Cour constitutionnelle

Arrêt n° 84/2023
du 1er juin 2023
Numéro du rôle : 7648

En cause : le recours en annulation de la loi du 2 avril 2021, du décret de la Communauté flamande du 2 avril 2021, du décret de la Communauté française du 25 mars 2021, du décret de la Communauté germanophone du 29 mars 2021, de l'ordonnance de la Commission communautaire commune du 2 avril 2021, du décret de la Région wallonne du 1er avril 2021 et du décret de la Commission communautaire française du 1er avril 2021 « portant assentiment à l'accord de coopération du 12 mars 2021 entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 », introduit par Charlotte D'Hondt.

La Cour constitutionnelle,

composée des présidents P. Nihoul et L. Lavrysen, et des juges T. Giet, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne, D. Pieters, S. de Bethune, E. Bribosia, W. Verrijdt et K. Jadin, assistée du greffier F. Meersschaut, présidée par le président P. Nihoul,

après en avoir délibéré, rend l'arrêt suivant :

I. *Objet du recours et procédure*

Par requête adressée à la Cour par lettre recommandée à la poste le 7 octobre 2021 et parvenue au greffe le 8 octobre 2021, Charlotte D'Hondt, assistée et représentée par Me P. Joassart, avocat au barreau de Bruxelles, a introduit un recours en annulation de la loi du 2 avril 2021, du décret de la Communauté flamande du 2 avril 2021, du décret de la Communauté française du 25 mars 2021, du décret de la Communauté germanophone du 29 mars 2021, de l'ordonnance de la Commission communautaire commune du 2 avril 2021, du décret de la Région wallonne du 1er avril 2021 et du décret de la Commission communautaire française du 1er avril 2021 « portant assentiment à l'accord de coopération du 12 mars 2021 entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et

la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 » (publiés respectivement au *Moniteur belge* du 12 avril 2021, deuxième édition, du 9 avril 2021, du 6 avril 2021, du 12 avril 2021, deuxième édition, du 9 avril 2021, du 12 avril 2021, deuxième édition, et du 7 avril 2021).

Des mémoires et mémoires en réplique ont été introduits par :

- le Conseil des ministres, assisté et représenté par Me P. Slegers, Me S. Ben Messaoud et Me J. Duval, avocats au barreau de Bruxelles;

- le Gouvernement flamand, le Gouvernement wallon, le Collège de la Commission communautaire française, le Collège réuni de la Commission communautaire commune, le Gouvernement de la Communauté française et le Gouvernement de la Communauté germanophone, assistés et représentés par Me M. Feys, avocat au barreau de Gand.

La partie requérante a introduit un mémoire en réponse.

Par ordonnance du 15 mars 2023, la Cour, après avoir entendu les juges-rapporteurs T. Giet et S. de Bethune, a décidé que l'affaire était en état, qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de cette ordonnance, à être entendue, et qu'en l'absence d'une telle demande, les débats seraient clos le 29 mars 2023 et l'affaire mise en délibéré.

Aucune demande d'audience n'ayant été introduite, l'affaire a été mise en délibéré le 29 mars 2023.

Les dispositions de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle relatives à la procédure et à l'emploi des langues ont été appliquées.

II. *En droit*

– A –

A.1. Le recours en annulation est dirigé contre les différentes normes portant assentiment à l'accord de coopération du 12 mars 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 (ci-après : l'accord de coopération du 12 mars 2021), en ce que ces dispositions concernent l'enregistrement des vaccinations contre la COVID-19 dans la base de données « Vaccinnet ». Les dispositions de cet accord de coopération sont en grande partie identiques à celles qui sont contenues dans l'arrêté royal du 24 décembre 2020 « concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 » (ci-après : l'arrêté royal du 24 décembre 2020), contre lequel la partie requérante a également introduit un recours en annulation devant le Conseil d'État.

Quant à la recevabilité

A.2. La partie requérante justifie son intérêt à agir par le fait qu'elle est une personne physique résidant en Belgique et qu'elle est susceptible de se faire vacciner contre la COVID-19, de sorte que les dispositions attaquées peuvent l'affecter directement et défavorablement. En effet, si elle décide de se faire vacciner, son nom et ses différentes données à caractère personnel figureront dans « Vaccinnet », en méconnaissance de son droit au respect de la vie privée, lu en combinaison avec le principe de la non-rétroactivité des lois. Si elle décide de ne pas se faire vacciner, il existe un risque sérieux que des restrictions (par exemple, l'interdiction de prendre un avion) l'affectent en raison de sa non-vaccination.

A.3. Le Conseil des ministres, le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune contestent l'intérêt à agir de la partie requérante, qui ne démontre pas qu'elle serait directement et défavorablement affectée par les normes attaquées, de sorte que son recours s'apparente à une action populaire.

Ainsi, la partie requérante ne démontre pas qu'elle serait vaccinée, ni qu'elle compte se faire vacciner et que les normes attaquées l'en empêchent. La qualité de « victime potentielle » ne suffit pas à justifier d'un intérêt. Le préjudice lié à la présomption de futures restrictions liées à l'absence de vaccination est purement hypothétique – le seul exemple concret de l'interdiction potentielle de prendre l'avion n'est pas sérieux – et découlerait d'une autre norme que celles qui sont présentement attaquées. Enfin, le fait de justifier son intérêt à agir par la violation de ses droits fondamentaux revient à confondre intérêt et fondement du moyen.

A.4. Le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune estiment également que le recours en annulation, introduit le 7 octobre 2021, est manifestement irrecevable *ratione temporis* en ce qu'il est dirigé contre le décret d'assentiment de la Communauté française, publié au *Moniteur belge* le 6 avril 2021.

L'irrecevabilité manifeste du recours en ce qu'il est dirigé contre ce décret d'assentiment entraîne par ailleurs la perte d'intérêt au recours dans son ensemble. En effet, à supposer que la Cour fasse droit au recours en ce qu'il est dirigé contre les autres normes attaquées, ce décret subsisterait dans l'ordre juridique de sorte que, d'une part, il pourrait toujours être applicable à la partie requérante et, d'autre part, l'accord de coopération ne pourrait être dénoncé par l'ensemble de ses auteurs agissant conjointement.

A.5.1. Concernant l'irrecevabilité *ratione temporis*, la partie requérante répond qu'un accord de coopération ne produit d'effets qu'après avoir reçu l'assentiment de toutes les entités concernées, de sorte qu'on ne peut pas calculer le délai de recours à compter de la première publication d'une norme d'assentiment, puisqu'à ce moment l'accord de coopération est encore dépourvu d'effets et que cela risquerait de réduire significativement les délais de recours contre les autres normes d'assentiment publiées ultérieurement. La partie requérante invite dès lors la Cour à considérer – de manière analogue aux règles qui prévalent en matière d'affichage urbanistique – que le point de départ du délai de recours en annulation est la publication au *Moniteur belge* de la dernière norme d'assentiment à l'accord de coopération.

À supposer que le recours soit irrecevable *ratione temporis* à l'égard du seul décret d'assentiment de la Communauté française – qui pourrait, seul, subsister dans l'ordre juridique –, il resterait recevable à l'égard des autres normes d'assentiment.

A.5.2. La partie requérante répond que son intérêt n'est pas potentiel puisque la campagne de vaccination massive s'adresse à toute personne qui répond aux conditions d'âge et de santé et qu'il existe un risque sérieux que des restrictions s'attachent à une absence de vaccination, et que le Covid Safe Ticket se transforme en un « pass vaccinal » comme en France. En toute hypothèse, l'absence de vaccination crée, pour de nombreuses activités de la vie quotidienne, des contraintes supplémentaires liées à l'obligation de présenter le Covid Safe Ticket, analogue à une obligation officieuse, mais réelle, de vaccination.

À supposer que le recours soit irrecevable *ratione temporis* à l'égard du seul décret d'assentiment de la Communauté française, cette irrecevabilité ne peut aucunement entraîner la perte d'intérêt pour l'ensemble du recours présentement examiné. Ainsi, si ce décret subsistait dans l'ordre juridique, seules les dispositions de l'accord de coopération, relevant des compétences de la Communauté française, lesquelles se limitent à la vaccination des personnes âgées de moins de dix-huit ans, seraient encore dotées d'effet. Or, la partie requérante est adulte et n'a pas d'enfant à charge, de sorte qu'elle n'est pas concernée par cette compétence de la Communauté française.

Enfin, une dénonciation unilatérale d'un accord de coopération peut avoir lieu dans certaines hypothèses, telles que l'état de nécessité ou le cas de force majeure. Si la Cour annulait les normes d'assentiment autres que le décret de la Communauté française, cette annulation pourrait alors fonder une dénonciation unilatérale de la part de la Communauté française.

A.6.1. Le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune répliquent que, conformément à l'article 3, § 1er, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le délai de recours en annulation court à partir de la publication de chaque norme d'assentiment à l'accord de coopération, et non à partir de la date d'entrée en vigueur de l'accord de coopération. Par ailleurs, le parallélisme entre l'affichage d'un permis d'urbanisme et la publication d'une norme législative au *Moniteur belge* n'est pas sérieux.

Le Conseil des ministres réplique qu'en vertu de l'autonomie de l'autorité fédérale et des entités fédérées, chaque norme d'assentiment à un accord de coopération constitue une norme autonome dont la validité ne dépend pas de l'existence d'une autre norme d'assentiment. Il est dès lors possible d'attaquer une seule norme d'assentiment, sans contester par un recours unique l'ensemble des textes portant assentiment à un accord de coopération. En outre, la partie requérante admet elle-même que le maintien dans l'ordre juridique du décret d'assentiment de la Communauté française ne changerait pas sa situation personnelle.

A.6.2. Concernant l'intérêt à agir, la partie requérante admet elle-même que son préjudice est hypothétique puisqu'elle se réfère à la possibilité, nullement confirmée, d'un passage à un « pass vaccinal ». Par ailleurs, les contraintes liées à l'usage du Covid Safe Ticket ne découlent pas davantage des normes attaquées en l'espèce. Enfin, l'intérêt à obtenir l'annulation de normes d'assentiment à un accord de coopération s'apprécie au jour de l'introduction du recours, de sorte que les circonstances postérieures que la partie requérante ajoute dans son mémoire ne peuvent être prises en considération.

Le Conseil des ministres réplique que la partie requérante se limite à des considérations générales pour justifier son intérêt à agir, sans démontrer en quoi elle subit, personnellement, un préjudice direct découlant des normes attaquées.

Quant au fond

A.7.1. Le moyen unique est pris de la violation de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, avec les articles 5, 6, 9 et 35 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) » (ci-après : le RGPD), ainsi qu'avec le principe de la non-rétroactivité des lois.

L'accord de coopération du 12 mars 2021 prévoit différents traitements de données à caractère personnel sensibles – puisqu'elles concernent la santé – qui constituent des ingérences dans le droit au respect de la vie privée : l'enregistrement dans « Vaccinnet » des vaccinations administrées (article 2, § 2), les catégories de données qui sont traitées dans « Vaccinnet » (article 3, § 2), les finalités de traitement (article 4, § 2), la communication des données à des tiers, moyennant délibération préalable de la chambre « sécurité sociale et santé » du Comité de sécurité de l'information (article 5) et le délai de conservation des données dans « Vaccinnet » (article 6, § 2). Selon la partie requérante, ces ingérences dans le droit au respect de la vie privée

sont contraires au principe de la légalité inscrit à l'article 22 de la Constitution (première branche), disproportionnées à l'objectif poursuivi (deuxième branche) et contraires au principe de la non-rétroactivité des lois (troisième branche).

A.7.2. Tout d'abord, l'accord de coopération du 12 mars 2021 ne fixe pas de manière suffisamment précise certains éléments essentiels du traitement de données à caractère personnel qu'il autorise.

Ainsi, l'article 4, § 2, définit pas moins de onze finalités pour l'enregistrement des vaccinations dans « Vaccinnet », l'Autorité de protection des données ayant souligné le caractère large et peu précis de certaines finalités, qui ne sont dès lors pas suffisamment « déterminées et explicites » pour permettre aux intéressés de comprendre ce qu'il adviendra de leurs données, lesquelles peuvent, en outre, être communiquées à des tiers.

Ensuite, les catégories de destinataires des données à caractère personnel fixées ont fait l'objet de réserves de la part de l'Autorité de protection des données, en l'absence de garanties suffisantes de prévisibilité. En outre, l'article 5, alinéa 3, de l'accord de coopération du 12 mars 2021 délègue au Comité de sécurité de l'information la compétence de déterminer, seul, quelles instances tierces sont habilitées à utiliser ou à réutiliser les données collectées et pour quelles finalités : même s'il s'agit d'une autorité indépendante, elle ne peut en principe se voir déléguer des éléments essentiels de matières réservées à la loi.

A.7.3. Ensuite, même si elle poursuit un objectif légitime de santé publique et de protection des droits et libertés d'autrui, l'ingérence dans le respect de la vie privée est disproportionnée.

Ainsi, tant la section de législation du Conseil d'État que l'Autorité de protection des données ont souligné le caractère excessif du délai de 30 ans pour la conservation des données à dater de la date de vaccination contre la COVID-19. La section de législation du Conseil d'État a aussi critiqué le fait que la disposition contienne un délai minimum de conservation, et non un délai maximum.

Ensuite, l'analyse d'impact relative à la protection des données découlant de l'accord de coopération du 12 mars 2021, exigée par l'article 35 du RGPD, n'a pas été réalisée, de sorte qu'en l'absence de cette analyse d'impact, les dispositions visées dans le moyen ont été violées par les dispositions attaquées.

A.7.4. Enfin, les normes attaquées sont contraires au principe de la non-rétroactivité des lois qui exige que le contenu du droit soit prévisible et accessible, de sorte que le justiciable puisse prévoir, à un degré raisonnable, les conséquences d'un acte déterminé au moment où cet acte est accompli.

Ainsi, l'article 12 de l'accord de coopération du 12 mars 2021 prévoit que les dispositions de cet accord rétroagissent au jour de l'entrée en vigueur de l'arrêté royal du 24 décembre 2020. La section de législation du Conseil d'État a toutefois souligné que, si l'urgence de prévoir un cadre pour lutter contre la pandémie de COVID-19 pouvait justifier cette rétroactivité, elle ne valait cependant pas pour les nouveaux éléments qui ne correspondent pas au traitement des données à caractère personnel tel qu'il s'est concrétisé dans les faits depuis le 24 décembre 2020. La partie requérante souligne, à cet égard, que la onzième finalité reprise dans l'article 4, § 2, de l'accord de coopération ne figurait pas dans l'arrêté royal du 24 décembre 2020.

A.8.1. Le Conseil des ministres rappelle que l'accord de coopération du 12 mars 2021 prévoit l'existence de deux bases de données : d'une part, la base de données contenant les codes de vaccination qui est gérée conjointement par les entités fédérées responsables de l'organisation de la vaccination et par Sciensano et, d'autre part, « Vaccinnet » – seule concernée par les griefs de la partie requérante – qui est le système d'enregistrement visé à l'article 9 de l'arrêté du Gouvernement flamand du 16 mai 2014 « portant diverses dispositions en exécution du décret du 21 novembre 2003 relatif à la politique de santé préventive et modifiant des arrêtés d'exécution de ce décret ».

Le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune rappellent que la vaccination constitue un instrument dont l'importance a été soulignée par l'Organisation mondiale de la santé en vue de lutter contre la propagation du

coronavirus SARS-CoV-2. L'enregistrement des vaccinations dans « Vaccinnet » est nécessaire pour mener, de manière coordonnée entre les entités fédérées et l'État fédéral, une politique optimale de gestion de crise, permettre la pharmacovigilance, suivre le taux de vaccination dans la population et estimer les répercussions sur l'assurance maladie, dans le respect du droit à la vie privée.

A.8.2. Concernant la première branche du moyen, le principe de la légalité est respecté en l'espèce concernant les finalités du traitement. Le fait de détailler de manière circonstanciée, dans l'article 4, § 2, de l'accord de coopération du 12 mars 2021, onze finalités vise en effet à offrir aux personnes concernées la transparence et la prévisibilité, l'accord de coopération étant lié à une grande quantité d'autres instruments législatifs pour lesquels le traitement des données à caractère personnel relatives à la vaccination contre la COVID-19 est nécessaire. Ces finalités sont définies limitativement, en lien avec la lutte contre la COVID-19, et avec suffisamment de précision, en renvoyant chaque fois à la législation associée. La médecine et les soins de santé préventifs, ainsi que la gestion des services de santé, constituent d'ailleurs des finalités reconnues par le RGPD. La collecte de données personnelles est indispensable pour permettre aux autorités d'administrer les vaccins contre la COVID-19 et est pleinement liée au droit reconnu par la loi du 22 août 2002 « sur les droits du patient », dont l'article 9 prévoit le droit du patient à ce que son « dossier de patient » soit tenu à jour et conservé. La finalité relative à l'information et à la sensibilisation des personnes concernant la vaccination contre la COVID-19 est une finalité en lien avec le rôle des prestataires de soins et des organismes assureurs. La critique de l'Autorité de protection des données à l'égard de la finalité d'appréciation de la capacité de travail a par ailleurs perdu son objet puisque la version finale de l'accord de coopération du 12 mars 2021 a été adaptée afin de suivre l'avis de l'Autorité de protection des données.

Les finalités liées au certificat COVID numérique de l'UE ou au Covid Safe Ticket ne pouvaient pas être prévues lors de l'élaboration de l'accord de coopération du 12 mars 2021, mais elles l'ont été ultérieurement dans l'article 11, § 4, de l'accord de coopération du 14 juillet 2021, qui organise le traitement de données liées au certificat COVID numérique de l'UE, au COVID Safe Ticket et au *passenger locator form* (formulaire de localisation des passagers), et qui déroge à l'article 4, § 2, de l'accord de coopération du 12 mars 2021, offrant ainsi une base légale suffisante à cette finalité du traitement des données à caractère personnel. Le principe de la minimisation des données a par ailleurs été respecté, puisque des données peuvent être anonymisées ou pseudonymisées lorsque cela est possible, ce qui ne l'est évidemment pas pour la finalité d'information et de sensibilisation à la vaccination.

Il ressort par ailleurs du commentaire de l'accord de coopération que les tiers auxquelles les données peuvent être communiquées ont été déterminés avec précision et qu'une telle communication ne peut avoir lieu que pour atteindre les finalités prévues dans l'accord de coopération.

Le rôle du Comité de sécurité de l'information est défini très précisément dans l'article 5, alinéa 3, de l'accord de coopération du 12 mars 2021 et il constitue un filtre supplémentaire en vue de garantir le respect des règles en matière de protection des données. Contrairement à ce qu'avance la partie requérante, ce Comité n'est nullement compétent pour déterminer seul les instances pouvant utiliser, ou réutiliser, les données collectées et leurs finalités. Par ailleurs, le législateur peut confier une mission technique et complexe à une autorité administrative indépendante, dans le respect des articles 33, 105 et 108 de la Constitution, dont la violation n'est même pas alléguée dans le recours présentement examiné. Enfin, ce Comité est soumis à un contrôle tant juridictionnel que parlementaire, de même qu'au contrôle de l'Autorité de protection des données.

A.8.3. Concernant la deuxième branche du moyen, contrairement à ce qu'allègue la partie requérante, l'article 6, § 2, de l'accord de coopération du 12 mars 2021 prévoit un délai maximum pour la conservation des données de vaccination visées à l'article 3, § 2, de l'accord, à savoir jusqu'au décès de la personne vaccinée, et un délai minimum, à savoir 30 ans après la vaccination. La conservation de ces données jusqu'au décès de la personne est largement justifiée dans l'exposé des motifs de l'accord de coopération au regard du contexte et des finalités de surveillance et de suivi des vaccins à long terme, dans un processus de « mise en confiance » et dans le respect du principe de précaution, mais aussi en cas d'enquête sociale et de responsabilité, en vue d'évaluer les effets à long terme de ces nouveaux vaccins, ou encore afin de lutter contre d'éventuelles nouvelles pandémies. Le délai minimal de 30 ans poursuit ces mêmes buts, conformément au droit médical, afin d'éviter que les données soient perdues si la personne vient à décéder moins de 30 ans après l'administration du vaccin.

Contrairement à ce qu'allègue la partie requérante, une analyse d'impact sur la protection des données a été établie avec les autres parties à l'accord de coopération, conformément aux articles 35 et 36 du RGPD, cette analyse ne devant pas nécessairement précéder l'élaboration de la disposition légale autorisant le traitement. Au regard de son contenu, cette analyse est communiquée à la Cour à titre confidentiel.

La proportionnalité d'une ingérence dans la vie privée doit par ailleurs être évaluée de manière globale, en tenant compte des garanties concernant l'accès aux données de vaccination, qui requiert une délibération du Comité de sécurité de l'information (article 5), du fait que les finalités sont clairement définies (article 4, § 2) et du fait que les intéressés disposent d'un point de contact unique pour exercer leurs droits (article 7).

A.8.4. Concernant la troisième branche du moyen, le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune estiment que la partie requérante ne justifie pas d'un intérêt à la critique prise de l'atteinte au principe de la non-rétroactivité des lois, dont le respect ne peut être contrôlé directement par la Cour.

En l'espèce, la rétroactivité n'influence aucune procédure juridictionnelle, mais poursuit uniquement un objectif d'intérêt général, qui est de mener une gestion de crise optimale, permettre la pharmacovigilance, suivre le taux de vaccination de la population et estimer les répercussions sur l'assurance maladie. La section de législation du Conseil d'État a d'ailleurs accepté qu'un effet rétroactif soit conféré aux dispositions de l'accord de coopération du 12 mars 2021, compte tenu de la nécessité de lutte contre la pandémie de COVID-19. La partie requérante admet d'ailleurs elle-même que les dispositions de l'accord de coopération et celles de l'arrêté royal du 24 décembre 2020 sont largement identiques. En outre, l'article 12 de l'accord de coopération du 12 mars 2021 ne prévoit une entrée en vigueur rétroactive que pour les dispositions qui correspondent à cet arrêté, les autres dispositions entrant en vigueur le 11 février 2021, à savoir la date de publication du protocole d'accord du 27 janvier 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française « concernant le traitement de données relatives aux vaccinations contre la COVID-19 ».

La circonstance qu'une finalité aussi limitée que celle qui est visée à l'article 4, § 2, 11°, de l'accord de coopération ait été ajoutée ne saurait constituer, au regard des objectifs poursuivis en l'espèce, une violation injustifiée du principe de la non-rétroactivité des lois. Enfin, la partie requérante n'établit pas en quoi la rétroactivité aurait pour but de couvrir les « inconstitutionnalités » de l'arrêté royal du 24 décembre 2020, qui n'ont nullement été constatées par une juridiction compétente.

Le Conseil des ministres souligne que toutes les dispositions de l'accord de coopération du 12 mars 2021 relatives à « Vaccinnet » correspondent au traitement des données tel qu'il s'est concrétisé dans les faits. Il en va ainsi, notamment, de la collecte des données sur la base du numéro d'identification – qui correspond au numéro national pour les personnes concernées –, du lieu d'administration du vaccin ou des données relatives aux effets indésirables, des finalités existantes, de la conservation des données ou des personnes responsables du traitement – ces notions étant précisées, mais pas modifiées par rapport à la pratique. Les normes prévues par l'accord de coopération étaient dès lors totalement prévisibles puisqu'elles étaient déjà en vigueur et appliquées conformément à l'arrêté royal du 24 décembre 2020.

A.9. À titre subsidiaire, le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune estiment qu'à supposer que la Cour conclue à une inconstitutionnalité, seules devraient être annulées les normes d'assentiment en ce qu'elles portent sur les articles 4, § 2, 5, 6, § 2, et 12 de l'accord de coopération du 12 mars 2021; pour le surplus, les normes attaquées devraient être maintenues en ce qu'elles portent sur les autres dispositions de l'accord de coopération.

A.10. À titre infiniment subsidiaire, le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune invitent la Cour à maintenir les effets des normes annulées.

Ainsi, un maintien des effets est nécessaire pour permettre d'assurer la continuité et la sécurité juridique de la politique de lutte contre la COVID-19 menée par les autorités, le système « Vaccinnet » servant de support à plusieurs normes et accords de coopération, notamment en lien avec le certificat COVID numérique de l'UE ou le COVID Safe Ticket. Les effets des normes attaquées doivent dès lors être maintenus, pour le passé comme pour le futur, aussi longtemps que la pandémie perdure, mais aussi ultérieurement, pour garantir le suivi et le traitement des personnes concernées.

A.11.1. Concernant la première branche du moyen, la partie requérante répond, en ce qui concerne les finalités, qu'elle ne voit pas le lien entre la médecine préventive et le droit du patient à disposer d'un dossier de patient à jour et conservé. Le dossier de patient intervient dans un contexte visant à lui permettre de recevoir les meilleurs soins selon ses antécédents, alors que « Vaccinnet » n'est pas un outil centré sur le patient, mais sur une politique de santé publique visant à endiguer une pandémie, en enregistrant des données de manière préventive. L'accord de coopération du 12 mars 2021 n'a pas remédié aux critiques émises par l'Autorité de protection des données et la bonne organisation de la vaccination ne justifie pas que la finalité liée à l'information et à la sensibilisation nécessite un enregistrement des données à caractère personnel. Par ailleurs, le très grand nombre de finalités rend encore plus floue l'identification des destinataires des données.

En outre, le rôle du Comité de sécurité de l'information a été critiqué par la section de législation du Conseil d'État, sans que toutes ses remarques aient été prises en considération. Rien ne permet de considérer qu'il constitue un « filtre supplémentaire » et le pouvoir qui lui est conféré d'autoriser un échange de données revient à lui accorder un « droit de véto ».

A.11.2. Concernant la deuxième branche du moyen, la partie requérante répond que tant la section de législation du Conseil d'État que l'Autorité de protection des données ont souligné le caractère excessif du délai de conservation, qui n'a pas changé, de sorte qu'il n'existe pas de garanties à ce sujet.

La partie requérante conteste par ailleurs le caractère confidentiel de l'analyse d'impact, sollicité par les entités fédérées, car il irait à l'encontre de l'esprit du RGPD. Cette analyse d'impact doit dès lors être rendue publique, afin de permettre au citoyen d'évaluer la norme qui lui sera appliquée.

A.11.3. Concernant la troisième branche du moyen, la partie requérante répond que, d'une part, l'accord de coopération du 12 mars 2021 vise à couvrir plusieurs inconstitutionnalités de l'arrêté royal du 24 décembre 2020, qui ont été admises par le ministre de la Santé et que, d'autre part, à supposer que les dispositions de l'accord de coopération soient en grande partie identiques à celles de l'arrêté royal, elles ne correspondent pas parfaitement au traitement de données à caractère personnel concrétisé sur la base de cet arrêté royal.

A.12.1. Concernant la première branche du moyen, le Conseil des ministres, le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune répliquent que le fait d'avoir prévu onze finalités démontre qu'une réflexion approfondie a été menée sur les données qui ne peuvent pas être traitées en étant anonymisées ou pseudonymisées.

La finalité liée à la médecine préventive correspond à celle qui est visée à l'article 9, paragraphe 2, point h), du RGPD. L'administration d'un vaccin est un traitement médical qui fait partie de la médecine préventive, et l'« état vaccinal » doit être mentionné dans le dossier médical du patient, car il peut avoir de conséquences sur la stratégie à suivre par les prestataires de soins. « Vaccinnet » est donc orienté vers les droits du patient, puisqu'elle permet d'assurer le suivi post-vaccinal du patient.

La finalité liée à l'information et à la sensibilisation des personnes concernant la vaccination contre la COVID-19 s'inscrit dans l'objectif de créer une immunité collective. Le traitement des données de vaccination

peut être nécessaire pour des groupes à risque, par exemple pour la population âgée résidant dans les maisons de retraite. Le fait qu'il y ait, dans cette finalité, la combinaison d'une dimension individuelle et d'une dimension collective n'a pas pour conséquence qu'elle manque de précision.

Les personnes auxquelles les données traitées peuvent être transmises sont limitativement énumérées dans l'article 5 de l'accord de coopération du 12 mars 2021, de sorte qu'on ne peut prétendre, comme le fait la partie requérante, que ces tiers seraient définis de manière large. Le Comité de sécurité de l'information joue effectivement un rôle de filtre supplémentaire, en garantissant ainsi un contrôle externe.

A.12.2. Concernant la deuxième branche du moyen, il est répliqué que la confidentialité de l'analyse d'impact se justifie pour des raisons de sécurité liées au système de traitement des données mis en place et, notamment, en raison de la description technique des mesures de protection envisagées afin d'appréhender les risques. L'analyse d'impact a été communiquée à la Cour afin que celle-ci puisse vérifier qu'elle a été effectivement réalisée. Le Conseil des ministres souligne aussi que la partie requérante se contente de contester la confidentialité de l'analyse d'impact, sans indiquer la règle en vertu de laquelle une publicité aurait dû être assurée, le RGPD se limitant à exiger que l'analyse d'impact ait lieu, ce qui a été fait.

Pour le surplus, l'analyse du contenu et du caractère adéquat de l'analyse d'impact relève de la compétence exclusive de l'Autorité de protection des données - et non de la Cour constitutionnelle -, qu'il appartient dès lors à la partie requérante de saisir par le biais d'une plainte ou d'une notification.

A.12.3. Concernant la troisième branche du moyen, le Conseil des ministres réplique que la partie requérante n'a pas répondu aux critiques prises de l'irrecevabilité de cette branche du moyen.

– B –

Quant aux actes attaqués et à leur contexte

B.1. La partie requérante demande l'annulation de la loi du 2 avril 2021, du décret de la Communauté flamande du 2 avril 2021, du décret de la Communauté française du 25 mars 2021, du décret de la Communauté germanophone du 29 mars 2021, de l'ordonnance de la Commission communautaire commune du 2 avril 2021, du décret de la Région wallonne du 1er avril 2021 et du décret de la Commission communautaire française du 1er avril 2021 « portant assentiment à l'accord de coopération du 12 mars 2021 entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 » (ci-après : l'accord de coopération du 12 mars 2021).

L'accord de coopération du 12 mars 2021 a été publié, dans les trois langues nationales, en annexe de la loi du 2 avril 2021, au *Moniteur belge* du 12 avril 2021.

B.2.1. Le 11 mars 2020, l'Organisation mondiale de la santé a qualifié de pandémie l'explosion du nombre de contaminations au coronavirus SARS-CoV-2. Depuis mars 2020, la Belgique aussi est confrontée à cette pandémie et à ses conséquences. Le coronavirus SARS-CoV-2 est un virus très contagieux, qui cause la COVID-19, maladie qui peut entraîner de sérieux problèmes médicaux, voire la mort, principalement chez les personnes âgées et chez les personnes ayant des comorbidités (*Doc. parl.*, Parlement flamand, 2019-2020, n° 415/1, p. 2; *Doc. parl.*, Parlement flamand, 2020-2021, n° 488/1, p. 2; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2019-2020, n° B-41/1, p. 1).

Dans le cadre de cette crise sanitaire et pour lutter contre la propagation de la COVID-19, le Conseil national de sécurité, d'abord, puis le Comité de concertation, qui regroupe des représentants de l'autorité fédérale et des entités fédérées, ont été chargés de prendre des mesures concertées afin de freiner cette propagation (*Doc. parl.*, Parlement flamand, 2019-2020, n° 415/1, p. 2; *Doc. parl.*, Parlement flamand, 2020-2021, n° 488/1, p. 2).

B.2.2. Les actes attaqués s'inscrivent dans le cadre visant à compléter et à actualiser l'arsenal des mesures que les différentes autorités ont prises pour lutter contre la pandémie de COVID-19 et contre la propagation du coronavirus SARS-CoV-2, ainsi qu'éviter une résurgence de la pandémie liée à la COVID-19. Les actes attaqués s'inscrivent plus précisément dans le cadre des mesures nécessaires pour l'organisation de la vaccination contre la COVID-19.

Comme dans d'autres pays participant à la procédure européenne d'achat des vaccins contre la COVID-19, dans laquelle la Commission européenne négocie avec les entreprises au nom des États membres, après autorisation de mise sur le marché et en fonction des capacités de production, l'autorité fédérale et les entités fédérées ont décidé de coopérer afin d'organiser une campagne de vaccination massive, volontaire et gratuite contre la COVID-19.

Cette décision s'est notamment fondée sur des études démontrant l'efficacité clinique de la vaccination à grande échelle contre le coronavirus très contagieux SARS-CoV-2 qui cause la maladie de la COVID-19, pour lutter contre la propagation des contaminations de cette maladie

et éviter une surcharge des hôpitaux en raison des hospitalisations qui en découlent, ainsi que pour éviter une résurgence de la pandémie de COVID-19. L'Organisation mondiale de la santé conseille également au public de se faire vacciner contre la COVID-19.

La Conférence Interministérielle Santé publique du 16 novembre 2020 a défini les grands principes qui sous-tendent la stratégie belge de vaccination contre la COVID-19 :

- Objectif de couverture vaccinale de 70 % de la population;

- Détermination des groupes prioritaires sur la base d'avis scientifiques;

- Vaccination gratuite sur base volontaire pour chaque citoyen;

- Cofinancement de l'ensemble du programme de vaccination par l'autorité fédérale et les entités fédérées.

Ces décisions dépendent des éléments suivants :

- Des campagnes de vaccination de masse, les vaccins étant fournis dans des flacons multidoses qui doivent être administrés le même jour;

- La mise à la disposition de la Belgique d'un ou de plusieurs vaccins efficaces et sûrs contre la COVID-19.

- La capacité du système de santé belge à distribuer et à vacciner progressivement et efficacement la population, les autorités de santé étant soutenues par la Task force interfédérale « vaccin COVID-19 » créée par la Conférence Interministérielle Santé publique le 16 novembre 2020, l'ensemble des structures de santé du pays dont Sciensano et l'Agence fédérale des médicaments et des produits de santé (AFMPS). Le logiciel d'enregistrement Vaccinnet+ sera utilisé par toutes les entités fédérées à cette fin;

- La volonté de surmonter, par la persuasion et la transparence, l'hésitation vaccinale et d'obtenir ainsi l'adhésion de la population à cette stratégie de santé publique.

La stratégie de vaccination contre la COVID-19 s'est déployée en plusieurs phases, dès le mois de janvier 2021, avec une hiérarchisation des groupes cibles, les groupes prioritaires étant les résidents de maisons de repos et une partie des membres du personnel des maisons de repos, le personnel hospitalier et le personnel de soins et d'aide œuvrant en première ligne. Dès février 2021, les groupes prioritaires ont été étendus aux personnes à risques présentant des comorbidités, aux personnes âgées de 65 ans et plus et aux personnes âgées de 18 à 55 ans dans les forces de police, avant d'être progressivement élargis, sur la base du critère de l'âge et de la vulnérabilité, à toute la population de plus de 18 ans, puis de plus de 16 ans, plus de 12 ans et, enfin, à partir de 5 ans.

Sur la base des connaissances scientifiques actualisées, un schéma vaccinal d'une ou de deux doses de vaccin, en fonction du vaccin administré, a été établi par la Task force interfédérale « vaccin COVID-19 », et la possibilité de bénéficier d'une dose « booster » a également été offerte à la population.

B.2.3.1. Cette campagne de vaccination massive est également étroitement liée aux nouvelles mesures prises en juillet 2020 afin de lutter contre les risques de propagation liés aux assouplissements des restrictions des contacts physiques et à la possibilité de voyager à nouveau, compte tenu de la nouvelle phase de la crise de la COVID-19.

B.2.3.2. Le règlement (UE) 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 » (ci-après : le règlement (UE) 2021/953) prévoit, aux termes de son article 1er, paragraphe 1, un cadre pour la délivrance, la vérification et l'acceptation du certificat COVID numérique de l'UE, à savoir un certificat interopérable contenant des informations sur la vaccination, les résultats des tests ou le rétablissement de son titulaire, délivré dans le contexte de la pandémie

de COVID-19, et ce afin de faciliter l'exercice, par les titulaires de tels certificats, du droit à la libre circulation pendant la pandémie de COVID-19.

Le certificat COVID numérique de l'UE permet la délivrance, la vérification et l'acceptation transfrontières, notamment, d'un certificat de vaccination confirmant que le titulaire a reçu un vaccin contre la COVID-19 dans l'État membre qui délivre le certificat.

Les considérants 8 et 29 du règlement (UE) 2021/953 indiquent :

« 8. De nombreux États membres ont lancé ou prévoient de lancer des initiatives visant à délivrer des certificats de vaccination COVID-19. Toutefois, pour que ces certificats de vaccination puissent être utilisés de manière efficace dans un contexte transfrontière lorsque les citoyens de l'Union exercent leur droit à la libre circulation, ils doivent être pleinement interopérables, compatibles, sûrs et vérifiables. Une approche commune entre les États membres est nécessaire pour ce qui est du contenu, du format, des principes, des normes techniques et du niveau de sécurité de ces certificats de vaccination.

[…]

29. Dans l'optique de faciliter la libre circulation et pour garantir que les restrictions à la libre circulation actuellement en place pendant la pandémie de COVID-19 peuvent être levées de manière coordonnée sur la base des preuves scientifiques les plus récentes et des orientations mises à disposition par le comité de sécurité sanitaire institué par l'article 17 de la décision n° 1082/2013/UE du Parlement européen et du Conseil, l'ECDC et l'Agence européenne des médicaments (EMA), il convient de mettre en place un certificat de vaccination interopérable. Un tel certificat de vaccination devrait servir à confirmer que son titulaire a été vacciné contre la COVID-19 dans un État membre et devrait contribuer à la levée progressive des restrictions à la libre circulation. Le certificat de vaccination ne devrait contenir que les informations nécessaires pour identifier clairement le titulaire ainsi que le vaccin contre la COVID-19 qui a été administré, le nombre de doses ainsi que la date et le lieu de vaccination. Les États membres devraient délivrer des certificats de vaccination aux personnes ayant reçu des vaccins contre la COVID-19 pour lesquels une autorisation de mise sur le marché a été délivrée en vertu du règlement (CE) nº 726/2004 du Parlement européen et du Conseil, aux personnes ayant reçu des vaccins contre la COVID-19 pour lesquels une autorisation de mise sur le marché a été délivrée par l'autorité compétente d'un État membre en vertu de la directive 2001/83/CE du Parlement et du Conseil, et aux personnes ayant reçu des vaccins contre la COVID-19 dont la distribution a été temporairement autorisée en vertu de l'article 5, paragraphe 2, de ladite directive ».

Intitulé « Certificat de vaccination », l'article 5 du règlement (UE) 2021/953 dispose :

« 1. Chaque État membre délivre, automatiquement ou à la demande des personnes concernées, les certificats de vaccination visés à l'article 3, paragraphe 1, point a), aux

personnes à qui un vaccin contre la COVID-19 a été administré. Ces personnes sont informées de leur droit à un certificat de vaccination.

2. Le certificat de vaccination contient les catégories suivantes de données à caractère personnel :

a) l'identité du titulaire;

b) des informations sur le vaccin contre la COVID-19 administré et sur le nombre de doses administrées au titulaire;

c) les métadonnées du certificat, telles que l'émetteur du certificat ou un identifiant unique du certificat.

Les données à caractère personnel sont incluses dans le certificat de vaccination conformément aux champs de données spécifiques indiqués au point 1 de l'annexe.

La Commission est habilitée à adopter des actes délégués conformément à l'article 12 pour modifier le point 1 de l'annexe en modifiant ou en supprimant des champs de données, ou en ajoutant des champs de données relevant des catégories de données à caractère personnel visées aux points b) et c) du premier alinéa du présent paragraphe, lorsqu'une telle modification est nécessaire pour vérifier et confirmer l'authenticité, la validité et l'intégrité du certificat de vaccination, en cas de progrès scientifiques accomplis dans la maîtrise de la pandémie de COVID-19, ou pour assurer l'interopérabilité avec les normes internationales.

3. Le certificat de vaccination est délivré dans un format sécurisé et interopérable conformément à l'article 3, paragraphe 2, après l'administration de chaque dose et indique clairement si le schéma de vaccination est achevé ou non.

4. Lorsque, en cas d'émergence de nouvelles preuves scientifiques ou pour assurer l'interopérabilité avec les normes internationales et les systèmes technologiques, des raisons d'urgence impérieuses l'imposent, la procédure prévue à l'article 13 est applicable aux actes délégués adoptés en vertu du présent article.

5. Si les États membres acceptent une preuve de vaccination afin de lever les restrictions à la libre circulation mises en place, conformément au droit de l'Union, pour limiter la propagation du SARS-CoV-2, ils acceptent également, dans les mêmes conditions, les certificats de vaccination délivrés par d'autres États membres conformément au présent règlement pour un vaccin contre la COVID-19 pour lequel une autorisation de mise sur le marché a été délivrée en vertu du règlement (CE) nº 726/2004.

Les États membres peuvent également accepter, aux mêmes fins, des certificats de vaccination délivrés par d'autres États membres conformément au présent règlement pour un vaccin contre la COVID-19 pour lequel une autorisation de mise sur le marché a été délivrée par l'autorité compétente d'un État membre en vertu de la directive 2001/83/CE, un vaccin contre la COVID-19 dont la distribution a été autorisée temporairement en vertu de l'article 5, paragraphe 2, de ladite directive, ou un vaccin contre la COVID-19 pour lequel la procédure d'inscription sur la liste d'utilisation d'urgence de l'OMS est terminée.

Si les États membres acceptent des certificats de vaccination pour un vaccin contre la COVID-19 visé au deuxième alinéa, ils acceptent également, dans les mêmes conditions, les certificats de vaccination délivrés par d'autres États membres conformément au présent règlement pour le même vaccin contre la COVID-19 ».

L'annexe intitulée « Ensemble des données des certificats » prévoit en son point 1 :

« Champs de données à inclure dans le certificat de vaccination :

a) nom : nom(s) de famille et prénom(s), dans cet ordre;

b) date de naissance;

c) maladie ou agent ciblé : COVID-19 (SARS-CoV-2 ou l'un de ses variants);

d) vaccin ou prophylaxie contre la COVID-19;

e) dénomination du vaccin contre la COVID-19;

f) titulaire de l'autorisation de mise sur le marché ou fabricant du vaccin contre la COVID-19;

g) nombre dans une série de doses ainsi que le nombre total de doses dans la série;

h) date de la vaccination, indiquant la date de la dernière dose reçue;

i) État membre ou pays tiers dans lequel le vaccin a été administré;

j) émetteur du certificat;

k) identifiant unique du certificat ».

B.2.3.3. L'exposé général de l'accord de coopération du 11 juin 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 l'opérationnalisation du Règlement (UE) du Parlement Européen et du Conseil relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats interopérables de vaccination, de test et de rétablissement afin de faciliter la libre circulation pendant la pandémie de COVID-19 (Certificat Numérique COVID de l'UE) indique :

« L'accord de coopération du 12 mars 2021 entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le

traitement de données relatives aux vaccinations contre la COVID-19 […] régit le système d'information commun qui est mis en place pour l'invitation à la vaccination des personnes, pour l'organisation de la vaccination et pour l'enregistrement de la vaccination. Les entités fédérées et l'autorité fédérale considèrent la mise en place d'un système d'information commun comme une condition fondamentale. En vue de soutenir l'invitation des personnes à se faire vacciner et l'organisation de la vaccination, un système d'information commun était nécessaire afin d'éviter que les personnes ne soient invitées de manière non coordonnée ou que des personnes déjà vaccinées soient à nouveau invitées. Par ailleurs, le système doit permettre d'identifier le schéma posologique adéquat, notamment en ce qui concerne les différentes doses d'un vaccin à administrer (intervalle optimal proposé en cas de vaccins multidoses) et doit veiller à ce que l'organisation de la vaccination se déroule de manière optimale en fonction de la disponibilité du matériel et du personnel (médical) nécessaires. L'enregistrement des vaccinations dans un système d'information commun (Vaccinnet) par les vaccinateurs flamands, wallons, bruxellois et germanophones était notamment nécessaire. Compte tenu du fait qu'il s'agit d'une nécessité et qu'elle concerne le traitement de données à caractère personnel, une telle obligation d'enregistrement requiert une base juridique solide. La base de données est créée et gérée en collaboration très étroite entre les entités fédérées et l'Etat fédéral. Il est donc également approprié d'utiliser le même système opérationnel pour la délivrance des certificats » (*Moniteur belge* du 14 juin 2021, deuxième édition, p. 61955).

B.2.3.4. Les accords de coopération du 14 juillet 2021 et du 27 septembre 2021 entre l'Etat 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 , ainsi que l'accord de coopération du 28 octobre 2021 modifiant celui du 14 juillet 2021 définissent une base juridique pour l'utilisation nationale du certificat COVID numérique de l'UE et la génération du COVID Safe Ticket (ci-après : le CST) basée sur le certificat COVID numérique de l'UE. La vaccination d'une personne contre la COVID-19 permet de générer automatiquement le CST.

L'exposé général de l'accord de coopération du 14 juillet 2021, précité, indique à cet égard que, selon les connaissances scientifiques disponibles au moment de l'adoption de l'accord, les personnes qui ont été vaccinées présentent un risque moindre de contaminer d'autres personnes avec le coronavirus SARS-CoV-2 (*Moniteur belge* du 23 juillet 2021, p. 76172; voy. aussi le considérant 7 du règlement (UE) 2021/953).

L'article 11 de l'accord de coopération du 14 juillet 2021 dispose :

« § 1er. Aux fins de la vérification et pour la création et la délivrance du certificat COVID numérique de l'UE aux titulaires d'un certificat de vaccination, certificat de test ou certificat de rétablissement, les catégories de données à caractère personnel suivantes sont traitées conformément au règlement relatif au certificat COVID numérique de l'UE :

1° les catégories de données à caractère personnel visées à l'article 9, §§ 1, 2 ou 3;

2° 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; et

3° la résidence principale, visées à l'article 3, premier alinéa, 5°, de la loi du 8 août 1983 organisant un registre national des personnes physique;

§ 2. Les catégories de données à caractère personnel mentionnées au § 1 sont obtenues à partir des banques de données suivantes :

[…]

2° Vaccinnet : en ce qui concerne 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 et les catégories de données à caractère personnel dans le certificat de vaccination, décrites à l'article 9, § 1;

[…]

§ 4. Par dérogation à l'article 3, § 1, de l'accord de coopération du 25 août 2020 et à l'article 4, § 2, de l'accord de coopération du 12 mars 2021, les données à caractère personnel visées au § 1, peuvent être traitées pour les finalités de traitement visées à l'article 10 par les responsables du traitement, pour l'exercice de leurs missions légales définies dans le présent accord de coopération, les entités fédérées et Sciensano ».

B.3.1. Par l'accord de coopération du 12 mars 2021, l'autorité fédérale et les entités fédérées ont mis en place « le système d'information commun […] pour l'invitation à la vaccination des personnes, pour l'organisation de la vaccination et pour l'enregistrement de la vaccination » (*Moniteur belge* du 12 avril 2021, deuxième édition, p. 32397) :

« L'enregistrement des vaccinations dans un système d'information commun (Vaccinnet) par les vaccinateurs flamands, wallons, bruxellois et germanophones est notamment nécessaire pour mener une gestion de crise optimale, permettre la pharmacovigilance, comme visée à l'article 4, 2°, du présent accord, suivre le taux de vaccination de la population et estimer l'impact sur l'assurance maladie.

Compte tenu du fait qu'il s'agit d'une nécessité et qu'elle concerne le traitement de données à caractère personnel, une telle obligation d'enregistrement requiert une base juridique solide.

La base de données est créée et gérée en collaboration très étroite entre les entités fédérées et l'Etat fédéral » (*ibid.*, pp. 32397-32398).

B.3.2. Dans ce contexte, l'accord de coopération du 12 mars 2021 organise deux bases de données différentes.

D'une part, une première base de données contenant les codes de vaccination est créée « afin d'assurer, la campagne de vaccination massive dans le contexte de la pandémie de COVID-19 en permettant l'invitation des personnes à se faire vacciner, l'identification du schéma posologique adéquat et de la bonne organisation de la vaccination en fonction de la disponibilité des vaccins et du matériel ainsi que du personnel (médical et infirmier) nécessaires à cet effet » (*ibid.*, p. 32398).

Cette banque de données génère un code de vaccination aléatoire pour l'ensemble de la population *a priori* vaccinable, et recueille les données relatives à ces personnes afin de coordonner le schéma de vaccination contre la COVID-19 et éviter de générer un nouveau code de vaccination pour une personne qui a déjà été vaccinée (article 2, § 1er). Les données enregistrées dans cette banque de données sont identifiées par l'article 3, § 1er, de l'accord de coopération du 12 mars 2021. Elles sont conservées jusqu'à cinq jours à compter du lendemain de la publication de l'arrêté royal annonçant la fin de l'épidémie due au coronavirus SARS-CoV-2 (article 6, § 1er).

D'autre part, une seconde base de données, « Vaccinnet », concerne l'enregistrement pour l'ensemble du pays, par la personne qui a administré le vaccin contre la COVID-19 ou son mandataire, des données de vaccination, en tant que telles, des personnes qui se sont fait vacciner (article 2, § 2). Les données de vaccination sont définies par l'article 3, § 2, de l'accord de coopération du 12 mars 2021 comme étant les données d'identité de la personne à laquelle le vaccin a été administré (1°), les données d'identité et de contact éventuelles de la personne qui a administré le vaccin (2°), les données relatives au vaccin (3°), la date et le lieu d'administration de chaque dose du vaccin (4°), les données relatives au schéma de vaccinations contre la COVID-19 de la personne à laquelle est administré le vaccin (5°) et, le cas échéant, les données relatives aux effets indésirables observés pendant ou après la

vaccination sur la personne concernée, dont la personne qui a administré le vaccin ou son mandataire a connaissance (6°). Ces données sont conservées jusqu'au décès de la personne à laquelle le vaccin contre la COVD-19 a été administré et pendant 30 ans au minimum à compter de la vaccination (article 6, § 2).

La banque de données « Vaccinnet » « vise plusieurs objectifs en lien avec la vaccination : il s'agit de la prestation de soins de santé de qualité, la pharmacovigilance, la traçabilité des vaccins, la gestion de schémas de vaccination, l'organisation logistique de la vaccination, la détermination du taux de vaccination, l'organisation du suivi des contacts, l'exécution du suivi et de la surveillance, le calcul de la répartition des coûts de vaccination, l'exécution d'études scientifiques ou statistiques » (*ibid.*, p. 32400).

Les finalités de traitement des données enregistrées dans les deux banques de données sont mentionnées dans l'article 4 de l'accord de coopération du 12 mars 2021. Les données recueillies dans ces deux banques de données « ne peuvent pas être transmises à des tiers sauf lorsqu'une loi, un décret ou une ordonnance autorisent un tiers à avoir accès ou à recevoir de telles données et ce, uniquement pour qu'ils puissent poursuivre les mêmes finalités liées à la vaccination que celles visées à l'article 4 de l'accord de coopération » (*ibid.*, p. 32401), après autorisation par le Comité de sécurité de l'information.

Pour les deux banques de données, les entités fédérées compétentes ou les agences désignées par les entités fédérées compétentes et l'autorité fédérale agissent, chacune dans le cadre de leur compétence, en tant que responsables du traitement des données (article 7, § 1er). Pour les personnes qui ressortissent aux compétences de l'Autorité fédérale, Sciensano est identifié comme le responsable du traitement des données (article 7, § 1er, 7°). Un point de contact centralisé par entité et un droit d'accès électronique sont prévus (article 7, § 2).

La mise en œuvre et le respect de l'accord de coopération du 12 mars 2021 sont surveillés par la Conférence interministérielle Santé publique (article 9, § 1er).

B.4.1. Les dispositions de l'accord de coopération du 12 mars 2021 correspondent en substance à celles de l'arrêté royal du 24 décembre 2020 « concernant l'enregistrement et le

traitement de données relatives aux vaccinations contre la COVID-19 » (ci-après : l'arrêté royal du 24 décembre 2020), contre lequel la partie requérante a également introduit un recours en annulation devant le Conseil d'État. Le préambule de cet arrêté royal indiquait qu'« il est d'une importance vitale pour la santé publique et pour éviter une résurgence de la pandémie liée au COVID-19, que les mesures nécessaires en matière de vaccinations puissent être prises » (*Moniteur belge* du 24 décembre 2020, deuxième édition, p. 94404), dans l'attente de la conclusion d'un accord de coopération.

Cet arrêté royal est entré en vigueur le 24 décembre 2020, date de sa publication au *Moniteur belge*.

L'article 9 de l'arrêté royal du 24 décembre 2020 disposait :

« Le présent arrêté entre en vigueur au jour de sa publication dans le *Moniteur belge* et cesse ses effets le jour où entre en vigueur un accord de coopération entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 ».

B.4.2.1. L'arrêté royal du 24 décembre 2020 a été pris conformément à l'article 11 de la loi du 22 décembre 2020 « portant diverses mesures relatives aux tests antigéniques rapides et concernant l'enregistrement et le traitement de données relatives aux vaccinations dans le cadre de la lutte contre la pandémie de COVID-19 » (ci-après : la loi du 22 décembre 2020), qui disposait :

« Le médecin ou l'infirmier qui administre un vaccin contre la COVID-19 ou qui supervise la vaccination enregistre chaque vaccination dans la base de données désignée par la Conférence interministérielle Santé publique. Le Roi précise, par arrêté délibéré en Conseil des ministres, les modalités de cet enregistrement et définit au moins les finalités du traitement de données, les catégories de personnes à propos desquelles des données sont traitées, les catégories de données traitées, les responsables du traitement des données ainsi que la durée de conservation des données ».

B.4.2.2. Les travaux préparatoires de la loi du 22 décembre 2020 exposent à cet égard :

« L'article 11 impose l'obligation d'enregistrer chaque vaccination contre la COVID-19. Seuls les médecins ou les infirmiers sont légalement habilités à administrer des vaccins. La vaccination et l'enregistrement de la vaccination peuvent néanmoins être effectués par d'autres personnes sous leur supervision.

L'enregistrement des vaccinations est nécessaire pour mener une gestion de crise réfléchie, garantir le suivi médical (vigilance) de la personne vaccinée, suivre l'immunisation de la population et estimer l'impact sur l'assurance maladie et sur le nombre d'hospitalisations attendues.

L'enregistrement d'une vaccination implique le stockage dans une banque de données de données relatives à la personne vaccinée, de données relatives à la personne qui administre le vaccin, de données relatives aux circonstances d'administration du vaccin et de données relatives aux éventuels effets indésirables du vaccin.

La base de données sera créée et gérée en collaboration très étroite avec les entités fédérées. La Conférence interministérielle Santé publique désignera à cette fin la base de données dans laquelle les données visées seront sauvegardées.

Le Roi est habilité à fixer les conditions et les modalités s'appliquant à cet enregistrement, avec une attention particulière pour les aspects relatifs à la protection de la vie privée.

Il va toutefois sans dire que les données à caractère personnel collectées et traitées dans le cadre de cet enregistrement, seront traitées conformément à la réglementation relative à la protection à l'égard du traitement de données à caractère personnel, en particulier le Règlement général sur la protection des données, la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth.

Les entités fédérées et l'entité fédérale ont l'intention de préciser les règles de l'enregistrement et du traitement de données que celui-ci implique dans un Accord de coopération au sens de l'article 92*bis* de la loi spéciale de réformes institutionnelles du 8 août 1980. Vu l'extrême urgence d'entamer la vaccination et l'absolue nécessité d'enregistrer les vaccinations pour les raisons susmentionnées, il est entre-temps pourvu à la présente réglementation » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1677/001, pp. 10-11).

B.4.2.3. L'article 11 de la loi du 22 décembre 2020 a été abrogé par l'article 11 de l'accord de coopération du 12 mars 2021.

B.4.3. Le préambule de l'arrêté royal du 24 décembre 2020 indique que la base de données des vaccinations a été désignée par la Conférence interministérielle Santé publique du 3 décembre 2020 (*Moniteur belge* du 24 décembre 2020, p. 94404). L'article 1er, 2°, de l'arrêté royal du 24 décembre 2020 définit la « base de données des vaccinations » comme « la base de données désignée par la Conférence interministérielle Santé publique en vertu de l'article 11 de

la loi du 22 décembre 2020 portant diverses mesures relatives aux tests antigéniques rapides et concernant l'enregistrement et le traitement de données relatives aux vaccinations dans le cadre de la lutte contre la pandémie de COVID-19 ».

Au sujet de cette banque de données, les travaux préparatoires de la loi du 22 décembre 2020 indiquent :

« La proposition de loi à l'examen confère d'urgence un fondement légal à l'obligation d'enregistrer et de collecter les données relatives à la vaccination. Cet enregistrement est nécessaire pour pouvoir contrôler tous les aspects de la gestion de la crise. Il a été décidé d'inclure tous les enregistrements des différentes vaccinations dans la banque de données de vaccination flamande VaccinNet » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1677/002, p. 4).

B.4.4.1. Un protocole d'accord du 27 janvier 2021 « entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 » (ci-après : le protocole d'accord du 27 janvier 2021) reprend en grande partie le contenu des dispositions de l'arrêté royal du 24 décembre 2020. Le préambule de ce protocole d'accord indique que ce protocole « a pu être réalisé en respect de la répartition de compétences qui en vertu de la loi spéciale de réformes institutionnelles ont été attribuées aux différents niveaux de pouvoirs grâce à une collaboration intense au sein de la Conférence Interministérielle qui s'inscrit dans une longue tradition de collaboration au sein de la Conférence Interministérielle de santé entre les différents niveaux de pouvoirs de notre pays » et que, « dans le cadre de la vaccination contre la COVID-19, un enregistrement des données de vaccination dans une base de données commune par les vaccinateurs flamands, bruxellois, wallons et germanophones est absolument nécessaire pour diverses finalités » (*Moniteur belge* du 11 février 2021, p. 13033).

L'article 1er, 3°, du protocole d'accord du 27 janvier 2021 définit « Vaccinnet » comme « le système d'enregistrement visé à l'article 9 de l'arrêté du Gouvernement flamand du 16 mai 2014 portant diverses dispositions en exécution du décret [flamand] du 21 novembre 2003 relatif à la politique de santé préventive et modifiant des arrêtés d'exécution de ce décret ». Conformément à l'article 43 du décret, précité, du 21 novembre 2003, les vaccinateurs doivent

collaborer au système d'enregistrement « Vaccinnet » lorsque, sur la base de sa compétence en matière de politique de santé préventive, le Gouvernement flamand établit un schéma de vaccination qui reprend les vaccinations recommandées pour la population.

La banque de données « Vaccinnet » visée dans le protocole d'accord du 27 janvier 2021 constitue ainsi une extension, concernant les vaccinations contre la COVID-19, de la banque de données existante « Vaccinnet », créée au niveau de la Communauté flamande. La répartition du coût de développement de « Vaccinnet » a été fixée dans l'article 6 du protocole d'accord du 9 février 2022 conclu entre le Gouvernement fédéral et les autorités visées aux articles 128, 130 et 135 de la Constitution « concernant le cofinancement du programme de vaccination contre la COVID-19 ».

B.4.4.2. L'article 11 du protocole d'accord du 27 janvier 2021 dispose :

« Le présent protocole d'accord n'est pas un accord de coopération au sens de l'article 92*bis* de la loi spéciale de réformes institutionnelles du 8 août 1980. Les parties se proposent, sur la base des dispositions du présent protocole d'accord, de parvenir à un accord de coopération pour le 21 avril 2021 ».

L'article 12 du protocole d'accord du 27 janvier 2021 dispose :

« Le présent protocole d'accord produit ses effets à dater du 24 décembre 2020 et cesse ses effets le jour où entre en vigueur un accord de coopération entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 ».

B.5. Conformément à son article 12, alinéa 1er, l'accord de coopération du 12 mars 2021 produit ses effets à partir du 24 décembre 2020 pour ce qui concerne les dispositions dont le contenu correspond à celui de l'arrêté royal du 24 décembre 2020 concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 et à partir du 11 février 2021 pour ce qui concerne les autres dispositions.

Conformément à l'article 9 de l'arrêté royal du 24 décembre 2020 et à l'article 12 du protocole d'accord du 27 janvier 2021, l'arrêté royal du 24 décembre 2020 et le protocole

d'accord du 27 janvier 2021 ont cessé de produire leurs effets le jour de l'entrée en vigueur de l'accord de coopération du 12 mars 2021, soit le 22 avril 2021.

B.6. Les sept législations attaquées (ci-après : les actes attaqués) se limitent à porter assentiment à l'accord de coopération du 12 mars 2021.

Quant à la recevabilité ratione temporis *du recours*

B.7. Le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune estiment que le recours en annulation, introduit le 7 octobre 2021, est manifestement irrecevable *ratione temporis* en ce qu'il est dirigé contre le décret d'assentiment de la Communauté française du 25 mars 2021, publié au *Moniteur belge* le 6 avril 2021.

B.8.1. Pour satisfaire aux exigences de l'article 3, § 1er, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, un recours en annulation doit être introduit dans le délai de six mois suivant la publication de la norme attaquée au *Moniteur belge*.

B.8.2. La disposition précitée n'établit aucune distinction quant à la prise d'effet du délai de recours en annulation dirigé contre la norme attaquée, selon qu'elle porte ou non assentiment à un accord de coopération.

Contrairement à ce qu'allègue la partie requérante, le délai pour introduire un recours en annulation contre des actes d'assentiment à un accord de coopération ne prend pas cours à dater de l'entrée en vigueur de cet accord de coopération, mais commence à courir à la date de la publication des actes attaqués.

B.8.3. Dans une série d'arrêts précédents, la Cour a déjà indiqué que, pour fixer le délai d'introduction d'un recours ou d'une demande de suspension, il faut – à défaut de précision dans la loi spéciale du 6 janvier 1989 et par analogie avec le régime de l'article 54 du Code judiciaire – calculer de quantième à veille de quantième (voy. l'arrêt n° 125/2012 du 18 octobre 2012, ECLI:BE:GHCC:2012:ARR.125, B.2; l'arrêt n° 169/2016 du 22 décembre 2016, ECLI:BE:GHCC:2016:ARR.169, B.2).

Le décret d'assentiment de la Communauté française du 25 mars 2021 a été publié au *Moniteur belge* du 6 avril 2021. Le délai pour introduire un recours contre cet acte a donc pris cours le 7 avril 2021 et a expiré le 6 octobre 2021. Il s'ensuit que le recours en annulation introduit par requête déposée à la poste le 7 octobre 2021 est manifestement irrecevable.

B.8.4. En ce qu'il est dirigé contre le décret d'assentiment de la Communauté française du 25 mars 2021, le recours en annulation est irrecevable *ratione temporis*.

Quant à l'étendue du recours en annulation

B.9.1. Pour satisfaire aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989, les moyens de la requête doivent faire connaître, parmi les règles dont la Cour garantit le respect, celles qui seraient violées ainsi que les dispositions qui violeraient ces règles et exposer en quoi ces règles auraient été transgressées par ces dispositions.

B.9.2. La Cour détermine l'étendue du recours en annulation en fonction du contenu de la requête et en particulier sur la base de l'exposé des moyens. La Cour limite son examen aux dispositions contre lesquelles des griefs sont effectivement dirigés.

B.10.1. Il ressort de l'exposé du moyen unique que les griefs de la partie requérante ne sont dirigés contre les actes attaqués qu'en ce qu'ils portent assentiment à certaines dispositions de l'accord de coopération du 12 mars 2021 qui organisent l'enregistrement et le traitement des

données à caractère personnel dans la banque de données « Vaccinnet », que la partie requérante identifie expressément dans son moyen :

- l'article 2, § 2, qui vise l'enregistrement des données de vaccination;

- l'article 3, § 2, qui détermine les données de vaccination recueillies dans « Vaccinnet »;

- l'article 4, § 2, qui fixe les finalités pour le traitement des données visées à l'article 3, § 2;

- l'article 5, qui permet la communication à des tiers des données figurant dans « Vaccinnet »;

- l'article 6, § 2, qui fixe la durée de conservation des données visées à l'article 3, § 2;

- l'article 12, qui fixe la date d'entrée en vigueur des dispositions de l'accord de coopération du 12 mars 2021.

B.10.2. Cependant, lorsqu'elle critique ces dispositions dans son moyen unique, la partie requérante ne formule aucun grief contre le principe même de l'enregistrement des données de vaccination, ni contre les données de vaccination recueillies dans « Vaccinnet ». En dehors d'une critique générale, elle n'expose pas en quoi, en portant assentiment aux articles 2, § 2, et 3, § 2, de l'accord de coopération du 12 mars 2021, les actes attaqués violeraient les dispositions visées dans le moyen.

En ce qu'il vise ces dispositions, le moyen unique ne répond dès lors pas aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989.

B.10.3. La Cour limite par conséquent son examen du recours en annulation dirigé contre les actes attaqués en ce qu'ils portent assentiment aux articles 4, § 2, 5 et 6, § 2, de l'accord de coopération du 12 mars 2021, et à l'article 12 de l'accord de coopération, précité, en ce que ce dernier fixe la date d'entrée en vigueur des articles 4, § 2, 5 et 6, § 2, précités.

Le recours en annulation est par conséquent irrecevable en ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment aux autres dispositions de l'accord de coopération précité.

B.10.4. La Cour rappelle qu'elle ne peut utilement contrôler les actes attaqués sans impliquer dans son examen le contenu des dispositions pertinentes de l'accord de coopération précité.

Quant à l'intérêt de la partie requérante

B.11. La partie requérante justifie son intérêt à agir par le fait qu'elle est une personne physique résidant en Belgique et qu'elle est susceptible de se faire vacciner contre la COVID-19, de sorte que les actes attaqués peuvent l'affecter directement et défavorablement. En effet, si elle décide de se faire vacciner, son nom et ses différentes données à caractère personnel figureront dans « Vaccinnet », en violation de son droit au respect de la vie privée, lu en combinaison avec le principe de la non-rétroactivité des lois. Si, par contre, elle décide de ne pas se faire vacciner, il existerait un risque sérieux que des restrictions l'affectent en raison de sa non-vaccination.

B.12. Le Conseil des ministres, le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté française, le Gouvernement de la Communauté germanophone, le Collège de la Commission communautaire française et le Collège réuni de la Commission communautaire commune contestent l'intérêt à agir de la partie requérante, estimant que son action s'apparente à un recours populaire.

B.13. La Constitution et la loi spéciale du 6 janvier 1989 imposent à toute personne physique ou morale qui introduit un recours en annulation de justifier d'un intérêt. Ne justifient de l'intérêt requis que les personnes dont la situation pourrait être affectée directement et défavorablement par la norme attaquée.

B.14.1. En vertu de l'article 2, § 1er, non attaqué, de l'accord de coopération du 12 mars 2021, toute personne physique se trouvant sur le territoire de la Belgique est appelée à recevoir

une invitation à se faire vacciner par le biais d'un code de vaccination contre la COVID-19, conformément à la stratégie de vaccination définie par les autorités compétentes. Ce code de vaccination sans signification est généré par la banque de données organisée conformément à l'article 3, § 1er, non attaqué, de l'accord de coopération du 12 mars 2021.

Conformément à l'article 2, § 2, de l'accord de coopération du 12 mars 2021, chaque vaccination donne lieu à l'enregistrement, dans « Vaccinnet », des données de vaccination mentionnées à l'article 3, § 2, de l'accord de coopération du 12 mars 2021. Toutes les personnes qui se font vacciner contre la COVID-19 sont par conséquent soumises à l'enregistrement automatique de leurs données de vaccination dans la banque de données « Vaccinnet » et aux traitements de ces données conformément à ce que prévoit cet accord de coopération.

En sa qualité de personne physique se trouvant sur le territoire de la Belgique, la partie requérante a nécessairement été invitée à se faire vacciner et elle ne pouvait accepter l'invitation de se faire vacciner qu'en donnant son consentement pour que ses données de vaccination soient enregistrées et traitées dans « Vaccinnet » conformément aux actes attaqués portant assentiment à l'accord de coopération du 12 mars 2021. Les implications des actes attaqués en matière de traitement des données de vaccination sont dès lors susceptibles d'influencer directement le choix de la partie requérante quant à sa vaccination contre la COVID-19.

B.14.2. Il découle de ce qui précède que les actes attaqués sont susceptibles d'affecter directement et défavorablement la partie requérante dans sa décision de se faire vacciner.

B.14.3. Pour le surplus, l'accord de coopération du 12 mars 2021 se limite à organiser le système commun pour l'enregistrement des données de vaccination contre la COVID-19 sur le territoire de la Belgique. Cet accord de coopération ne crée aucune obligation vaccinale, la stratégie vaccinale exposée en B.2.2 étant fondée sur une vaccination volontaire et gratuite.

Contrairement à ce qu'allègue la partie requérante, les actes attaqués ne prévoient aucune conséquence qui serait liée à l'absence de vaccination. Les incidences d'un certificat de vaccination, mais également d'un certificat de test et de rétablissement, pour l'obtention d'un

CST, sont quant à elles déterminées dans les accords de coopération du 14 juillet 2021, du 27 septembre 2021 et du 28 octobre 2021, cités en B.2.3.4. Non seulement la partie requérante ne démontre pas la réalité des restrictions qu'elle invoque et qui découleraient de l'absence de vaccination – ce qui suffit pour établir que le préjudice allégué est purement hypothétique –, mais ces éventuelles restrictions ne constituent pas un préjudice qui découlerait directement des actes attaqués par le recours présentement examiné.

En ce qu'elle invoque les conséquences liées à la non-vaccination contre la COVID-19, la partie requérante ne justifie pas de l'intérêt requis.

Quant au fond

B.15. Le moyen unique est pris de la violation de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, avec les articles 5, 6, 9 et 35 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) » (ci-après : le RGPD), ainsi qu'avec le principe de la non-rétroactivité des lois.

B.16.1. L'article 22 de la Constitution dispose :

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

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

B.16.2. L'article 8 de la Convention européenne des droits de l'homme dispose :

« 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 ».

B.16.3. Le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme (*Doc. parl*., Chambre, 1992-1993, n° 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un tout indissociable.

B.16.4. Le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelles et conventionnelles précitées a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée.

Ce droit a une portée étendue et englobe, entre autres, le respect de l'intégrité physique de la personne (CEDH, grande chambre, 8 avril 2021, *Vavřička e.a. c. République tchèque*, ECLI:CE:ECHR:2021:0408JUD004762113, § 261) et la protection des données à caractère personnel et des informations personnelles relatives à la santé (CEDH, 25 février 1997, *Z. c. Finlande*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; 10 octobre 2006, *L.L. c. France*, ECLI:CE:ECHR:2006:1010JUD000750802, § 32; 27 février 2018, *Mockuté c. Lituanie*, ECLI:CE:ECHR:2018:0227JUD006649009, § 93). La jurisprudence de la Cour européenne des droits de l'homme fait apparaître que de la protection de ce droit relèvent notamment les données et informations personnelles suivantes : le nom, l'adresse, les activités professionnelles, les relations personnelles, les empreintes digitales, les images filmées, les photographies, les communications, les données ADN, les données judiciaires (condamnations ou inculpations), les données financières, les informations concernant des biens et les données médicales (voy. notamment CEDH, 26 mars 1987, *Leander c. Suède*, ECLI:CE:ECHR:1987:0326JUD000924881, §§ 47-48; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 66-68; 17 décembre 2009, *B.B. c. France*, ECLI:CE:ECHR:2009:1217JUD000533506, § 57; 10 février 2011, *Dimitrov-Kazakov c. Bulgarie*, ECLI:CE:ECHR:2011:0210JUD001137903, §§ 29-31; 18 octobre 2011, *Khelili c. Suisse*, ECLI:CE:ECHR:2011:1018JUD001618807, §§ 55-57; 9 octobre 2012, *Alkaya c. Turquie*, ECLI:CE:ECHR:2012:1009JUD004281106,

§ 29; 18 avril 2013, *M.K. c. France*, ECLI:CE:ECHR:2013:0418JUD001952209, § 26; 18 septembre 2014, *Brunet c. France*, ECLI:CE:ECHR:2014:0918JUD002101010, § 31; 13 octobre 2020, *Frâncu c. Roumanie*, ECLI:CE:ECHR:2020:1013JUD006935613, § 51).

La protection des données à caractère personnel relatives à la santé est capitale non seulement pour protéger la vie privée de la personne, mais également pour préserver sa confiance dans les services de santé (CEDH, 25 février 1997, *Z. c. Finlande*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95). Faute d'une telle protection, les personnes pourraient être dissuadées de fournir les informations à caractère personnel et intime nécessaires à la prescription du traitement approprié, ce qui pourrait mettre en danger leur santé voire, dans les cas des maladies transmissibles, celle de la collectivité (*ibid.*, § 95).

B.16.5. Le droit au respect de la vie privée n'est toutefois pas absolu. L'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme n'excluent pas une ingérence d'une autorité publique dans l'exercice de ce droit, pourvu que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit. Ces dispositions engendrent de surcroît l'obligation positive, pour l'autorité publique, de prendre des mesures qui assurent le respect effectif de la vie privée, même dans la sphère des relations entre les individus (CEDH, 27 octobre 1994, *Kroon et autres c. Pays-Bas*, ECLI:CE:ECHR:1994:1027JUD001853591, § 31; grande chambre, 12 novembre 2013, *Söderman c. Suède*, ECLI:CE:ECHR:2013:1112JUD000578608, § 78).

Lorsqu'elles mettent en balance l'intérêt de l'État à traiter des données à caractère personnel et l'intérêt individuel à la protection de la confidentialité de ces données, les autorités nationales disposent d'une certaine marge d'appréciation (*ibid.*, § 99). Eu égard à l'importance fondamentale de la protection des données à caractère personnel, cette marge est toutefois assez limitée (CEDH, 26 janvier 2017, *Surikov c. Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 73). Pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut qu'un juste équilibre soit atteint entre tous les droits et intérêts en cause. Pour juger de cet équilibre, il faut tenir compte notamment des dispositions

de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après : la Convention n° 108) (CEDH, 25 février 1997, *Z c. Finlande*, ECLI:CE:ECHR:1997:0225JUD002200993, § 95; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, § 103; 26 janvier 2017, *Surikov c. Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

La Convention n° 108 contient, entre autres, les principes relatifs au traitement de données à caractère personnel : licéité, loyauté, transparence, limitation des finalités, proportionnalité, exactitude, limitation de la conservation, intégrité et confidentialité, et responsabilité.

La même Convention est actualisée par un protocole d'amendement ouvert à signature le 10 octobre 2018.

Il découle de la Convention n° 108 que le droit national doit notamment garantir que les données à caractère personnel sont pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou détenues, que les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire et que les données détenues sont protégées efficacement contre les usages impropres et abusifs. Elle a aussi indiqué qu'il est essentiel que le droit national prévoie des règles claires et détaillées relatives à la portée et à l'application des mesures concernées, ainsi que des garanties minimales concernant, entre autres, la durée, la conservation, l'utilisation, l'accès des tiers, les procédures de préservation de l'intégrité et de la confidentialité des données et les procédures de destruction de celles-ci, de sorte qu'il existe suffisamment de garanties contre le risque d'abus et d'arbitraire à chaque étape du traitement des données (CEDH, 26 janvier 2017, *Surikov c. Ukraine*, ECLI:CE:ECHR:2017:0126JUD004278806, § 74).

B.16.6. Dans le champ d'application du droit de l'Union européenne, l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme et l'article 7 de la Charte garantissent des droits fondamentaux analogues (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke GbR e.a.,* ECLI:EU:C:2010:662), alors que l'article 8 de cette Charte vise spécifiquement la protection des données à caractère personnel.

B.16.7. La Cour de justice de l'Union européenne considère que le respect du droit à la vie privée à l'égard du traitement de données à caractère personnel se rapporte à toute information concernant une personne physique identifiée ou identifiable (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke GbR e.a,* ECLI:EU:C:2010:662, point 52; 16 janvier 2019, C-496/17, *Deutsche Post AG*, ECLI:EU:C:2019:26, point 54).

B.16.8. Les droits consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne n'apparaissent pas non plus comme étant des prérogatives absolues (CJUE, grande chambre, 16 juillet 2020, C-311/18, *Data Protection Commissioner*, ECLI:EU:C:2020:559, point 172).

Conformément à l'article 52, paragraphe 1, première phrase, de la Charte des droits fondamentaux de l'Union européenne, toute limitation de l'exercice des droits et libertés reconnus par celle-ci, dont notamment le droit au respect de la vie privée garanti par l'article 7 et le droit à la protection des données à caractère personnel consacré par l'article 8, doit être prévue par la loi, respecter le contenu essentiel de ces droits et, dans le respect du principe de proportionnalité, être nécessaire et répondre effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui (CJUE, grande chambre, 6 octobre 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, point 64). Dans le même sens, conformément à l'article 23 du RGPD, les limitations apportées à certaines obligations des responsables du traitement prévues par la Charte des droits fondamentaux de l'Union européenne et aux droits des intéressés doivent être prévues par la loi, respecter l'essence des libertés et des droits fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique pour atteindre le but poursuivi et respecter les dispositions spécifiques contenues au paragraphe 2 (CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791, points 209-210; 10 décembre 2020, C-620/19, *Land Nordrhein-Westfalen*, ECLI:EU:C:2020:1011, point 46).

B.16.9. L'article 22 de la Constitution réserve au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée. Il garantit ainsi à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur.

Par conséquent, les éléments essentiels du traitement des données à caractère personnel doivent être fixés dans la loi, le décret ou l'ordonnance même. À cet égard, quelle que soit la matière concernée, les éléments suivants constituent en principe, des éléments essentiels : (1°) la catégorie de données traitées; (2°) la catégorie de personnes concernées; (3°) la finalité poursuivie par le traitement; (4°) la catégorie de personnes ayant accès aux données traitées et (5°) le délai maximal de conservation des données (avis de l'assemblée générale de la section de législation du Conseil d'État n° 68.936/AG du 7 avril 2021 sur un avant-projet de loi « relative aux mesures de police administrative lors d'une situation d'urgence épidémique », (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1951/001, p. 119).

B.16.10. Outre l'exigence de légalité formelle, l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne, impose que l'ingérence dans l'exercice du droit au respect de la vie privée et du droit à la protection des données à caractère personnel soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

En matière de protection des données, cette exigence de prévisibilité implique qu'il doit être prévu de manière suffisamment précise dans quelles circonstances les traitements de données à caractère personnel sont autorisés (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). L'exigence selon laquelle la limitation doit être prévue par la loi implique notamment que la base légale qui permet l'ingérence dans ces droits doit elle-même définir la portée de la limitation de l'exercice du droit concerné (CJUE, 6 octobre 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, point 65).

Toute personne doit dès lors pouvoir avoir une idée suffisamment claire des données traitées, des personnes concernées par un traitement de données déterminé et des conditions et finalités dudit traitement.

B.16.11. L'article 5 du RGPD, intitulé « Principes relatifs au traitement », dispose :

« 1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

L'article 6 du RGPD, intitulé « Licéité du traitement », dispose :

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

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

2. Les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX.

3. Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par :

a) le droit de l'Union; ou

b) le droit de l'État membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres : les conditions générales régissant

la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi.

4. Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1, le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres :

a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé;

b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement;

c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10;

d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées;

e) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation ».

L'article 9 du RGPD, intitulé « Traitement portant sur des catégories particulières de données à caractère personnel », dispose :

« 1. Le 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, 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 sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;

[…]

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 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 et soumis aux conditions et garanties visées au paragraphe 3;

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, 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;

[…]

3. Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents.

4. Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé ».

L'article 35 du RGPD, intitulé « Analyse d'impact relative à la protection des données », dispose :

« 1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

2. Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

3. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants :

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

4. L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68.

5. L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité.

6. Avant d'adopter les listes visées aux paragraphes 4 et 5, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.

7. L'analyse contient au moins:

a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;

b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;

c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et

d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

8. Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

9. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

10. Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

11. Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement ».

B.16.12. La non-rétroactivité des lois est une garantie ayant pour but de prévenir l'insécurité juridique. Cette garantie exige que le contenu du droit soit prévisible et accessible, de sorte que le justiciable puisse prévoir, dans une mesure raisonnable, les conséquences d'un acte déterminé au moment où cet acte est accompli. La rétroactivité ne se justifie que si elle est indispensable à la réalisation d'un objectif d'intérêt général.

S'il s'avère que la rétroactivité a en outre pour but ou pour effet d'influencer dans un sens l'issue de procédures judiciaires ou que les juridictions soient empêchées de se prononcer sur une question de droit bien précise, la nature du principe en cause exige que des circonstances exceptionnelles ou des motifs impérieux d'intérêt général justifient l'intervention du législateur, laquelle porte atteinte, au préjudice d'une catégorie de citoyens, aux garanties juridictionnelles offertes à tous.

B.17. Les griefs de la partie requérante portent sur les aspects suivants :

I. les finalités du traitement des données de vaccination, visées à l'article 4, § 2 (première branche) (B.18-B.24);

II. l'habilitation, visée à l'article 5, conférée au Comité de sécurité de l'information d'autoriser la communication de données à caractère personnel à des tiers (première branche) (B.25-B.32);

III. la durée de conservation des données enregistrées dans « Vaccinnet », visée à l'article 6 (deuxième branche) (B.33-B.38);

IV. l'absence d'analyse d'impact préalable requise par l'article 35 du RGPD (deuxième branche) (B.39-B.45);

V. la rétroactivité des effets de l'accord de coopération au 24 décembre 2020, prévue par l'article 12 (troisième branche) (B.46-B.50).

I. En ce qui concerne les finalités du traitement des données de vaccination, visées à l'article 4, § 2 (première branche)

B.18. Dans la première branche du moyen, la partie requérante estime que les onze finalités définies dans l'article 4, § 2, de l'accord de coopération du 12 mars 2021 ne sont pas suffisamment « déterminées et explicites », de sorte que ne sont pas respectés les principes de légalité et de prévisibilité à l'égard d'éléments essentiels du traitement de données sensibles à caractère personnel. Elle critique plus précisément le caractère large de la finalité visée au 1° ainsi que la nécessité de la finalité visée au 11°.

B.19. L'article 4, § 2, de l'accord de coopération du 12 mars 2021 dispose :

« Le traitement des données à caractère personnel visées à l'article 3, § 2, poursuit les finalités de traitement suivantes :

1° la prestation de soins de santé et de traitements, telle que visée à l'article 9, 2, h du Règlement général sur la Protection des données, ce que visent exclusivement l'acte de vaccination et les mesures de soutien, d'information, de sensibilisation des citoyens en rapport avec la vaccination;

2° la pharmacovigilance des vaccins contre la COVID-19, conformément à l'article 12*sexies* 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;

3° 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, 3ème 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;

4° la gestion de schémas de vaccinations contre la COVID-19 par personne à vacciner ou vaccinée et la planification des plages de vaccination, notamment par les centres de vaccination;

5° 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;

6° la détermination du taux de vaccination anonyme contre la COVID-19 de la population;

7° l'organisation du suivi des contacts en exécution de l'Accord de coopération du 25 août 2020 entre l'Etat 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;

8° l'exécution du suivi et de la surveillance post-autorisation des vaccins 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;

9° sans préjudice de la réglementation relative à l'assurance maladie, le calcul de la répartition des coûts de vaccination entre l'Etat fédéral et les entités fédérées, après anonymisation des données ou à tout le moins pseudonymisation des données dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser le calcul de répartition;

10° l'exécution d'études scientifiques ou statistiques, conformément à l'article 89, § 1er, du Règlement général sur la protection des données et, le cas échéant, à l'article 89, §§ 2 et 3, du Règlement général sur la protection des données et 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, après anonymisation, ou à tout le moins pseudonymisation, dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser l'étude scientifique ou statistique.

11° l'information et la sensibilisation des personnes concernant la vaccination contre la COVID-19 par les prestataires de soins et les organismes assureurs ».

B.20.1. Concernant les finalités visées à l'article 4, l'exposé général de l'accord de coopération du 12 mars 2021 indique :

« L'article 4 décrit les finalités de traitement par base de données; il s'agit dans l'ensemble des finalités suivantes :

- la prestation des soins de qualité pour la personne concernée, ce que visent exclusivement l'acte de vaccination et les mesures de soutien, d'information, de sensibilisation des citoyens en rapport avec la vaccination;

- la pharmacovigilance;

- la traçabilité des vaccins;

- la gestion de schémas de vaccination contre la COVID-19 et la planification des plages de vaccination, notamment par les centres de vaccination et par les prestataires de soins;

- l'organisation logistique de la vaccination contre la COVID-19; à cet égard, il est utile de préciser que pour atteindre cette finalité, tant la base de données des codes de vaccination que la base de données d'enregistrement des vaccinations sont nécessaires, la seconde permettant notamment d'alimenter la première par exemple afin d'éviter de réinviter des personnes déjà vaccinées ou encore d'identifier les besoins en vaccins ou de personnel médical au regard des vaccinations devant encore être administrées;

- la détermination du taux de vaccination anonyme contre la COVID-19 de la population;

- l'organisation du traçage des contacts;

- l'exécution du suivi et de la surveillance post-autorisation des vaccins;

- le calcul de la répartition des coûts de vaccination entre l'Etat fédéral et les entités fédérées;

- le soutien de la recherche scientifique, notamment en matière d'efficacité et de sécurité des vaccins;

- l'information et la sensibilisation des personnes concernant la vaccination contre la COVID-19 par les services d'inspection d'hygiène des entités fédérées, les prestataires de soins et les organismes assureurs afin d'obtenir un degré de vaccination maximal;

- l'invitation et l'offre d'aide lors du processus d'invitation des personnes à se faire vacciner contre la COVID-19 par les prestataires de soins, les organismes assureurs, les centres de vaccination, l'autorité fédérale, les entités fédérées compétentes et les administrations locales.

Concernant la finalité relative au suivi et à la surveillance post-autorisation des vaccins, il peut être précisé les éléments suivants.

Les études sur l'acceptation et l'utilisation des vaccins et la couverture vaccinale permettent de savoir combien de personnes sont prêtes à se faire vacciner et combien le font effectivement. Plus précisément, les études de couverture vaccinale permettent d'estimer la proportion de personnes vaccinées dans des groupes à risque spécifiques, comme les personnes âgées ou les personnes souffrant de troubles sous-jacents spécifiques. Ces études donneront un aperçu des attitudes de la population à l'égard des vaccins et aideront à identifier les lacunes du programme de vaccination qui doivent être comblées.

Le suivi de l'efficacité, de la séroprévalence et de l'immunogénicité des vaccins permet d'évaluer la capacité du vaccin à induire une réponse immunitaire et à prévenir l'infection à long terme et en cas de nouvelles souches en circulation.

Enfin, il est crucial de surveiller la qualité des vaccins et de mettre en place un système capable de détecter les effets indésirables tardifs ou rares afin de continuer à garantir la sécurité des vaccins.

Dans l'ensemble, les résultats de la surveillance post-autorisation sont utilisés pour orienter la politique en matière de vaccins et pour informer les professionnels de la santé et la population générale des résultats du programme de vaccination COVID-19 de la Belgique.

En tout état de cause, ce suivi et la surveillance post-autorisation des vaccins est organisée conformément aux bonnes pratiques recommandées par l'Organisation mondiale de la Santé en la matière.

Il y a lieu de souligner l'importance du rapport avec le traçage des contacts dès lors qu'une des finalités concerne l'organisation du traçage. Les scénarios visés qui permettent la liaison entre la vaccination et le suivi de contact doit impérativement s'inscrire dans un but exclusif de suivi de contact infectieux et du suivi de la vaccination. Sont notamment envisageables :

- l'avis qui doit être formulé par le centre de contact peut varier en fonction du fait qu'une personne a ou non été vaccinée;

- la source est vaccinée mais a infecté plusieurs contacts; il s'agit d'un cas d'échec du vaccin ou d'un variant de la souche contre lequel le vaccin n'offre pas de protection et donc d'informations très importantes pour la santé publique;

- la source n'est pas vaccinée, ce qui a causé l'infection d'autres personnes;

- les contacts sont susceptibles d'être vaccinés, ce qui permet à l'épidémie de s'éteindre dès lors que le vaccin s'avère être une mesure de prophylaxie efficace;

- les contacts ne sont pas vaccinés, il y a donc lieu de continuer à cartographier activement l'épidémie.

Les données qui sont transmises dans ce cadre à partir de Vaccinnet vers la banque de données de Sciensano concernent a priori le NISS, le statut de vaccination et le type de vaccin, mais une flexibilité s'impose en fonction de l'évolution des connaissances scientifiques en ce qui concerne l'impact de la vaccination sur les risques d'infection.

Par ailleurs, il y a lieu de souligner que les données à caractère personnel sont nécessaires pour assurer le suivi médical du patient en rapport avec la vaccination COVID-19 dès lors qu'une couverture vaccinale importante au sein de la population constitue un enjeu majeur et fondamental de santé publique au regard de la crise pandémique inédite de la COVID-19 ainsi qu'à l'échelle de l'individu qui doit pouvoir réaliser un choix pour sa santé personnelle de manière informée. Ceci requiert, en effet, une combinaison d'informations générales et ciblées (à l'initiative du médecin traitant ou de l'organisme assureur pour leurs propres patients et membres). Il est notamment d'une importance capitale que le médecin (le médecin généraliste, le spécialiste) évalue, sur la base de ses connaissances détaillées de l'anamnèse médicale du patient confié à ses soins, si la vaccination du patient qui a été correctement informé, est ou non importante. Dans ce cadre, il convient de souligner qu'il y a lieu de veiller en permanence à un taux de vaccination suffisant (par exemple, 70 pour cent) et qu'il est important d'assurer un suivi ciblé (via des campagnes et au niveau individuel) à ce niveau. Il va de soi qu'il est interdit de contacter, si elles ne le souhaitent pas, les personnes qui ont explicitement déclaré qu'elles refusent le vaccin.

N'est pas visé dans la finalité relative à la prestation de soins de qualité, le fait de limiter ou de conditionner l'accès à des soins de qualité de quelque manière que ce soit en raison de l'état vaccinal d'une personne.

Il y a ensuite lieu d'observer que le degré de vaccination anonyme contre la COVID-19 doit pouvoir être déterminé de manière granulaire (par exemple dans les centres de soins résidentiels, une distinction doit être opérée entre le personnel soignant et les résidents) et que cette détermination ne peut pas toujours être réalisée au moyen de données anonymes ou à tout le moins pseudonymisées au cas où l'anonymisation ne permettrait pas d'atteindre l'objectif visé.

Par ailleurs, il est utile de préciser que toutes les catégories de données enregistrées à la fois dans la banque de données des codes de vaccination et dans la banque de données d'enregistrement des vaccinations peuvent en principe être traitées et conservées pour chacune des finalités. Le texte de l'accord de coopération précise, par ailleurs, les cas où seules des données anonymes ou à tout le moins pseudonymisées sont concernées, au cas où l'anonymisation ne permettrait pas d'atteindre l'objectif visé.

Les données collectées dans le cadre du présent accord de coopération ne peuvent être utilisées à d'autres fins que celles prévues dans le présent accord.

Les données collectées dans le cadre du présent accord de coopération ne peuvent donc pas être utilisées à d'autres fins que celles prévues par le présent article, notamment mais pas exclusivement à des fins policières, commerciales, fiscales, pénales ou de sécurité de l'Etat.

Finalement, l'utilisation des données des bases de données doit évidemment être conforme à l'article 14 de la Convention européenne des droits de l'homme, aux articles 10 et 11 de la Constitution et à la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination.

Tout utilisateur de soins a le droit d'obtenir une attestation de vaccination. Cette attestation ne peut cependant jamais donner lieu à une discrimination à l'égard des utilisateurs de soins » (*Moniteur belge* du 12 avril 2021, pp. 32404-32408; voy. aussi *Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, pp. 9-13).

B.20.2. Dans son avis sur l'avant-projet de loi devenu la loi du 2 avril 2021 portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé, concernant les finalités du traitement de données :

« Le paragraphe 2, 9°, prévoit comme finalité de traitement

' la répartition des coûts de vaccination entre l'État fédéral et les entités fédérées, après anonymisation des données ou à tout le moins pseudonymisation des données dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser le calcul de répartition '.

Conformément au principe de minimisation des données, si l'enregistrement de données anonymisées suffit pour atteindre l'objectif poursuivi, il ne convient pas de prévoir la possibilité de pseudonymisation.

Interrogés quant aux hypothèses dans lesquelles l'anonymisation des données ne permettrait pas de réaliser le calcul de répartition des coûts de vaccination, les délégués ont précisé ce qui suit :

' *In het kader van de regelgeving inzake de ziekteverzekering kan het nodig zijn over persoonsgegevens te beschikken* '.

Il n'est pas possible, à la lumière de cette réponse, de se prononcer quant à l'admissibilité du dispositif à l'examen. L'auteur de l'avant-projet est donc invité à préciser davantage, dans le commentaire de l'article, les situations dans lesquelles l'anonymisation des données ne permettrait pas de réaliser le calcul de répartition des coûts de vaccination » (*ibid.*, pp. 51-52; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, p. 88; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, p. 84; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 31-32; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 16-17; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, p. 32).

B.20.3. Dans son avis n° 16/2021 du 10 février 2021, relatif au projet d'accord de coopération devenu l'accord de coopération du 12 mars 2021, l'Autorité de protection des données a observé :

« 33. Les finalités suivantes formulées de manière large nécessitent (toujours) au moins d'être davantage délimitées et précisées :

- *' la prestation de soins de santé et de traitements, telle que visée à l'article 9, 2, h du RGPD ',*

- ' *l'exécution du suivi et de la surveillance post-autorisation des vaccins conformément aux bonnes pratiques recommandées par l'Organisation mondiale de la Santé* ',

- ' *l'exécution d'études scientifiques ou statistiques* ',

- ainsi que la nouvelle finalité apparue dans le projet d'accord de coopération ' *l'information et la sensibilisation des utilisateurs de soins concernant la vaccination contre la COVID-19 par les prestataires de soins '.*

34. Conformément à la remarque de l'Autorité dans son avis n° 138/2020 (point 34), les finalités ' *la pharmacovigilance des vaccins contre la COVID-19* ' et ' la traçabilité des vaccins contre la COVID-19 ' sont complétées par la réglementation en vigueur en la matière. L'Autorité en prend acte.

35. En vertu de l'article 4, § 2, 4° et 5° du projet d'accord de coopération, les données enregistrées dans Vaccinnet (dont une proportion importante de données de santé sensibles) doivent également permettre de planifier des plages de vaccination ainsi que l'organisation logistique de la vaccination contre la COVID-19. L'Autorité ne peut toutefois pas se défaire de l'impression que la ' base de données des codes de vaccination ' (qui ne contiendra pratiquement aucune donnée de santé sensible (hormis l'état de vaccination)) créée par le projet d'accord de coopération avait précisément pour finalité de couvrir le volet organisationnel et logistique de planification de plages de vaccination et d'invitation à des plages de vaccination (comme il ressort d'ailleurs de l'article 4, § 1er, 1° et 2° du projet d'accord de coopération). Qu'en est-il ? La double mention (article 4, § 1er, 1° et § 2, 4°) d'une finalité (quasi textuellement) identique (gestion des schémas de vaccination et planification des plages de vaccination) résulte peut-être d'une erreur ?

36. Dans l'avis n° 138/2020, l'Autorité constatait (au point 35) que ' la détermination du taux de vaccination contre la COVID-19 ' semblait être une finalité statistique qui pouvait être réalisée à l'aide de données anonymes (ou au moins de données à caractère personnel pseudonymisées si une anonymisation ne permettait pas de déterminer le taux de vaccination). L'Autorité recommandait dès lors au demandeur de l'ajouter explicitement dans le projet. L'Autorité constate à cet égard que le mot ' anonyme ' a uniquement été ajouté dans l'Exposé des motifs; elle insiste néanmoins (par analogie avec d'autres finalités qui peuvent être réalisées à l'aide de données anonymes/à tout le moins pseudonymisées) pour que ce terme soit repris dans le texte proprement dit du projet d'accord de coopération.

37. Suite à la demande en ce sens de l'Autorité dans l'avis n° 138/2020 (point 36), l'article 4, § 2, 7° du projet d'accord de coopération complète la finalité de ' l'organisation du suivi des contacts ' par un renvoi explicite à ' en exécution de l'Accord de coopération du 25 août 2020 (…) '.

Dans l'Exposé des motifs, l'importance du rapport avec le suivi des contacts est expliquée à l'aide des scénarios suivants :

- *' l'avis qui doit être formulé par le centre de contact peut varier en fonction du fait qu'une personne a ou non été vaccinée;*

- *la source est vaccinée mais a infecté plusieurs contacts; il s'agit d'un cas d'échec du vaccin ou d'un variant de la souche contre lequel le vaccin n'offre pas de protection et donc d'informations très importantes pour la santé publique;*

- *la source n'est pas vaccinée, ce qui a causé l'infection d'autres personnes;*

- *les contacts sont susceptibles d'être vaccinés, ce qui permet à l'épidémie de s'éteindre;*

- *les contacts ne sont pas vaccinés, il y a donc lieu de continuer à cartographier activement l'épidémie '.*

38. L'Autorité prend acte de cette explication et comprend la plus-value des informations relatives à l'état de vaccination pour le suivi des contacts. Elle estime néanmoins indiqué de préciser dans le projet d'accord de coopération quelles données seront par conséquent exportées depuis Vaccinnet vers la (les) Base(s) de données de Sciensano, et au moins d'apporter les modifications nécessaires aux dispositions de l'Accord de coopération du 25 août 2020 où sont décrites les catégories de données de la (des) Base(s) de données qui y est (sont) encadrée(s) et leurs sources. Une éventuelle délibération du Comité de sécurité de l'information concernant un tel flux de données doit en effet correspondre à ce que prescrit sur ce plan la réglementation en la matière, notamment le présent projet d'accord de coopération et davantage encore, l'Accord de coopération du 25 août 2020.

39. L'article 4, § 2, 10° du projet d'accord de coopération mentionne que des études scientifiques ou statistiques seront réalisées ' *conformément 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* '. L'Autorité fait observer que le titre 4 de la LTD exécute l'article 89, §§ 2 et 3 du RGPD et définit par conséquent le régime d'exception pour des recherches qui ne peuvent être réalisées qu'avec des limitations / dérogations aux droits des personnes concernées, tels que mentionnés aux articles 15 et suivants du RGPD. Qu'en est-il ?

40. À l'article 4, § 2, 11° du projet d'accord de coopération apparaît pour la première fois une nouvelle finalité à atteindre – grâce à l'enregistrement des vaccinations dans Vaccinnet -, à savoir *' l'information et la sensibilisation des utilisateurs de soins concernant la vaccination contre la COVID-19 par les prestataires de soins* '. L'Autorité ne voit pas du tout clairement dans quelle mesure la réalisation d'une finalité telle que ' l'information et la sensibilisation à la vaccination contre la COVID-19 ' nécessite des données à caractère personnel. Si le but est une information et une sensibilisation ' personnalisées ' des citoyens qui refusent un vaccin, cela devrait être clairement énoncé dans le projet d'accord de coopération, afin que les parlements concernés puissent l'accepter ou non en connaissance de cause. L'Autorité considère que des campagnes de sensibilisation (de certains groupes cibles) à grande échelle peuvent parfaitement s'effectuer au moyen de données anonymes ».

B.20.4. Le ministre de la Santé publique a précisé que « l'accord de coopération ne concerne que la campagne de vaccination contre le COVID-19 et que les données ne peuvent pas être utilisées pour d'autres finalités », que celles qui « concernent exclusivement la campagne de vaccination » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/002, p. 12).

B.21.1. En vertu du principe de la minimisation des données, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (article 5, paragraphe 1, point c), du RGPD).

B.21.2. Comme il est dit en B.16.4, le droit au respect de la vie privée englobe la protection des données à caractère personnel et des informations personnelles dont relèvent, notamment, le nom et les données de santé.

Les actes attaqués, qui portent assentiment à des dispositions qui prévoient le traitement des données à caractère personnel, y compris des données sensibles sur la santé, dans la banque de données « Vaccinnet », entraînent une ingérence dans le droit à la protection des données à caractère personnel, garanti par les dispositions citées en B.16.

L'article 4, paragraphe 15, du RGPD définit les « données concernant la santé », comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ». Dès lors que les données enregistrées dans la banque de données « Vaccinnet » portent notamment sur des données concernant la santé au sens de la disposition précitée, elles doivent être traitées conformément à l'article 9 du RGPD.

L'article 9, paragraphe 1, du RGPD interdit en principe le traitement de données à caractère personnel sensibles, telles les données concernant la santé. L'article 9, paragraphe 2, point h), du RGPD permet toutefois un tel traitement lorsqu'il 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 » et

qu'il est soumis à une obligation de secret professionnel. L'article 9, paragraphe 2, point i), du RGPD prévoit que le traitement de telles données est également autorisé lorsqu'il 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 ».

Le considérant 54 du RGPD énonce à cet égard :

« Le 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) nº 1338/2008 du Parlement européen et du Conseil, 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 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 ».

B.21.3. En vertu du principe de la limitation des finalités, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et le traitement ultérieur éventuel de ces données doit être compatible avec ces finalités initiales (article 5, paragraphe 1, point b), du RGPD).

Comme il est dit en B.16.9 et B.16.10, en vertu du principe de légalité, toute personne doit avoir une idée suffisamment claire des finalités du traitement des données qui la concernent.

B.22.1. Les actes attaqués poursuivent un objectif légitime de lutte contre la propagation du coronavirus SARS-CoV-2, qui est un virus aéroporté très contagieux. La pandémie de

COVID-19 se caractérise par un taux de reproduction élevé. Si des mesures sanitaires ne sont pas prises, ce virus se propage très rapidement, de manière exponentielle.

Comme il est dit en B.2, l'enregistrement des données de vaccination s'inscrit, d'une part, dans la stratégie de vaccination belge établie sur la base des données scientifiques en matière de vaccins contre la COVID-19, telles qu'elles étaient disponibles au moment de l'adoption des actes attaqués, afin de lutter contre la pandémie de COVID-19 en diminuant les contaminations liées au coronavirus COVID-19, ainsi que, d'autre part, dans la mise en œuvre au niveau européen d'un certificat COVID numérique de l'UE, basé sur le souci d'interopérabilité, entre autres, des certificats de vaccination.

Dans ce contexte, l'enregistrement des données de vaccination est indispensable à la poursuite de ces objectifs, et la centralisation de l'enregistrement de ces données permet d'« identifier le schéma posologique adéquat, notamment en ce qui concerne les différentes doses d'un vaccin à administrer (intervalle optimal proposé en cas de vaccins multi-doses) et vise à assurer le bon fonctionnement de la campagne [de] vaccination massive contre la COVID-19 » (*Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, p. 3).

Une telle mesure vise dès lors à garantir la santé d'autrui et la santé publique, ainsi que les droits et libertés d'autrui.

B.22.2. L'accord de coopération du 12 mars 2021 identifie expressément, dans ce contexte, onze finalités pour lesquelles les données à caractère personnel mentionnées dans l'article 3, § 2, sont collectées et traitées dans la banque de données « Vaccinnet », et l'exposé général de l'accord de coopération du 12 mars 2021 précise expressément que ces données « ne peuvent être utilisées à d'autres fins que celles prévues dans le présent accord », « notamment mais pas exclusivement à des fins policières, commerciales, fiscales, pénales ou de sécurité de l'Etat » (*Moniteur belge* du 12 avril 2021, p. 32407).

En adoptant les actes attaqués, les différents législateurs compétents ont réglé eux-mêmes les éléments essentiels du traitement des données à caractère personnel, conformément à ce qui est dit en B.16.9 et B.16.10, en définissant de manière exhaustive les finalités du traitement des données figurant dans la banque de données « Vaccinnet ».

Par ailleurs, l'exposé général de l'accord de coopération du 12 mars 2021 apporte de nombreuses précisions quant aux finalités, répondant ainsi aux critiques formulées par l'Autorité de protection des données dans son avis cité en B.20.3.

B.23.1. Pour examiner le caractère déterminé des finalités visées à l'article 4, § 2, de l'accord de coopération, la Cour doit, dans le contexte rappelé en B.2, prendre en compte le caractère intrinsèquement évolutif des connaissances scientifiques relatives aux spécificités du coronavirus SARS-CoV-2 et de ses possibles mutations, mais aussi à l'efficacité des vaccins mis sur le marché peu de temps avant le lancement de la campagne de vaccination et leur efficacité à moyen et long terme.

B.23.2.1. Il ressort des travaux préparatoires cités en B.20 que les onze finalités définies dans l'article 4, § 2, sont directement liées à la campagne de vaccination massive, déployée au niveau national, menée sur la base des connaissances scientifiques disponibles au moment du lancement de cette campagne.

Le seul fait que les finalités d'un traitement de données soient au nombre de onze ne permet pas, comme le soutient la partie requérante, de conclure que ces finalités seraient, en soi, excessives. En effet, le caractère déterminé d'une finalité doit s'apprécier en fonction des circonstances d'espèce et l'explicitation des différentes finalités peut constituer une garantie pour le traitement des données (opinion 03/2013 sur la limitation des finalités, 2 avril 2013, Groupe de travail « Article 29 » sur la protection des données, p. 15).

B.23.2.2. Ainsi, les finalités de « pharmacovigilance des vaccins contre la COVID-19 » (2°), de « traçabilité des vaccins » (3°), de « gestion des schémas de vaccinations » (4°), d'« organisation logistique de la vaccination contre la COVID-19 » (5°), de « détermination du taux de vaccination anonyme contre la COVID-19 de la population » (6°) et d'« exécution du suivi et de la surveillance post-autorisation des vaccins » (8°) sont précises et directement liées à l'organisation de la campagne de vaccination massive contre la COVID-19, menée au niveau national.

Ces différents éléments sont en effet nécessaires pour mettre en œuvre l'organisation logistique de la vaccination, compte tenu des différents groupes cibles à inviter et du nombre de doses à administrer, mais aussi pour évaluer le taux de couverture vaccinale, la capacité du vaccin à induire une réponse immunitaire et pour détecter les éventuels effets indésirables de ce vaccin. Le suivi et la surveillance post-autorisation des vaccins sont organisés conformément aux bonnes pratiques de l'Organisation mondiale de la santé en la matière. Dans le cadre de la finalité de « pharmacovigilance des vaccins », l'article 45 de la loi du 13 juin 2021 « portant des mesures de gestion de la pandémie COVID-19 et d'autres mesures urgentes dans le domaine des soins de santé » prévoit l'intégration de données figurant dans « Vaccinnet » dans une base de données fédérale, dont le responsable du traitement est l'Agence fédérale des médicaments et des produits de santé.

Contrairement à ce que la partie requérante allègue, la finalité relative à la « prestation de soins de santé et de traitements » a été expressément limitée dans l'article 4, § 2, 1°, de l'accord de coopération du 12 mars 2021 comme visant « exclusivement l'acte de vaccination et les mesures de soutien, d'information, de sensibilisation des citoyens en rapport avec la vaccination », en référence à l'article 9, paragraphe 2, point h), du RGPD. Il a également été précisé que cette finalité ne porte aucunement sur « le fait de limiter ou de conditionner l'accès à des soins de qualité de quelque manière que ce soit en raison de l'état vaccinal d'une personne » (exposé général de l'accord de coopération du 12 mars 2021, *Moniteur belge* du 12 avril 2021, p. 32407). Il en résulte que cette finalité est également précise et directement liée à la vaccination contre la COVID-19 et au suivi médical de la personne vaccinée.

La finalité visée à l'article 4, § 2, 1°, est ainsi également liée à la finalité d'« exécution d'études scientifiques ou statistiques » visée à l'article 4, § 2, 10°, ainsi qu'à la finalité relative à « l'information et la sensibilisation des personnes concernant la vaccination contre la COVID-19 » visée à l'article 4, § 2, 11°. Il ressort en effet des principes décidés en matière de stratégie de vaccination que la Belgique tend à atteindre une forme d'immunité collective par un taux de vaccination suffisant de 70 % de la population. Le traitement des données à des fins de recherche scientifique et statistique est notamment visé par l'article 89, paragraphe 1, du

RGPD, qui prévoit le principe de minimisation des données, notamment la pseudonymisation qui est, à tout le moins prévue dans l'article 4, § 2, 10°, dans l'hypothèse où l'anonymisation ne permettrait pas de réaliser l'étude scientifique ou statistique. Il a été souligné à cet égard qu'une « couverture vaccinale importante au sein de la population constitue un enjeu majeur et fondamental de santé publique au regard de la crise pandémique inédite de la COVID-19 ainsi qu'à l'échelle de l'individu qui doit pouvoir réaliser un choix pour sa santé personnelle de manière informée » (exposé général de l'accord de coopération du 12 mars 2021, *Moniteur belge* du 12 avril 2021, p. 32407), de sorte que des études statistiques sur cette couverture vaccinale sont nécessaires. Des études sur la couverture vaccinale permettent d'estimer le pourcentage de personnes vaccinées dans les groupes à risques spécifiques et aident à estimer d'éventuelles lacunes du programme de vaccination qui devraient être comblées, le cas échéant par une information et une sensibilisation ciblées, au moyen de campagnes générales ou au niveau individuel, en fonction des attitudes constatées au sein de la population. Le fait que la vaccination s'opère sur une base volontaire rend, dans ce contexte, la finalité d'information et de sensibilisation nécessaire, au regard de l'objectif d'atteindre une couverture vaccinale suffisante. Sur la base de ces connaissances, le rôle du médecin dans cette information ciblée peut se révéler important, même s'il est interdit de contacter des personnes qui ont explicitement déclaré qu'elles refusent le vaccin (*ibid.*).

B.23.2.3. La finalité relative au « traçage des contacts » (7°) est liée au fait que, dans le but exclusif du suivi des contacts infectieux, le statut vaccinal influence directement le risque de contamination. Les données transmises dans ce cadre de « Vaccinnet » vers la banque de données de Sciensano sont limitées, mais « une flexibilité s'impose en fonction de l'évolution des connaissances scientifiques en ce qui concerne l'impact de la vaccination sur les risques d'infection » (*ibid.*, p. 32406).

B.23.2.4. La finalité relative au « calcul de la répartition du coût de vaccination » (9°) entre l'autorité fédérale et les entités fédérées est liée au fait que la campagne de vaccination, gratuite, a été organisée par le biais d'un accord de coopération entre les autorités compétentes, et que les parties à cet accord doivent financer cette vaccination.

Le fait que, comme le souligne la section de législation du Conseil d'État, il est possible que les données ne soient pas anonymisées mais seulement pseudonymisées peut se justifier,

comme l'indique l'exposé général de l'accord de coopération à l'égard du degré de vaccination anonyme contre la COVID-19 par le fait que l'anonymisation est susceptible de ne pas permettre d'atteindre l'objectif poursuivi (*ibid.*, p. 32407), mais l'article 4, § 2, 8° garantit que les données concernées seront, à tout le moins, pseudonymisées. Sur la base de cette finalité, le protocole d'accord du 9 février 2022 conclu entre le Gouvernement fédéral et les autorités visées aux articles 128, 130 et 135 de la Constitution « concernant le cofinancement du programme de vaccination contre la COVID-19 » a réparti le coût de la vaccination contre la COVID-19 entre les différentes autorités.

Quant à l'anonymisation ou à la pseudonymisation, il convient de constater qu'il s'agit là de mesures techniques et organisationnelles à adopter pour protéger le traitement des données à caractère personnel, mais qui garantissent toutes deux que l'identité de la personne concernée ne sera pas révélée. Certains éléments peuvent en effet devoir être déterminés de manière « granulaire » : l'exposé général de l'accord de coopération du 12 mars 2021 évoque à cet égard l'exemple des centres de soins résidentiels, dans lesquels une distinction doit être opérée entre le personnel soignant et les résidents (*ibid.*, p. 32407). L'évolution des circonstances et de la réalité épidémiologique peut en effet exiger que la situation soit réglée par une mesure plutôt que par l'autre, sans que la possibilité de recourir à une des deux mesures puisse être considérée comme une absence de détermination quant à un élément essentiel des finalités du traitement des données.

B.23.3. Il résulte de ce qui précède que les finalités définies dans l'article 4, § 2, de l'accord de coopération ont un lien direct avec la campagne de vaccination massive menée au niveau national, sont suffisamment précises et déterminées et sont limitées au strict nécessaire en ce qui concerne cette vaccination.

B.24. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment à l'article 4, § 2, de l'accord de coopération, le moyen unique, dans sa première branche, n'est pas fondé.

II. En ce qui concerne l'habilitation, visée à l'article 5, conférée au Comité de sécurité de l'information d'autoriser la communication de données à caractère personnel à des tiers (première branche)

B.25.1. Dans la première branche du moyen, la partie requérante estime que les catégories de destinataires des données à caractère personnel fixées dans l'article 5 de l'accord de coopération du 12 mars 2021 ne présentent pas de garanties suffisantes de prévisibilité. En outre, l'article 5, alinéa 3, de l'accord de coopération du 12 mars 2021 délègue au Comité de sécurité de l'information la compétence de déterminer des éléments essentiels que sont les instances tierces pouvant traiter les données collectées et ainsi que les finalités du traitement de ces données.

B.25.2. Comme il est dit en B.10.1, les griefs de la partie requérante ne concernent que la banque de données « Vaccinnet », de sorte que la Cour n'examine le moyen dirigé contre l'article 5 de l'accord de coopération du 12 mars 2021 qu'en ce qu'il concerne la communication des données visées à l'article 3, § 2, de l'accord de coopération précité, enregistrées dans la banque de données « Vaccinnet ».

B.26.1. L'article 5 de l'accord de coopération du 12 mars 2021 dispose :

« Dans le but exclusif d'atteindre les finalités listées à l'article 4, les données à caractère personnel visées à l'article 3 peuvent être communiquées à des personnes ou des instances chargées d'une mission d'intérêt public par ou en vertu d'une loi, d'un décret ou d'une ordonnance, à condition que cette communication soit nécessaire à l'exécution de la mission d'intérêt public des personnes ou des instances en question et que seules les données pertinentes au vu des finalités de l'article 4 soient communiquées.

Les données à caractère personnel visées à l'article 3 sont communiquées à des institutions de recherche si elles sont nécessaires pour la réalisation d'études scientifiques ou statistiques, après anonymisation ou à tout le moins pseudonymisation lorsque l'anonymisation ne permettrait pas de réaliser l'étude scientifique ou statistique.

Toute communication des données fait l'objet d'une délibération de la chambre ' sécurité sociale et santé ' du comité de sécurité de l'information, afin de vérifier le respect des conditions énoncées au présent article.

Le Comité de sécurité de l'information publie sur le portail eSanté une description fonctionnelle précise des systèmes d'information mis en place pour la mise en œuvre du présent accord de coopération et des flux d'informations entre ces systèmes d'information qui ont fait

l'objet d'une délibération du Comité de sécurité de l'information, en particulier en ce qui concerne le traitement des informations, les processus et les banques de données.

Les délibérations du Comité de sécurité de l'information sont systématiquement publiées sur le site web de la Plate-forme eHealth ».

B.26.2. Concernant la communication des données à des tiers, visée à l'article 5, l'exposé général de l'accord de coopération du 12 mars 2021 indique :

« Dans le but exclusif d'atteindre les finalités listées à l'article 4, les données à caractère personnel visées à l'article 3 peuvent être communiquées à des personnes ou des instances chargées d'une mission d'intérêt public par ou en vertu d'une loi, d'un décret ou d'une ordonnance, à condition que cette communication soit nécessaire à l'exécution de la mission d'intérêt public des personnes ou des instances en question et que seules les données pertinentes au vu des finalités de l'article 4 soient communiquées.

Les données à caractère personnel visées à l'article 3 sont communiquées après anonymisation ou, à tout le moins pseudonymisation, à des institutions de recherche si elles sont nécessaires pour la réalisation d'études scientifiques ou statistiques.(terminologie de l'article 89 du Règlement général sur la protection des données).

Toute communication des données fait l'objet d'une délibération de la chambre ' sécurité sociale et santé ' du comité de sécurité de l'information, afin de vérifier le respect des conditions énoncées au présent article.

Le Comité de sécurité de l'information peut uniquement délibérer pour des échanges de données concrets dans le cadre du présent accord de coopération et ne peut donc, en aucun cas, déterminer d'autres finalités de traitement, ni catégories de données à caractère personnel. Il n'est en aucun cas compétent pour déterminer un élément essentiel du traitement de données à caractère personnel, conformément au principe de légalité tel que prévu à l'article 22 de la Constitution. Il n'est donc pas chargé d'une telle mission sur base du présent accord de coopération.

Le Comité de sécurité de l'information publie sur le portail eSanté une description fonctionnelle précise des systèmes d'information mis en place pour la mise en œuvre du présent accord et des flux d'informations entre ces systèmes d'information qui ont fait l'objet d'une délibération du Comité de sécurité de l'information, en particulier concernant les traitements des informations, les processus et les banques de données.

En outre, les délibérations du Comité de sécurité de l'information sont systématiquement publiées sur le site web de la Plate-forme eHealth. Les délibérations du Comité de sécurité de l'information comprennent toujours les différents aspects nécessaires à l'évaluation du respect de la réglementation relative à la protection de la vie privée lors du traitement de données à caractère personnel (en particulier le Règlement général sur la protection des données). Ainsi, les parties concernées (responsables du traitement) sont toujours explicitement mentionnées, ainsi que les finalités visées et un aperçu (généralement exhaustif) des données à caractère personnel à traiter pour ces finalités. Le Comité de sécurité de l'information vérifie notamment

si le traitement de données à caractère personnel est légitime (et répond dès lors à une des conditions mentionnées à l'article 6 du RGPD) et si les principes de base sont respectés (limitation de la finalité, minimisation des données, limitation de la conservation et sécurité de l'information).

L'utilisation d'une base de données commune n'exclut pas que différentes interfaces utilisateur final, éventuellement spécifiques à une entité fédérée, soient utilisées pour alimenter ou consulter la base de données commune.

Il est fondamental de préciser que les données collectées sur base du présent accord de coopération ne peuvent être communiquées que dans deux cas de figure énoncés de manière strictement limitative :

- soit le tiers est, de manière cumulative, chargé d'une mission d'intérêt public et est habilité à traiter de telles données par ou en vertu d'une loi, d'un décret ou d'une ordonnance qui vise expressément une finalité prévue par le présent accord;

- soit le tiers est une institution de recherche pour la réalisation d'études scientifiques ou statistiques. Dans ce cas, sont uniquement communiquées les données anonymisées ou pseudonymisées lorsque l'anonymisation ne permet pas de rencontrer le but poursuivi.

Par tiers il y a lieu d'entendre notamment les prestataires de soins qui ont une relation thérapeutique avec l'utilisateur de soins et les organismes assureurs, dans les limites évidemment de leurs missions respectives.

S'il n'est pas possible ni pertinent de désigner nommément qui sont ces tiers dans un accord de coopération, ces critères permettent néanmoins d'encadrer et de limiter de manière stricte les catégories de tiers concernés. En outre, le rôle du Comité de sécurité de l'information vise à intégrer un filtre supplémentaire afin d'assurer que le flux de données s'inscrit bien dans l'objectif poursuivi et dans la volonté de limiter au maximum la communication de telles données. Ce faisant, il permet d'offrir une flexibilité nécessaire (en ne figeant pas des flux de données évolutives par exemple) et ne peut que renforcer les garanties offertes en matière de vie privée par un contrôle factuel. En effet, il permet d'éviter qu'un flux automatique soit généré sans que ne soit vérifié au préalable qu'il est effectivement permis. Comme le souligne l'Autorité de protection des données dans son avis 16-2021 du 18 février 2021, une délibération du Comité de sécurité de l'information permet également d'apporter une plus-value en précisant davantage les modalités d'exécution, notamment au niveau de la sécurité de l'information et la proportionnalité envisagée par la loi.

En réponse à l'avis du Conseil d'Etat 68/844/VR du 18 février 2021, et au regard de ce qui précède, il convient de préciser que la soumission de la communication de données à caractère personnel à une délibération du Comité de sécurité de l'information est une règle établie par la loi fédérale et constitue une mesure de protection des données dès la conception et par défaut au sens du Règlement Général sur la Protection des Données. Elle est basée sur les articles 6, § 2, et 9, § 4 du Règlement Général sur la Protection des Données.

En effet, les délibérations du Comité de sécurité de l'information précisent les mesures de sécurité de l'information que doivent respecter les acteurs d'une communication de données et

évaluent de manière préventive s'il n'y a pas plus de données à caractère personnel qui sont communiquées à l'organisme acquéreur que celles qui lui sont strictement nécessaires pour atteindre des finalités de traitement légitimes.

Les délibérations du Comité de sécurité de l'information sont contraignantes pour les acteurs de l'échange de données. D'autre part, elles visent à offrir une sécurité juridique aux acteurs de l'échange de données afin qu'un partage efficace et efficient des données ne soit pas inutilement hypothéqué par un manque de clarté concernant les mesures de sécurité de l'information à implémenter ou concernant la légitimité de la communication des données à caractère personnel.

Les délibérations du Comité de sécurité de l'information ne portent que sur l'échange (électronique) de données. Dans ses délibérations, le Comité de sécurité de l'information est lié par les dispositions légales régissant les finalités du traitement par les autorités qui reçoivent les données. Les délibérations du Comité de sécurité de l'information ne constituent qu'une base juridique permettant à un organisme traitant des données à caractère personnel sur la base de finalités légitimes de communiquer ces données à caractère personnel à d'autres organismes, dans le cadre des finalités légitimes pour lesquelles l'organisme destinataire peut lui-même traiter ces données à caractère personnel.

Les délibérations du Comité de sécurité de l'information ne constituent pas une base juridique pour la première collecte et le premier traitement de données à caractère personnel par l'organisme émetteur. L'organisme destinataire doit, également, traiter les données à caractère personnel en vertu des bases juridiques dont il dispose. Par conséquent, le Comité de sécurité de l'information ne peut pas étendre les finalités du traitement initial par l'instance qui fournit les données, ni offrir une base juridique pour des finalités de traitement par l'instance destinatrice autres que celles qui sont prévues par ou en vertu d'une loi. Les délibérations autorisent l'échange de données moyennant le respect des modalités décrites dans la délibération sur le plan de la sécurité de l'information et le respect du principe de proportionnalité, mais ne l'imposent pas.

Le Comité de sécurité de l'information n'est pas une autorité de contrôle au sens du Règlement Général sur la Protection des Données. Il n'est donc pas compétent pour contrôler le respect des règles, pour résoudre des problèmes et des litiges ou pour traiter des plaintes. En effet, c'est l'Autorité de protection des données qui est compétente pour ces questions. L'Autorité de protection des données peut à tout moment comparer toute délibération du Comité de sécurité de l'information avec des normes juridiques supérieures et, en cas de non-conformité, demander au Comité de sécurité de l'information de reconsidérer sa délibération sur les points qu'elle a soulevés.

Ce recours au Comité de sécurité de l'information ne se conçoit donc dès lors pas pour les parties prenantes au présent accord de coopération comme un abandon de compétence de par le fait d'une application des règles » (*Moniteur belge* du 12 avril 2021, pp. 32408-32411; voy. aussi *Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, pp. 13-16).

B.27.1. Dans son avis sur l'avant-projet de loi devenue la loi du 2 avril 2021 portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé :

« S'agissant de la communication de données à caractère personnel issues des bases de données à des tiers, l'article 5, alinéa 1er, de l'accord de coopération subordonne à l'autorisation préalable du Comité de sécurité de l'information toute communication de données à caractère personnel à ' des instances ayant une mission d'intérêt public pour les finalités dont sont chargées ces instances par ou en vertu d'une loi, d'un décret ou d'une ordonnance et pour la communication de ces données après anonymisation ou, à tout le moins, pseudonymisation, à des institutions de recherche pour la réalisation d'études scientifiques ou statistiques '.

Vu le caractère sensible des données à caractère personnel contenues dans les bases de données, les termes décrivant pareillement les tiers auxquels il pourrait être donné accès aux données apparaissent trop larges. L'accord de coopération sera davantage précisé sur ce point » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 45; voy. aussi *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, p. 81).

Pour autant qu'il entre dans l'intention des auteurs de l'accord de coopération de maintenir un pouvoir réglementaire au profit de la chambre « sécurité sociale et santé » du Comité de sécurité de l'information, la section de législation du Conseil d'État renvoie à l'observation formulée par l'avis 67.719 du 15 juillet 2020 sur un avant-projet devenu la loi du 9 octobre 2020 « portant assentiment à l'accord de coopération du 25 août 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspection d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 se fondant sur une base de données auprès de Sciensano », au sujet des compétences (réglementaires) qui avaient été déléguées à la chambre « sécurité sociale et santé » du Comité de sécurité de l'information :

« 27. Les articles 11, § 3, et 12, § 1er, de l'accord de coopération prévoient une délégation de pouvoir réglementaire à la chambre ' Sécurité sociale et Santé ' du Comité de sécurité de l'information, en ce qui concerne certains aspects de la réglementation du traitement des données à caractère personnel.

L'attribution d'un pouvoir réglementaire à un organisme public, comme le comité de sécurité de l'information, n'est en principe pas conforme aux principes généraux de droit public en ce qu'il est ainsi porté atteinte au principe de l'unité du pouvoir réglementaire et qu'un contrôle parlementaire direct fait défaut. En outre, les garanties dont est assortie la réglementation classique, telles que celles en matière de publication, de contrôle préventif exercé par le Conseil d'État, section de législation, et de rang précis dans la hiérarchie des normes, sont absentes. Pareilles délégations ne se justifient dès lors que dans la mesure où elles sont très limitées et ont un caractère non politique, en raison de leur portée secondaire ou

principalement technique. Les organismes qui doivent appliquer la réglementation concernée doivent être soumis à cet égard tant à un contrôle juridictionnel qu'à un contrôle politique.

Par ailleurs, le Comité de sécurité de l'information est un organisme fédéral et une délégation de pouvoir réglementaire à un tel organisme s'analyse comme un abandon de compétences de la part des entités fédérées qui sont parties à l'accord de coopération.

En conclusion, les délégations visées accordées au Comité de sécurité de l'information doivent être transformées en délégations à un accord de coopération d'exécution, à l'instar de l'article 14, § 9, de l'accord de coopération, pour autant du moins qu'il ne règle aucun nouvel élément essentiel du traitement des données à caractère personnel, mais concrétise tout au plus ce qui découle déjà de l'actuel accord de coopération. Si cela ne s'avère pas possible, cet accord de coopération sera d'abord complété » (*ibid.*, pp. 52-54; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, pp. 88-89; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, p. 85; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 32-33; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 17-18; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, p. 33).

B.27.2. Dans son avis n° 16/2021 du 10 février 2021 sur l'avant-projet d'accord de coopération devenu l'accord de coopération du 12 mars 2021, l'Autorité de protection des données a observé :

« 43. L'Autorité prend certes acte du fait que l'article 5 du projet d'accord de coopération renvoie expressément à son article 4, § 3 (' *Les données collectées dans le cadre du présent accord de coopération ne peuvent être utilisées à d'autres fins que celles prévues dans le présent accord.* ').

Étant donné que l'Autorité avait déjà constaté dans son avis n° 138/2020 et constate à nouveau dans le présent avis que certaines des finalités mentionnées dans le projet d'accord de coopération sont formulées de manière excessivement large – et de ce fait ne répondent pas à l'exigence qui s'applique en la matière d'être déterminées et explicites (voir l'article 5.1.b) du RGPD) -, le renvoi dans l'article 5 du projet d'accord de coopération à l'article 4, § 3 n'offre pas de garanties suffisantes aux personnes concernées sur le plan de la prévisibilité.

Comme déjà indiqué au point 10 du présent avis, le principe de légalité requiert que toute ingérence dans le droit au respect de la protection des données à caractère personnel soit encadrée par une norme qui soit non seulement nécessaire et proportionnée à l'objectif qu'elle poursuit mais qui soit aussi suffisamment claire et précise et dont l'application est prévisible pour les personnes concernées. Un manque de prévisibilité affecte donc inévitablement aussi la légalité de la norme.

[…]

45. Dans la mesure où le projet d'accord de coopération prévoit un énoncé plus clair des catégories de destinataires visées ainsi qu'une délimitation plus claire des finalités (à quelles

fins ces tiers peuvent-ils utiliser les données en question), une délibération du Comité de sécurité de l'information peut évidemment apporter une plus-value en précisant davantage les modalités d'exécution, notamment au niveau de la sécurité de l'information.

L'Autorité insiste à cet égard pour que – outre la description fonctionnelle des systèmes d'information et des flux d'informations qui ont fait l'objet d'une délibération (voir l'article 5, dernier alinéa du projet d'accord de coopération) – les délibérations proprement dites du Comité de sécurité de l'information soient aussi publiées immédiatement et intégralement et qu'elles puissent être consultées pendant une longue période ».

B.27.3. Le ministre de la Santé publique a précisé à ce sujet que « la tâche du comité de sécurité de l'information est strictement délimitée. Il ne pourra délibérer que sur les communications de données ayant lieu dans le cadre de cet accord de coopération. Ce comité ne pourra en aucun cas définir lui-même d'autres finalités ou d'autres catégories de données personnelles » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/002, p. 13).

La ministre wallonne de la Santé a aussi précisé que « seuls les tiers qui sont chargés d'une mission publique et qui sont légalement habilités à traiter les données à caractère personnel peuvent recevoir les données » (*Doc. parl.,* Parlement wallon, C.R.I., n° 25, 2020-2021, 31 mars 2021, p. 73).

B.28. En ce qui concerne les données à caractère personnel figurant dans la banque de données « Vaccinnet », l'article 5 de l'accord de coopération définit deux catégories de tiers auxquels ces données peuvent être communiquées : d'une part, « des personnes ou des instances chargées d'une mission d'intérêt public par ou en vertu d'une loi, d'un décret ou d'une ordonnance », auxquelles peuvent être communiquées, parmi les données visées à l'article 3, § 2, seules les données pertinentes au regard des finalités de l'article 4, § 2, et uniquement si cette communication est nécessaire à l'exécution de la mission d'intérêt public de ces personnes ou instances; d'autre part, des « institutions de recherche » si les données sont nécessaires pour réaliser des études scientifiques ou statistiques, après anonymisation ou, à tout le moins, pseudonymisation lorsque l'anonymisation ne permettrait pas de réaliser l'étude scientifique ou statistique.

L’article 5, alinéa 3, subordonne cependant la communication de ces données à caractère personnel à une délibération de la « chambre sécurité sociale et santé » du Comité de sécurité de l’information, aux fins de vérifier le respect des conditions énoncées dans cet article.

B.29.1. Comme il est dit en B.16.9 et B.16.10, en réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée et familiale, l’article 22 de la Constitution garantit à tout citoyen qu’aucune ingérence dans ce droit ne pourra avoir lieu qu’en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

Une délégation à un autre pouvoir n’est pas contraire au principe de légalité, pour autant que l’habilitation soit définie de manière suffisamment précise et porte sur l’exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.

B.29.2. L’article 6, paragraphe 2, du RGPD dispose que les États membres peuvent maintenir ou introduire des « dispositions plus spécifiques » pour adapter l’application des règles du RGPD en ce qui concerne le traitement nécessaire au respect d’une obligation légale à laquelle le responsable du traitement est soumis (article 6, paragraphe 1, point c)) et le traitement 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 (article 6, paragraphe 1, point e)). L’article 9, paragraphe 2, point h), du RGPD permet le traitement de données sensibles aux fins de la médecine préventive, entouré de différentes garanties, notamment le secret professionnel. L’article 9, paragraphe 2, point i), du RGPD prévoit que le droit de l’Union ou le droit de l’État membre en vertu duquel le traitement de données sensibles est nécessaire pour des motifs d’intérêt public dans le domaine de la santé publique prévoit des « mesures appropriées et spécifiques » pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel. L’article 9, paragraphe 4, prévoit que les États membres peuvent maintenir ou introduire des « conditions supplémentaires, y compris des limitations » en ce qui concerne notamment le traitement des données concernant la santé.

B.30.1. Le Comité de sécurité de l'information a été créé par l'article 2, § 1er, de la loi du 5 septembre 2018 « instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE » (ci-après : la loi du 5 septembre 2018). Contrairement aux comités sectoriels supprimés par la loi du 3 décembre 2017 « portant création de l'Autorité de protection des données » auxquels il succède et qui étaient intégrés au sein de l'ancienne Commission de protection de la vie privée, le Comité de sécurité de l'information a été institué comme un nouvel organe indépendant de l'Autorité de protection des données sur pied de l'article 6, paragraphe 2, et de l'article 9, paragraphe 4, précités, du RGPD (*Doc. parl*., Chambre, 2017-2018, DOC 54-3185/001, pp. 6-7 et 30; DOC 54-3185/005, pp. 7-10). Il ressort des travaux préparatoires de la loi du 5 septembre 2018 que le législateur a voulu que le Comité de sécurité de l'information ne soit considéré ni comme un responsable du traitement, ni comme une autorité de contrôle au sens du RGPD (*Doc. parl*., Chambre, 2017-2018, DOC 54-3185/001, pp. 8-10).

Conformément à l'article 2, § 2, de la loi du 5 septembre 2018, le Comité de sécurité de l'information est constitué de deux chambres : une chambre « sécurité sociale et santé » et une chambre « autorité fédérale ». Les articles 2, § 1er, et 4, § 1er, alinéa 1er, de la même loi disposent que ses membres sont nommés pour un terme de six ans renouvelable par la Chambre des représentants, qui peut aussi les décharger de leur mission. L'article 5 de la même loi dispose que les membres du Comité de sécurité de l'information « ne reçoivent d'instructions de personne ». Il ressort des travaux préparatoires que le législateur a voulu soustraire le Comité de sécurité de l'information à tout contrôle hiérarchique (*Doc. parl.,* Chambre, 2017-2018, DOC 54-3185/001, p. 10).

Le pouvoir de prendre des décisions administratives qui est confié à la chambre « sécurité sociale et santé » du Comité de sécurité de l'information par l'article 5 de l'accord de coopération du 12 mars 2021 (autoriser ou refuser la communication de données à caractère personnel) est analogue à celui qui est confié à cette chambre par l'article 15, § 1er, alinéa 1er, de la loi du 15 janvier 1990 « relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale », remplacé par l'article 18 de la loi du 5 septembre 2018, par l'article 42, § 2, 3°, de la loi du 13 décembre 2006 « portant dispositions diverses en matière de santé », tel

qu'il a été modifié par l'article 43 de la loi du 5 septembre 2018, et par l'article 11 de la loi du 21 août 2008 « relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions », tel qu'il a été modifié par l'article 50 de la loi du 5 septembre 2018. Ces dispositions habilitent la chambre « sécurité sociale et santé » du Comité de sécurité de l'information à autoriser, respectivement, (1) la communication de données sociales à caractère personnel par la Banque-carrefour de la sécurité sociale ou par une institution de sécurité sociale à destination d'une autre institution de sécurité sociale ou d'une instance autre qu'un service public fédéral, un service public de programmation ou un organisme fédéral d'intérêt public, (2) la communication de données à caractère personnel relatives à la santé et (3) la communication de données à caractère personnel par ou à destination de la plate-forme eHealth. Dans l'exercice de leur compétence d'autorisation, les chambres du Comité de sécurité de l'information se limitent à vérifier que la communication de données à caractère personnel concernée respecte les principes de limitation des finalités, de proportionnalité et de sécurité définis par le RGPD (*Doc. parl.,* Chambre, 2017-2018, DOC 54-3185/001, pp. 6, 8 et 9).

L'article 46, § 2, alinéa 1er, de la loi du 15 janvier 1990 « relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale », remplacé par l'article 39 de la loi du 5 septembre 2018, dispose que les délibérations du Comité de sécurité de l'information ont « une portée générale contraignante entre les parties et envers les tiers ». Selon les travaux préparatoires de la loi du 5 septembre 2018, ces délibérations « ont valeur normative (loi au sens matériel), conformément à l'ordre constitutionnel et peuvent être contestées par les voies de recours en vigueur si elles sont contraires aux normes juridiques supérieures » (*ibid.*, p. 8). L'alinéa 2 de la même disposition, dispose :

« L'Autorité de protection des données peut, à tout moment, confronter toute délibération du comité de sécurité de l'information aux normes juridiques supérieures, quel que soit le moment où elle a été rendue. Sans préjudice de ses autres compétences, elle peut demander au comité de sécurité de l'information, lorsqu'elle constate de manière motivée qu'une délibération n'est pas conforme à une norme juridique supérieure, de reconsidérer cette délibération sur les points qu'elle a indiqués, dans un délai de quarante-cinq jours et exclusivement pour le futur. Le cas échéant, le comité de sécurité de l'information soumet la délibération modifiée pour avis à l'Autorité de protection des données. Dans la mesure où cette dernière ne formule pas de remarques supplémentaires dans un délai de quarante-cinq jours, la délibération modifiée est censée être définitive ».

L'article 46, § 1er, 8°, de la loi du 15 janvier 1990 « relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale », remplacé par l'article 39 de la

loi du 5 septembre 2018, dispose par ailleurs que le Comité de sécurité de l'information publie chaque année sur le site internet de la Banque-carrefour et sur le site internet de la Plate-forme eHealth un rapport sommaire de l'accomplissement de ses missions au cours de l'année écoulée. Les travaux préparatoires de la loi du 5 septembre 2018 mentionnent enfin que les délibérations du Comité de sécurité de l'information peuvent faire l'objet d'un recours devant le Conseil d'État (*Doc. parl.,* Chambre, 2017-2018, DOC 54-3185/001, pp. 10 et 31).

B.30.2. Il ressort de ce qui précède que, comme la Cour l'a jugé par son arrêt n° 110/2022 du 22 septembre 2022 (ECLI:BE:GHCC:2022:ARR.110), les délibérations du Comité de sécurité de l'information ont une portée contraignante notamment pour les personnes dont le traitement des données personnelles est autorisé par ce Comité. Ces délibérations sont soumises à un contrôle faible de la part de l'Autorité de protection des données puisque celle-ci peut uniquement demander au Comité de sécurité de l'information de « reconsidérer » une décision qu'elle estimerait illégale et donner un avis sur la délibération modifiée à la suite de cette demande. Si les personnes concernées ne sont pas privées d'un recours juridictionnel contre les délibérations du Comité de sécurité de l'information, elles sont en revanche privées de la garantie de voir celles-ci soumises au contrôle parlementaire. En effet, ni la nomination et la décharge des membres du Comité de sécurité de l'information par la Chambre des représentants, ni l'obligation de publication annuelle du rapport sommaire de l'accomplissement des missions du Comité de sécurité de l'information sur le site internet de la Banque-carrefour et sur le site internet de la Plate-forme eHealth ne s'apparentent à un tel contrôle.

B.31. Comme la section de législation du Conseil d'État l'a observé dans son avis sur l'avant-projet de loi devenu la loi du 2 avril 2021, pareille délégation à un organisme tel que le Comité de sécurité de l'information « n'est en principe pas conforme aux principes généraux de droit public en ce qu'il est ainsi porté atteinte au principe de l'unité du pouvoir réglementaire et qu'un contrôle parlementaire direct fait défaut », en ce que « les garanties […] en matière de publication, de contrôle préventif exercé par le Conseil d'État, section de législation, et de rang précis dans la hiérarchie des normes » sont absentes (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 53). Pareilles délégations ne pourraient se justifier que dans la mesure où elles seraient très limitées, en raison de leur portée secondaire ou principalement technique, ce qui n'est pas le cas en l'espèce. Les dispositions, mesures et conditions que les États membres

peuvent adopter en vertu de l'article 6, paragraphe 2, de l'article 9, paragraphe 2, point i), et de l'article 9, paragraphe 4, du RGPD ne changent rien à ce constat.

En habilitant la chambre « sécurité sociale et santé » du Comité de sécurité de l'information, dont le statut n'est pas précisé par la loi ni le pouvoir d'appréciation délimité par celle-ci, à prendre des décisions en matière de traitement des données à caractère personnel qui lient les tiers, sans que de telles décisions puissent être soumises au contrôle parlementaire, l'article 5 de l'accord de coopération du 12 mars 2021 prive les personnes concernées de la garantie d'un tel contrôle, sans que cela soit justifié par une exigence découlant du droit de l'Union européenne.

B.32. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment à l'article 5 de l'accord de coopération du 12 mars 2021, le moyen unique, dans sa première branche est fondé dans la mesure où cet article concerne la communication des données visées dans l'article 3, § 2, de l'accord de coopération précité, enregistrées dans la banque de données « Vaccinnet ».

Les actes attaqués doivent être annulés dans cette mesure en ce qu'ils portent assentiment à l'article 5 de l'accord de coopération du 12 mars 2021.

III. En ce qui concerne la durée de conservation des données enregistrées dans « Vaccinnet », visée à l'article 6, § 2 (deuxième branche)

B.33. Dans la deuxième branche du moyen, la partie requérante estime que la durée de conservation des données enregistrées dans « Vaccinnet », prévue par l'article 6, § 2, de l'accord de coopération du 12 mars 2021, est disproportionnée, d'une part, en ce que le délai de 30 ans pour la conservation des données à dater de la date de vaccination contre la COVID-19 serait excessif, et, d'autre part, en l'absence d'un délai maximum de conservation des données.

B.34.1. L'article 6, § 2, de l'accord de coopération du 12 mars 2021 dispose :

« Les données visées à l'article 3, § 2, sont conservées jusqu'au décès de la personne à laquelle le vaccin contre la COVID-19 a été administré et pendant 30 ans au minimum à compter de la vaccination ».

B.34.2. Concernant la durée de conservation des données, visée à l'article 6, l'exposé général de l'accord de coopération du 12 mars 2021 indique :

« Les données relatives au code de vaccination sont conservées jusqu'à 5 jours à compter du lendemain de la publication de l'arrêté royal annonçant la fin de l'épidémie due au coronavirus COVID-19. Un suivi minutieux doit être assuré dans ce cadre aussi longtemps que dure la pandémie.

En outre, l'article 6 régit la durée de conservation des données à caractère personnel de Vaccinnet jusqu'au décès de la personne à laquelle le vaccin contre la COVID-19 a été administré et pendant 30 ans au minimum à compter de la vaccination.

Outre l'importance pour l'utilisateur de soins et les prestataires de soins d'avoir à tout moment une idée précise des vaccinations administrées, ce délai de conservation est requis pour un suivi correct des rappels nécessaires, surtout pour les vaccins pour lesquels la durée de protection n'est pas encore connue. En général, les données à caractère personnel relatives à la santé sont conservées de manière standard dans le dossier médical pendant au moins 30 ans après le dernier contact. La durée de conservation permet par ailleurs un suivi longitudinal à des fins de recherche scientifique. Enfin, ce délai de conservation est important dans le cadre des règles de responsabilité vis-à-vis des acteurs concernés, étant donné l'incertitude relative aux potentiels effets indésirables sur le long terme.

L'intention est qu'un vaccin fonctionne à vie. C'est pourquoi de nombreux vaccins sont administrés à un jeune âge et aucun nouveau vaccin de rappel n'est nécessaire par la suite pour diverses maladies contre lesquelles la vaccination est pratiquée. Il est donc important de savoir si quelqu'un a reçu un certain vaccin même après, par exemple, 30 ans. Il est important pour le médecin mais aussi pour la personne vaccinée de connaître le statut vaccinal des vaccins qui ont été placés il y a longtemps.

En revanche, dans le suivi scientifique de l'efficacité des vaccins, il est également nécessaire de vérifier encore plus qu'après 30 ans si quelqu'un a été vacciné. Par exemple, on a vu que le vaccin contre la coqueluche chez les personnes âgées perd de sa force, de sorte qu'un vaccin de rappel est placé. Pour réaliser ces études, il faut bien sûr savoir s'il y a eu vaccination.

Au plus tard, les effets secondaires des médicaments auxquels appartiennent les vaccins n'apparaissent parfois qu'après de nombreuses années. Un exemple classique de médicament est le diéthylstilbestrol (DES), une hormone administrée aux femmes. On a constaté que de nombreuses filles nées de mères DES avaient un risque accru de cancer du vagin et du col de l'utérus à l'âge adulte. S'ils avaient détruit ces données, ils n'auraient peut-être pas pu établir le lien. Mais les effets différés peuvent également être positifs. Par exemple, il y a l'hypothèse que les personnes (par exemple les enfants) qui ont reçu il y a encore longtemps un vaccin BCG contre la tuberculose pourraient être moins sensibles au COVID-19.

Enfin, un ensemble limité de données en lien avec les résultats de laboratoire provenant de la Base de données I de l'Accord de coopération du 25 août 2020 ne peut pas être supprimé après 60 jours. Ces données sont, en effet, nécessaires pour les processus opérationnels et les finalités liés aux enregistrements des vaccinations. A cet égard, il s'agit dans un premier temps de la finalité de pharmacovigilance. Pour cette finalité, dans le cadre des cas dits ' de percée ' ou ' break through cases ', il pourra être demandé au laboratoire concerné, pour une personne vaccinée qui développe malgré tout la COVID-19, d'effectuer un séquençage du génome complet afin d'analyser la cause de l'échec des vaccinations. Par ailleurs, la conservation de ces données pendant une période plus longue est aussi nécessaire pour la finalité de l'organisation logistique des vaccinations contre la COVID-19. Les données relatives aux contaminations antérieures qui ont permis d'acquérir une certaine immunité, peuvent, en effet, être pertinentes lorsqu'il y a lieu de déterminer la priorité de vaccination des groupes cibles » (*Moniteur belge* du 12 avril 2021, pp. 32411-32412; voy. aussi *Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, pp. 16-18).

B.35.1. Dans son avis sur l'avant-projet de loi devenue la loi du 2 avril 2021 portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé :

« 30. Conformément au texte néerlandais de l'article 6, § 2, de l'accord de coopération, les données de la base de données Vaccinet sont conservées ' gedurende 30 jaar na de vaccinatie tegen COVID-19 of in elk geval tot minstens 1 jaar na het overlijden van de persoon waaraan het vaccin werd toegediend '. Selon le texte français, ces données sont conservées ' pendant 30 ans à compter de la date de vaccination contre la COVID-19 et en tout cas pendant un an au moins après le décès de la personne qui a reçu le vaccin '. Selon le texte allemand, les données sont conservées ' *dreißig Jahre nach dem Datum der Impfung gegen COVID-19 und in jedem Fall mindestens ein Jahr nach dem Tod der Person, der der Impfstoff verabreicht wurde* '.

Indépendamment de la question de savoir si les différentes conjonctions (' of ', ' et ' et ' und ') ne donnent pas une portée différente à cette disposition, le Conseil d'État se demande pourquoi il est prévu un si long délai de trente ans, compte tenu notamment de l'article 5, paragraphe 1, e), du RGPD.

Même s'il peut être admis que le délai d'un an après le décès de la personne vaccinée est dicté par des considérations relatives à la pharmacovigilance, la mention ' au moins ' ne fixe pas de délai maximum, mais un délai minimum de conservation. Sans doute faut-il écrire ' au maximum ' au lieu de ' au moins ' » (*ibid.*, pp. 54-55; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, p. 90; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, pp. 85-86; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 32-33; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 18-19; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, pp. 33-34).

B.35.2. Dans son avis n° 16/2021 du 10 février 2021 sur l'avant-projet d'accord de coopération devenu l'accord de coopération du 12 mars 2021, l'Autorité de protection des données a observé :

« 51. Les données à caractère personnel enregistrées dans Vaccinnet en application du projet d'accord de coopération sont conservées, en vertu de son article 6, § 2, pendant 30 ans à compter de la date de vaccination contre la COVID-19 et en tout cas pendant un an au moins après le décès de la personne qui a reçu le vaccin.

52. L'Autorité estime que le délai de conservation de 30 ans prévu dans le projet d'accord de coopération peut éventuellement être retenu pour des données pseudonymisées dans le cadre de finalités plutôt scientifiques/statistiques. Pour des finalités plus opérationnelles, ce délai de conservation extrêmement long paraît excessif ».

B.35.3. Sur la durée de conservation des données, la ministre wallonne de la Santé a rappelé que « la durée de validité du vaccin n'est pas encore connue à ce jour » et qu'« il est important de connaître le statut vaccinal d'une personne, en ce compris de nombreuses années après la vaccination » (*Doc. parl.,* Parlement wallon, C.R.I., n° 25, 2020-2021, 31 mars 2021, p. 74).

B.35.4. Devant l'assemblée de la Commission communautaire française, le ministre de la Santé a également précisé :

« Concernant la base de données Vaccinnet+, le délai de conservation des données est de 30 ans car cette durée préexistait à l'accord de coopération. Cela semble long mais fut jugé nécessaire par les scientifiques. En effet, il est primordial que la personne vaccinée ainsi que les prestataires de soins puissent se faire une idée des vaccinations administrées au fur et à mesure de la vie de cette personne.

Dans le cadre de rappels de vaccins, cela peut également être utile. La durée de protection du vaccin contre la Covid-19 n'est pas encore connue. Il est impossible de savoir, aujourd'hui, ce qui se passera dans six mois, un an, voire deux ans. Il est donc important d'avoir l'opportunité, à cet instant, de consulter les dossiers de vaccination des citoyens afin de savoir, exactement, quels sont les vaccins reçus, dans quels délais, etc.

Pour les études relatives au suivi scientifique de l'efficacité des vaccins, il est également nécessaire de vérifier, bien après 30 ans, si un citoyen est vacciné. Il cite en exemple le vaccin de la coqueluche, qui perd de sa force chez les personnes âgées et qui nécessite un rappel.

Ce délai de conservation est donc important, dans le cadre des règles de responsabilité vis-à-vis des acteurs concernés. Aussi, étant donné l'incertitude relative aux effets indésirables potentiels sur le long terme, bien que ceux-ci soient rares, voire extrêmement rares, il est primordial de pouvoir effectuer des anamnèses de nombreuses années après l'administration d'un vaccin » (*Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/2, p. 12).

B.36.1. Conformément au principe de limitation de la conservation des données, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (article 5, paragraphe 1, point e), du RGPD).

B.36.2. L'article 6, § 2, de l'accord de coopération du 12 mars 2021 fixe une durée maximale de conservation des données.

Les données enregistrées dans la banque de données « Vaccinnet » sont conservées au minimum 30 ans et au maximum jusqu'à la date du décès de la personne concernée.

B.37.1. La nécessité de la durée de conservation des données s'apprécie au regard des circonstances d'espèce, et en tenant compte du fait que le délai généralement accepté pour la conservation des dossiers concernant la santé et dans le cadre de la recherche scientifique en matière de santé est assez long.

B.37.2. En vertu de l'article 9, § 1er, de la loi du 22 août 2002 sur les droits du patient, le patient « a droit, de la part de son praticien professionnel, à un dossier de patient soigneusement tenu à jour et conservé en lieu sûr » et, à sa demande, « le praticien professionnel ajoute les documents fournis par le patient dans le dossier le concernant ».

Les travaux préparatoires de cette disposition indiquent :

« L'alinéa 1er de l'article 9, § 1er, dispose que le patient a droit à un dossier de patient soigneusement tenu à jour et conservé en lieu sûr. Les normes auxquelles le dossier de patient doit répondre, entre autres, sur le plan du contenu, ne sont pas réglées par le présent projet. A cet égard, on peut renvoyer entre autres à l'AR du 3 mai 1999 relatif au dossier médical général et à l'AR du 3 mai 1999 portant fixation des normes minimales générales auxquelles le dossier médical, tel que visé à l'article 15 de la loi sur les hôpitaux, doit répondre » (*Doc. parl.*, Chambre, 2001-2002, DOC 50-1642/001, p. 29).

L'article 1er de l'arrêté royal du 3 mai 1999 « relatif au dossier médical général » définit le « dossier médical général » (DMG) comme « un ensemble fonctionnel et sélectif de données médicales, sociales et administratives pertinentes relatives à un patient, qui font l'objet d'un

traitement manuel ou informatisé », et qui comprend, notamment « l'anamnèse et les antécédents (maladies, interventions, vaccins reçus) ».

L'article 1er, § 3, de l'arrêté royal du 3 mai 1999 « déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre », prévoit que le dossier médical ouvert pour chaque patient au sein d'un hôpital « doit être conservé pendant au moins trente ans dans l'hôpital ».

L'article 35 de la loi du 22 avril 2019 « relative à la qualité de la pratique des soins de santé » dispose :

« Le professionnel des soins de santé conserve le dossier du patient pendant minimum 30 ans et maximum 50 ans à compter du dernier contact avec le patient ».

L'article 24 du Code de déontologie médicale dispose :

« Les dossiers des patients doivent être conservés pendant trente ans après le dernier contact avec le patient, de manière sécurisée et en respectant le secret professionnel. Passé ce délai, le médecin peut détruire les dossiers.

Lorsque sa pratique cesse, le médecin transmet au médecin désigné par le patient ou au patient tous les renseignements utiles pour garantir la continuité des soins ».

Il résulte de ce qui précède qu'un délai de conservation de 30 ans au moins constitue le délai habituellement accepté en matière de données concernant la santé.

B.37.3. Il convient également d'avoir égard aux circonstances d'urgence pandémique entourant l'élaboration, l'autorisation de mise sur le marché, la production et l'administration des vaccins contre la COVID-19 et la nécessité de pouvoir évaluer, à moyen et à long terme, l'efficacité de ces vaccins, de même que leurs éventuels effets indésirables. C'est notamment dans le but de cette évaluation que les finalités liées à la prestation de soins et de traitement (article 4, § 2, 1°), à la pharmacovigilance des vaccins (article 4, § 2, 2°), au suivi et à la

surveillance post-autorisation des vaccins (article 4, § 2, 8°), ou à l'exécution d'études scientifiques ou statistiques (article 4, § 2, 10°) ont été définies.

B.37.4. Au vu de ce qui précède, la conservation des données de vaccination contre la COVID-19 jusqu'au décès de la personne vaccinée n'excède pas ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

B.38. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment à l'article 6, § 2, de l'accord de coopération, le moyen unique, dans sa deuxième branche, n'est pas fondé.

IV. En ce qui concerne l'absence d'analyse d'impact préalable requise par l'article 35 du RGPD (deuxième branche)

B.39. La partie requérante critique l'absence d'exécution d'une analyse d'impact préalable relative à la protection des données, au sens de l'article 35 du RGPD, de sorte qu'en l'absence de cette analyse d'impact, les dispositions visées au moyen seraient violées.

B.40. L'exposé général de l'accord de coopération du 12 mars 2021 indique :

« L'accord de coopération a été soumis à l'avis de l'Autorité de protection des données (avis 16-2021 du 10 février 2021), à l'avis de la ' Vlaamse Toezichtscommissie ' (avis 2021/13 du 17 février 2021), aux avis du Conseil d'Etat (68.832/VR, 68836/VR, 68 837/VR 68.839/VR, 68.840/VR, 68/844/VR du 18 février 2021), à l'avis du Conseil flamand pour l'Aide sociale, la Santé publique et la Famille (avis du 16 février 2021), à l'avis de l'Organe de concertation intra-francophone et de la concertation en Comité ministériel de concertation intra-francophone (avis du 15 février 2021).

Une analyse d'impact relative à la protection des données est établie en application des articles 35 et 36 du Règlement Général sur la Protection des Données » (*Moniteur belge* du 12 avril 2021, p. 32398).

B.41.1. Dans son avis sur l'avant-projet de loi devenue la loi du 2 avril 2021 portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé :

« À la question de savoir si cette analyse d'impact avait déjà été effectuée, les délégués ont répondu :

‘ *Nee, dit zal nog gebeuren* ’.

L'auteur de l'avant-projet veillera par conséquent au bon accomplissement de cette étude d'impact, si possible avant l'assentiment par l'assemblée législative de l'accord de coopération à l'examen » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 46; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, p. 82; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, pp. 81-82; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 27-28; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 11-12; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, p. 29).

B.41.2. Dans son avis n° 16/2021 du 10 février 2021, l'Autorité de protection des données a observé, comme elle l'avait déjà fait dans son avis n° 138/2020 du 18 décembre 2020 relatif à l'arrêté royal du 24 décembre 2020 (point 21) :

« Étant donné que les enregistrements de données en matière de vaccinations contre la COVID-19 encadrés dans le projet d'accord de coopération s'accompagnent de traitements à grande échelle d'une catégorie particulière de données à caractère personnel, à savoir des données relatives à la santé, le(s) responsable(s) du traitement est (sont) tenu(s), en vertu de l'article 35.3 du RGPD, de réaliser préalablement au traitement une analyse d'impact relative à la protection des données. Bien que l'Autorité ait déjà souligné l'importance de cette disposition dans son avis n° 138/2020, le demandeur indique toujours dans le formulaire de demande d'avis que les traitements visés par le projet d'accord de coopération n'ont pas été soumis à une telle analyse d'impact relative à la protection des données. L'Autorité insiste à nouveau dans le présent avis pour qu'une telle analyse soit réalisée » (point 19).

B.41.3. Dans le rapport du 23 mars 2021, le ministre de la Santé publique a indiqué :

« L'analyse d'impact relative à la protection des données (*data protection impact assessment*) a été réalisée et un résumé est disponible » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/002, p. 14).

B.42. Si le traitement de données personnelles est susceptible d'engendrer un « risque élevé pour les droits et libertés des personnes physiques », le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées

sur la protection des données à caractère personnel, conformément à l'article 35 du RGPD. En vertu de l'article 36 du RGPD, lorsque l'analyse d'impact indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque, le responsable du traitement doit consulter l'autorité de contrôle préalablement au traitement.

B.43. L'article 35 du RGPD impose la réalisation d'une analyse d'impact relative à la protection des données avant l'acte matériel de traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, mais ne l'impose pas avant ou lors de l'élaboration d'une disposition législative relative à un tel traitement. Dès lors que le caractère préalable de l'analyse d'impact concerne un acte matériel de traitement, il ne relève pas de la compétence de la Cour mais bien de la compétence du juge judiciaire ou administratif.

Ce constat ne porte pas préjudice à l'obligation pour les États membres de consulter « 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 », conformément à l'article 36, paragraphe 4, du RGPD, obligation à laquelle le législateur a déféré en l'espèce.

B.44.1. Enfin, en ce qui concerne la critique dirigée contre la confidentialité de l'analyse d'impact, soulevée par la partie requérante dans son mémoire en réponse, cette critique n'est pas recevable, car elle revient à modifier la portée de la deuxième branche du moyen, qui se limitait à critiquer l'absence d'analyse d'impact préalable.

Il n'appartient en effet pas à une partie requérante de modifier, dans son mémoire en réponse, le moyen tel qu'elle l'a elle-même formulé dans la requête. Un grief qui, comme en l'espèce, est articulé dans un mémoire en réponse mais qui diffère de celui qui est énoncé dans la requête constitue dès lors un moyen nouveau et n'est pas recevable.

B.44.2. Pour le surplus, le RGPD ne fait pas obligation de publier cette analyse (Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la

manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, 4 avril 2017, modifiées en dernier lieu le 4 octobre 2017, Groupe de travail « Article 29 » sur la protection des données, p. 21). La confidentialité peut en effet se justifier par le fait que l'analyse d'impact porte sur d'éventuels risques en matière de sécurité, et notamment la description technique des mesures envisagées afin d'atténuer ces risques. Le fait de rendre publique cette analyse risquerait par conséquent de compromettre la sécurité du traitement de ces données, et compromettrait dès lors le droit au respect de la vie privée et de la protection des données personnelles.

B.45. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils n'auraient pas été précédés d'une analyse d'impact préalable, le moyen unique, dans sa deuxième branche, n'est pas fondé.

V. En ce qui concerne la rétroactivité des effets de l'accord de coopération au 24 décembre 2020, prévue par l'article 12 (troisième branche)

B.46. Dans la troisième branche du moyen, la partie requérante estime que les actes attaqués sont contraires au principe de la non-rétroactivité des lois qui exige que le contenu du droit soit prévisible et accessible, de sorte que le justiciable puisse prévoir, à un degré raisonnable, les conséquences d'un acte déterminé au moment où cet acte est accompli.

Ainsi, l'article 12 de l'accord de coopération du 12 mars 2021 prévoit que les dispositions de cet accord rétroagissent au jour de l'entrée en vigueur de l'arrêté royal du 24 décembre 2020, alors que, souligne la partie requérante, la onzième finalité reprise dans l'article 4, § 2, de l'accord de coopération ne figurait pas dans l'arrêté royal du 24 décembre 2020.

B.47.1. L'article 12 de l'accord de coopération du 12 mars 2021 dispose :

« Le présent accord de coopération produit ses effets à partir du 24 décembre 2020 pour ce qui concerne les dispositions dont le contenu correspond à celui de l'arrêté royal du 24 décembre 2020 concernant l'enregistrement et le traitement de données relatives aux

vaccinations contre la COVID-19 et à partir du 11 février 2021 pour ce qui concerne les autres dispositions.

Le présent accord de coopération produit ses effets jusqu'à sa révision ou sa révocation qui intervient le jour où le Secrétariat central du Comité de concertation a reçu l'accord écrit de toutes les parties pour mettre fin à l'accord de coopération et après la publication d'une communication confirmant cet accord écrit au *Moniteur belge* ».

B.47.2. L'exposé général de l'accord de coopération du 12 mars 2021 indique :

« L'article 12 régit les effets dans le temps de l'accord de coopération et prévoit la possibilité de le réviser ou révoquer » (*Moniteur belge* du 12 avril 2021, p. 32413; voy. aussi *Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 19).

B.48. Dans son avis sur l'avant-projet de loi devenue la loi du 2 avril 2021, attaquée, portant assentiment à l'accord de coopération du 12 mars 2021, la section de législation du Conseil d'État a observé :

« Conformément à l'article 12 de l'accord de coopération, celui-ci produit ses effets le 24 décembre 2020.

La non-rétroactivité des règles au niveau hiérarchique d'une norme législative est une garantie ayant pour but de prévenir l'insécurité juridique. Cette garantie exige que le contenu du droit soit prévisible et accessible, de sorte que le justiciable puisse prévoir, à un degré raisonnable, les conséquences d'un acte déterminé au moment où cet acte est accompli. La rétroactivité peut uniquement être justifiée lorsqu'elle est indispensable à la réalisation d'un objectif d'intérêt général.

En l'occurrence, la rétroactivité poursuit un objectif d'intérêt général, à savoir le maintien d'un cadre juridique offrant une sécurité juridique suffisante pour lutter contre la pandémie de COVID-19.

Ainsi qu'il a déjà été exposé dans les avis concernant les textes d'assentiment à l'accord de coopération relatif au traçage des contacts, un effet rétroactif peut, dans ces circonstances, être exceptionnellement conféré aux dispositions de l'accord de coopération qui correspondent sur le fond à ce qui a été réglé dans la réglementation fédérale, laquelle répond d'urgence à la nécessité de lutter contre la pandémie de COVID-19, à compter de la date d'entrée en vigueur de cette réglementation fédérale, plus particulièrement l'arrêté royal du 24 décembre 2020 ' concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 '.

Cette justification ne vaut cependant pas pour les nouveaux éléments qui ne correspondent pas au traitement de données à caractère personnel tel qu'il s'est concrétisé dans les faits depuis cette date. Il faudra dès lors veiller à ce que les règles contenues dans cet accord de coopération s'accordent parfaitement avec cette concrétisation effective » (*Doc. parl.*, Chambre,

2020-2021, DOC 55-1853/001, pp. 56-57; voy. aussi *Doc. parl.*, Parlement flamand, 2020-2021, n° 708/1, p. 92; *Doc. parl.*, Parlement wallon, 2020-2021, n° 509/1, pp. 86-87; *Doc. parl.*, Parlement de la Communauté germanophone, 2020-2021, n° 132/1, pp. 34-35; *Doc. parl.*, Assemblée réunie de la Commission communautaire commune, 2020-2021, n° B-65/1, pp. 20-21; *Doc. parl.*, Assemblée de la Commission communautaire française, 2020-2021, n° 45/1, p. 35).

B.49.1. Dans le contexte rappelé en B.2, il convient de souligner que l'accord de coopération du 12 mars 2021 a été conclu dans un délai de moins de trois mois, parallèlement au lancement en janvier 2021 de la campagne de vaccination dans des conditions d'urgence, en vue de lutter contre la pandémie de COVID-19.

Par l'arrêté royal du 24 décembre 2020, pris conformément à l'article 11 de la loi du 22 décembre 2020, de même que par le protocole d'accord du 27 janvier 2021, les différentes autorités du pays ont adopté le fondement juridique permettant l'enregistrement des données de vaccination, dans l'attente d'un accord de coopération.

B.49.2. Comme il est dit en B.4, le contenu de l'accord de coopération reprend le contenu du protocole d'accord du 27 janvier 2021 qui, lui-même, reprenait, en l'adaptant, le contenu de l'arrêté royal du 24 décembre 2020. La date d'abrogation de l'arrêté royal du 24 décembre 2020, de même que celle du protocole d'accord du 27 janvier 2021 sont fixées à la date à laquelle l'accord de coopération du 12 mars 2021 sortit ses effets.

Il résulte de ce qui précède que la rétroactivité contenue dans l'article 12 de l'accord de coopération du 12 mars 2021 est justifiée par l'objectif d'intérêt général d'assurer la sécurité juridique en consolidant et remplaçant la base légale de l'enregistrement des données de vaccination dans « Vaccinnet ». Comme l'a souligné la section de législation du Conseil d'État, cette rétroactivité « poursuit un objectif d'intérêt général, à savoir le maintien d'un cadre juridique offrant une sécurité juridique suffisante pour lutter contre la pandémie de COVID-19 » (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1853/001, p. 56).

B.49.3. Cette rétroactivité n'entraîne par ailleurs pas d'effets disproportionnés. En prévoyant que l'accord de coopération du 12 mars 2021 produit ses effets à partir du

24 décembre 2020 pour ce qui concerne les dispositions dont le contenu correspond à celui de l'arrêté royal du 24 décembre 2020 « concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la COVID-19 » et à partir du 11 février 2021 pour ce qui concerne les autres dispositions, l'article 12 de l'accord de coopération du 12 mars 2021 ne porte en effet pas atteinte à la sécurité juridique et aux attentes légitimes, dès lors qu'il n'emporte aucune modification du contenu du régime existant antérieurement, mais se limite à le consolider.

Il convient en effet de constater que, pour les éléments qui correspondent au traitement de données à caractère personnel tel qu'il était prévu par l'arrêté royal du 24 décembre 2020, l'accord de coopération sortit ses effets à la date d'entrée en vigueur de cet arrêté royal, tandis que, pour les nouveaux éléments qui ne correspondent pas au traitement de données à caractère personnel tel qu'il s'est concrétisé dans les faits depuis cette date, l'accord de coopération sortit ses effets à la date d'entrée en vigueur du protocole d'accord du 27 janvier 2021, soit le 11 février 2021. Il convient à cet égard de constater que la finalité visée à l'article 4, § 2, 11°, de l'accord de coopération du 12 mars 2021, que critique la partie requérante, était déjà contenue dans le protocole d'accord du 27 janvier 2021.

B.50. En ce qu'il est dirigé contre les actes attaqués en ce qu'ils portent assentiment à l'article 12 de l'accord de coopération du 12 mars 2021, le moyen unique, dans sa troisième branche, n'est pas fondé.

En ce qui concerne la demande de maintien des effets

B.51. Les autorités institutionnelles demandent le maintien des effets des actes attaqués en cas d'annulation.

B.52.1. Lorsqu'un recours en annulation, dirigé contre une norme législative, est fondé, la Cour a uniquement, en vertu de l'article 8, alinéa 1er, de la loi spéciale du 6 janvier 1989, le pouvoir d'annuler l'acte attaqué en tout ou en partie.

Lorsqu'elle annule, comme en l'espèce, une norme législative, de manière inconstitutionnelle, la Cour peut, en vertu de l'article 8, alinéa 3, de la loi spéciale, maintenir provisoirement les effets d'une disposition annulée, jusqu'à ce que le législateur ait mis fin à l'inconstitutionnalité constatée, et pour le délai qu'elle détermine.

B.52.2. Il ressort de la jurisprudence de la Cour de justice que les principes de primauté et de plein effet du droit de l'Union européenne s'opposent à un maintien provisoire de mesures nationales qui sont contraires au droit de l'Union directement applicable (CJUE, grande chambre, 8 septembre 2010, C-409/06, *Winner Wetten GmbH*). Eu égard à cette jurisprudence, la Cour constitutionnelle ne peut donc pas donner suite à une demande de maintien des effets d'un acte législatif annulé, en ce qu'il serait ainsi porté atteinte au plein effet du droit de l'Union.

B.52.3. Pour le surplus, il n'y a pas lieu de faire droit à cette demande, compte tenu de la portée limitée de l'annulation prononcée.

Par ces motifs,

la Cour

- annule la loi du 2 avril 2021, le décret de la Communauté flamande du 2 avril 2021, le décret de la Communauté germanophone du 29 mars 2021, l'ordonnance de la Commission communautaire commune du 2 avril 2021, le décret de la Région wallonne du 1er avril 2021 et le décret de la Commission communautaire française du 1er avril 2021 « portant assentiment à l'accord de coopération du 12 mars 2021 entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 », en ce qu'ils portent assentiment à l'article 5 de l'accord de coopération du 12 mars 2021, dans la mesure où cet article concerne la communication des données visées à l'article 3, § 2, de l'accord de coopération précité, enregistrées dans la banque de données « Vaccinnet »;

- rejette le recours pour le surplus.

Ainsi rendu en langue française, en langue néerlandaise et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 1er juin 2023.

Le greffier, Le président,

F. Meersschaut P. Nihoul