciser les catégories de destinataires des données et les circonstances dans lesquelles ils pourront les utiliser[185].

L'on constate, à la lecture de l'accord vaccination, qu'il est fait mention comme « destinataires » potentiels de toutes « instances ayant une mission d'intérêt général pour les finalités dont sont chargées ces instances par ou en vertu d'une loi, d'un décret ou d'une ordonnance »[186]. De plus, l'autorisation de transfert est accordée après délibération de la chambre « sécurité sociale et santé » du Comité de sécurité de l'information.

Pour paraphraser l'Autorité de protection des données dans son avis du 18 décembre 2020[187], cette disposition est si large qu'elle ne permet en aucune façon à la personne concernée d'avoir une vision claire du ou des traitements effectués sur ses données, par quel(s) tiers, à quelles fins et dans quelles circonstances ce traitement est autorisé. Ceci est d'autant plus vrai que le traitement

183 T. Tombal, « Les droits de la personne concernée dans le RGPD », *in Le Réglement* général sur la protection des données, Collection du CRIDS, 2018, p. 410.

184 CEDH, *Rotaru c. Roumanie*, req. n° 28341/95, 4 mai 2000, n° 57, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2228341/95%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-63075%22]} (dernière consultation le 10 janvier 2022).

185 Art. 13 et 14 RGPD.

186 Art. 5 de l'accord vaccination.

187 APD, *advies nr 138/2020 van 18 december 2020.*

par des tiers ne semble aucunement limité aux finalités qui entrent dans le champ d'application des finalités reprises à l'accord vaccination.

L'on constate en outre qu'il revient au Comité de sécurité de l'information de décider si la finalité annoncée par le tiers est acceptable ou pas. Il est à noter que l'accord vaccination charge ainsi ce Comité de sécurité de l'information de rendre un avis contraignant et ayant valeur normative, dans le cadre d'échange de données, se substituant donc au législateur ainsi qu'à l'Autorité de protection des données belge.

En effet :

1. il appartient au législateur de définir dans une norme de rang de loi les éléments essentiels d'un traitement de données à caractère personnel ; tout transfert de données liées à la vaccination à une instance publique doit être prévu et encadré dans une norme de rang de loi, de même que la finalité du traitement de ces données par cette instance et la durée pendant laquelle elle conservera ces données ;
2. la compétence de rendre un avis préalable sur cette norme de rang de loi revient, en vertu de l'article 23 de la loi belge du 3 décembre 2017, à l'Autorité de protection des données telle que visée par le chapitre VI du RGPD.

Pour être complet, il est utile de relever que le législateur belge a volontairement mis fin au système des comités sectoriels préexistants afin d'éviter une violation par la Belgique du RGPD en ce qu'il institue le principe de responsabilisation (« *accountability* »), impose la nomination d'un DPO et l'émission d'un avis par ledit DPO sur les transferts et utilisations de données entre institutions et, enfin, interdit la mise en place d'un système national d'autorisations préalables à moins que les États membres ne décident de conférer un tel pouvoir d'autorisation, dans certaines matières, à leur autorité de contrôle (uniquement). Or ce Comité de sécurité de l'information est en réalité un retour du Comité sectoriel de la sécurité sociale et de la santé, mais en dehors du giron de l'Autorité de protection des données. Ceci constitue une violation flagrante du RGPD et de la volonté d'harmonisation entre tous les régimes de protection des données au sein des États membres voulue par le législateur européen.

Il ressort, de courriels échangés avec la Commission européenne dans lesquels cette dernière émet des réserves quant à la légalité du CSI de loi par rapport au RGPD, que la Commission européenne souligne[188] :

> From your explanation we understand that your intention is that the body will itself issue decisions with normative value. Such body is not foreseen in the GDPR and we have strong reservations that such body would fit within the structural setting of the Regulation.

188 « D'après votre explication, nous comprenons que votre intention est que l'organe prenne lui-même des décisions ayant une valeur normative. Un tel organe n'est pas prévu dans le RGPD et nous avons de fortes réserves sur le fait qu'un tel organe s'inscrive dans le cadre structurel du Règlement » (traduction libre).

L'on constate donc que l'accord vaccination ne précise pas les catégories de destinataires des données au sens de l'article 8 de la CEDH et, partant, de l'article 22 de la Constitution ainsi que du RGPD, et soumet la détermination de ces destinataires au Comité de sécurité de l'information dont l'existence même et donc les décisions violent le RGPD.

Nous sommes donc très éloignés d'une conformité de l'accord vaccination aux règles applicables en matière de protection des données et, plus particulièrement, au RGPD.

B. Accord CST

Dans le cadre de cette section, nous allons nous attacher à analyser le « Covid Safe Ticket » (ci-après, « CST ») qui soulève de nombreuses critiques et a donné lieu à deux décisions de justice divergentes.

Plusieurs accords CST sont intervenus et le dernier en date est celui du 28 octobre 2021 suite à l'activation de la loi « pandémie » et modifiant l'accord de coopération du 14 juillet 2021 modifié lui-même par l'accord de coopération du 27 septembre 2021. Par ailleurs, le décret de la Région wallonne du 21 octobre 2021 relatif à l'usage du Covid Safe Ticket et à l'obligation du port du masque fixe les conditions d'usage du Covid Safe Ticket. Ainsi, l'usage du CST a été imposé pour pouvoir assister à des événements ou entrer dans certains lieux.

Il est indéniable que le CST impacte de manière significative des libertés fondamentales telles que le droit de circuler librement, la liberté de réunion, outre des droits garantis par la Constitution tels que celui du droit à l'épanouissement culturel et social prévu par l'article 23, alinéa 2, 5°, de la Constitution. Il reflète également une certaine fourberie de la part des autorités qui n'ont pas eu le courage politique de rendre la vaccination obligatoire, préférant restreindre progressivement les libertés des non-vaccinés. Une telle situation ne pouvait qu'appeler des recours de la part de citoyens soucieux du respect de leurs libertés fondamentales, mais également pour éviter que des mesures exceptionnelles prises pour faire face à la pandémie ne deviennent définitives.

La cour d'appel de Liège a, dans un appel d'une ordonnance prononcée par le tribunal de première instance de Namur, division Namur, siégeant en référé du 3 novembre 2021, constaté que :

> « Sur le plan formel, il ne fait aucun doute que le décret du 21 octobre 2021 est contraire, notamment, à la Convention européenne des droits de l'homme, et plus particulièrement aux dispositions suivantes :
> - article 8 (droit au respect de la vie privée et familiale) ;
> - article 11 (liberté d'association) ;
> - article 14 (interdiction de discrimination).

En outre, le décret du 21 octobre 2021 est contraire à la Charte des droits fondamentaux de l'Union européenne et plus spécifiquement à :

- l'article 3 (Droit à l'intégrité de la personne) ;
- l'article 7 (Respect de la vie privée) ;
- l'article 8 (Protection des données à caractère personnel) ;
- l'article 12 (Liberté de réunion et d'association) ;
- l'article 13 (Liberté des arts) ;
- l'article 16 (Liberté d'entreprise) ;
- l'article 21 (Non-discrimination) ;
- l'article 24 (Droits de l'enfant) ;
- l'article 25 (Droits des personnes âgées).

Prima facie, cette violation est indiscutable dès lors que le Covid Safe Ticket est une entrave à un exercice normal et habituel de ces libertés et droits »[189].

Partant de ce constat de base, la Cour a procédé, de manière logique et conformément à la jurisprudence de la Cour EDH, à une analyse de proportionnalité. Elle rappelle ainsi que, « pour qu'une restriction puisse être apportée aux droits et libertés fondamentaux, l' (les) objectif(s) général(aux) qui sous-tend(ent) la restriction doit(vent) être défini(s) de manière précise par le législateur. Il faut que la norme prise, qui restreint ces droits et libertés, soit apte à atteindre l' (les) objectif(s) poursuivi(s) et que cette norme soit proportionnelle. Il faut donc que la norme soit nécessaire au regard du but poursuivi. il importe donc de vérifier si la norme permet d'atteindre l' (les) objectif(s) poursuivi(s) et de s'assurer qu'elle constitue la voie la moins attentatoire aux droits fondamentaux »[190].

À la suite d'un long examen de la question de proportionnalité, la Cour a admis « que le Covid Safe Ticket est un délicat précédent contraire, d'une part, aux libertés telles que consacrées par les normes internationales ou notre Constitution et, d'autre part, à une philosophie de non contrôle social. Il comporte en outre un risque d'entrave au secret médical et au respect de la vie privée. Reste que la Cour estime que *prima facie* la distinction opérée par le Covid Safe Ticket est objective, nécessaire et proportionnée vis-àvis des objectifs poursuivis par la Région wallonne et ce, au moment où la Cour statue, soit à un moment où le niveau d'épidémie pour l'ensemble du pays est fixé à son plus haut niveau »[191].

Au niveau de la discrimination qui a été un des arguments développés par les demandeurs originaires, la Cour a même considéré que

> « traiter de la même manière les [personnes vaccinées] et les [personnes non vaccinées] au bénéfice de l'égalité serait en réalité discriminatoire pour les premiers. En effet, le Covid Safe Ticket, constatant la vaccination ou la guérison ou encore le résultat d'un test, peut constituer un moyen proportionné et nécessaire pour permettre à la fois de maintenir les droits et les libertés des personnes vaccinées représentant la majeure partie de la population tout en assurant un risque modéré de propagation du virus, d'engorgement des hôpitaux et, par voie de conséquence, un risque modéré de fermeture de secteurs particuliers.
> Il importe de souligner que cette différence ne se fait pas sur un état de santé des personnes concernées, mais bien sur un risque de contagiosité.
> Surtout, la différence entre les personnes vaccinées et celles non vaccinées est atténuée par le fait qu'ont également accès au Covid Safe Ticket les personnes guéries ou encore les personnes ayant réalisé un test dans les 24 ou 48 heures.
> Cette différence telle qu'atténuée est donc proportionnée vis-à-vis des buts poursuivis. »[192]

Nous constatons donc que la cour d'appel de Liège a procédé à cette fameuse analyse de proportionnalité pour juger que les atteintes aux libertés individuelles constatées étaient proportionnées.

Il convient cependant de relever que cet arrêt a été rendu en référé, ce qui implique que, « s'agissant d'une action en référé, [l'examen de proportionnalité est] réalisé *prima facie*. La Cour insiste sur ce point. La charge de la preuve que la norme prise n'est pas disproportionnée repose sur la Région wallonne. Reste que la mesure de cette preuve est d'une ampleur qui doit être apparente dès lors que l'on se situe dans le cadre d'une action en référé. Tout[e] autre serait la preuve à apporter s'il s'agissait d'une action au fond »[193]. Nous pourrions donc avoir une décision différente suite à une analyse au fond de ce type d'action.

Il est également utile de relever que la cour d'appel de Liège a considéré que la Région wallonne a commis une faute en ne demandant pas l'avis de l'APD sur l'accord CST du 28 octobre 2021 modifiant celui du 14 juillet 2021 tel que modifié le 27 septembre 2021. C'est une décision importante dès lors que la Cour rappelle ainsi que l'APD doit être consultée pour toute modification d'un texte entrant dans le champ d'application de l'article 36, 4., du RGPD. Il est utile que le gouvernement fédéral s'en souvienne, lui qui a une fâcheuse tendance à contourner cette obligation[194].

L'accord CST n'a cependant pas été sauvé par cet arrêt et restait en sursis, car la proportionnalité a été analysée *in concreto* en prenant en compte les éléments pertinents au jour de l'arrêt.

Ainsi, le Tribunal de première instance de Namur, division de Namur, saisi à nouveau d'une action par les mêmes parties a considéré, dans un jugement du 1er mars 2022, que la « Région wallonne n'apparaît plus en mesure, à l'heure actuelle, dans le cadre de l'examen des droits apparents, d'établir la nécessité et

189 Liège (12e ch. A), 7 janvier 2022, R.G. n° 2021/RF/24, pp. 33-34, inédit.
190 Liège (12e ch. A), 7 janvier 2022, préc., pp. 36-37.
191 Liège (12e ch. A), 7 janvier 2022, préc., p. 40.
192 Liège (12e ch. A), 7 janvier 2022, préc., p. 39.
193 Liège (12e ch. A), 7 janvier 2022, préc., p. 37.
194 Voy. E. Degrave, « L'activation de la loi pandémie sans passer par l'APD "est illégale" », *Le Soir*, 29 octobre 2021, https://www.lesoir.be/403552/article/2021-10-29/lactivation-de-la-loi-pandemie-sans-passer-par-lapd-est-illegale (dernière consultation le 17 janvier 2022).

la proportionnalité du maintien du régime du C.S.T dans des lieux spécifiques en regard de l'un de ses objectifs assignés, alors qu'il est de nature à restreindre les droits et libertés fondamentaux des parties demanderesses».

Le Tribunal est arrivé à cette conclusion après une analyse de la situation vaccinale au regard de la propagation du virus Covid-19. Il a ainsi considéré que :

> «Il résulte de ces éléments, non formellement contredits, à tout le moins en ce qui concerne le constat d'un effet très limité, voire inexistant, selon certains scientifiques, de la vaccination contre la propagation du variant Omicron (Omicron et Omicron BA.2), représentant 99,70 % des variants identifiés dans les échantillons dernièrement analysés (bulletin épidémiologique hebdomadaire du 18 février 2022, pièce 16, sous farde 3, du dossier de la RÉGION WALLONNE), que la distinction induite par le régime du C.S.T. entre les personnes vaccinées et celles qui ne le sont pas n'apparaît plus, prima facie, raisonnablement justifiée en regard de l'un des principaux objectifs assignés par la RÉGION WALLONNE, à savoir la réduction de la propagation, dans certains lieux, du virus SarsCov2 dans sa forme variante actuellement majoritaire.
> La RÉGION WALLONNE n'apparaît ainsi plus en mesure, à l'heure actuelle, dans le cadre de l'examen des droits apparents, d'établir la nécessité et la proportionnalité du maintien du régime du C.S.T. dans des lieux spécifiques en regard de l'un de ses objectifs assignés, alors qu'il est de nature à restreindre les droits et libertés fondamentaux des parties demanderesses.
> Par ailleurs, l'évolution de la situation épidémique, selon les dernières données produites aux débats (bulletin hebdomadaire du 18 février 2022), laisse apparaître une réduction des cas confirmés d'infection, ainsi que de l'occupation des lits d'hôpitaux, dont ceux des soins intensifs, soit une tendance à la baisse de la pression sur le système hospitalier. Il s'en suit qu'un autre objectif poursuivi par les autorités n'apparaît plus menacé, à tout le moins si cette tendance se confirme dans le temps.»[195]

Le Tribunal a donc travaillé au niveau de la proportionnalité en se plaçant au jour de la décision, ce qui nous semble parfaitement conforme au droit. Dans le décours de son analyse, il a procédé à une analyse de l'utilité du CST face à la propagation du virus pour arriver à la conclusion que la mesure imposant le CST et restreignant ainsi l'accès à certains lieux qu'aux personnes ayant un CST valide (vaccinées ou ayant un certificat de rétablissement ou encore un test PCR négatif de moins de 48 heures ou 72 heures) n'était plus proportionnée au regard des rapports scientifiques ou épidémiologiques.

Nous nous permettons d'attirer le regard sur le fait que cette décision ne constitue pas une victoire ainsi que cela a été présenté, à tort, dans la presse à travers certains interviews ni une reconnaissance d'une faute dans le chef de la Région wallonne. En effet, le tribunal a précisé avec bon sens que «si, *prima facie*, la RÉGION WALLONNE ne s'est *manifestement pas écartée du comportement de toute autorité publique normalement prudente et diligente* en ayant étendu le

[195] Civ. Namur, div. Namur, 1er mars 2022, p. 24, inédit ; nous soulignons.

régime du C.S.T. sur la base des données scientifiques et épidémiologiques dont *elle disposait à l'époque*, si, dans ce cadre, elle a légitimement pu faire *primer l'intérêt général et l'impératif de la protection du droit à la vie et à la santé des personnes* exposées au péril grave de la pandémie, il convient d'observer qu'à ce jour, l'évolution de cette même pandémie et de l'état de la science ne permettent plus de considérer la nécessité impérieuse de maintenir tel quel un régime attentatoire aux libertés et droits fondamentaux en regard des objectifs poursuivis»[196]. Cela rappelle que la situation évolue vite et que le même test de proportionnalité pouvait donner une réponse différente au moment de la prise du décret critiqué ou le peut encore dans le futur si la situation vient à nouveau de s'aggraver. Le terme victoire est donc bien loin d'être adéquat dans la situation pandémique que nous avons connue. Dommage que certains aient encore une pensée dichotomique en cette matière et parlent encore de victoire et de défaite.

Conclusion

Ainsi que cela a été évoqué tant au niveau international qu'au niveau national, la pandémie que nous connaissons depuis mars 2020 a nécessité, dans un premier temps, une réaction urgente. Dans ce contexte inédit et tendu, la Belgique a tracé sa voie entre la gestion de l'urgence sanitaire, la promotion des outils numériques qui y participent, la protection des droits et libertés fondamentaux, l'harmonisation des solutions de sécurité sanitaire proposée par l'Union européenne.

Force est de constater que les divers gouvernements ont maintenu cette situation d'urgence pour adopter des textes qui manquent de rigueur en termes de protection des libertés fondamentales et, plus particulièrement, de la protection des données à caractère personnel. Ils n'ont jamais basculé vers une gestion du risque avec ce que cela entraînait en termes de mouvement du balancier vers un rééquilibrage des libertés en jeu. Ainsi, la pandémie, dans le domaine de la protection des données comme dans beaucoup d'autres de notre équilibre social, a été un exhausteur de fragilités, fragilités humaines au premier rang, fragilité de la souveraineté des États également, fragilités institutionnelles, mais surtout fragilité des libertés fondamentales.

Si, en notre qualité de juristes, nous devons être conscients que certaines libertés doivent céder un peu plus de place à d'autres droits tels que celui de santé publique, cela ne peut s'effectuer que dans le respect des garde-fous mis en place, entre autres, par la Convention européenne des droits de l'Homme, la Charte des droits fondamentaux de l'Union et le RGPD. Un de ceux-ci est le principe de proportionnalité tel que nous l'avons repris dans la présente contribution.

[196] Civ. Namur, div. Namur, 1er mars.2022, p. 24, inédit ; nous soulignons.

Cette proportionnalité doit s'analyser *in concreto* et peut évoluer selon les circonstances. Ainsi, une même mesure pourra être considérée comme une atteinte proportionnée à une liberté fondamentale dès lors qu'elle s'inscrit dans une situation d'urgence, mais sera analysée comme disproportionnée dans une situation de gestion du risque. En d'autres termes, les mesures en vigueur actuellement et qui sont considérées comme des atteintes proportionnées devront être déclarées illégales si elles perdurent dans le temps, perdant ainsi leur caractère proportionné.

Les autorités doivent tenir compte de cette évolution et les juristes que nous sommes ainsi que les citoyens doivent être vigilants pour éviter que des mesures temporaires ne deviennent définitives avec une érosion inacceptable de nos libertés. Nous devons cependant résister à intervenir dans des débats, publics ou non, avec des slogans ou des idées de victoire ou de défaite. Les droits à la vie privée et à la santé ne peuvent se satisfaire de tels slogans ou termes guerriers que nous devons laisser à la pensée populiste qui n'a pas sa place dans des situations de pandémie impactant la santé publique et les individus dans son ensemble.

Il nous semble que, dans la recherche de l'équilibre entre sécurité et liberté, la contrepartie est chèrement payée en terme de violation des droits fondamentaux et particulièrement en matière de protection de la vie privée et de la protection des données personnel. La question de la nécessité et de la proportionnalité des mesures prises est aiguë et nous interroge encore.

Chacun est un « chien de garde » des libertés fondamentales et doit, en cas d'abus des autorités publiques, réagir de manière adéquate et réfléchie afin de ne pas discréditer la juste cause.