Cour constitutionnelle

Arrêt n° 110/2022
du 22 septembre 2022
Numéros du rôle : 7555, 7556, 7557, 7558, 7559 et 7560

En cause : les recours en annulation du décret de la Région wallonne du 30 septembre 2020, du décret de la Communauté germanophone du 12 octobre 2020, de l'article 2 de la loi du 9 octobre 2020, de l'ordonnance de la Commission communautaire commune du 1er octobre 2020 et du décret de la Communauté flamande du 2 octobre 2020 « portant assentiment à 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'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 », introduits par l'ASBL « Vivant Ostbelgien » et autres et par l'ASBL « Ligue des droits humains ».

La Cour constitutionnelle,

composée des présidents P. Nihoul et L. Lavrysen, des juges T. Giet, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne, D. Pieters, S. de Bethune, E. Bribosia et W. Verrijdt, et, conformément à l'article 60*bis* de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, du juge émérite J.-P. Moerman, assistée du greffier P.-Y. Dutilleux, présidée par le président P. Nihoul,

après en avoir délibéré, rend l'arrêt suivant :

I. *Objet des recours et procédure*

a. Par requête adressée à la Cour par lettre recommandée à la poste le 12 avril 2021 et parvenue au greffe le 14 avril 2021, un recours en annulation du décret de la Région wallonne du 30 septembre 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 » (publié au *Moniteur belge* du 15 octobre 2020, deuxième édition) a été introduit par l'ASBL « Vivant Ostbelgien », Diana Stiel, Alain Mertes et Michael Balter, assistés et représentés par Me R. Fonteyn, avocat au barreau de Bruxelles.

b. Par requête adressée à la Cour par lettre recommandée à la poste le 12 avril 2021 et parvenue au greffe le 14 avril 2021, un recours en annulation du décret de la Communauté germanophone du 12 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 » (publié au *Moniteur belge* du 15 octobre 2020, deuxième édition) a été introduit par l'ASBL « Vivant Ostbelgien », Diana Stiel, Alain Mertes et Michael Balter, assistés et représentés par Me R. Fonteyn.

c. Par requêtes adressées à la Cour par lettres recommandées à la poste le 12 avril 2021 et parvenues au greffe le 14 avril 2021, des recours en annulation de l'article 2 de 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 » (publiée au *Moniteur belge* du 15 octobre 2020, deuxième édition) ont été introduits par l'ASBL « Ligue des droits humains », assistée et représentée par Me C. Forget, Me S. Najmi, avocats au barreau de Bruxelles, et Me R. Fonteyn, et par l'ASBL « Vivant Ostbelgien », Diana Stiel, Alain Mertes et Michael Balter, assistés et représentés par Me R. Fonteyn.

d. Par requête adressée à la Cour par lettre recommandée à la poste le 12 avril 2021 et parvenue au greffe le 14 avril 2021, un recours en annulation de l'ordonnance de la Commission communautaire commune du 1er octobre 2020 « portant assentiment de l'accord de coopération du 25 août 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'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 » (publiée au *Moniteur belge* du 15 octobre 2020, deuxième édition) a été introduit par l'ASBL « Vivant Ostbelgien », Diana Stiel, Alain Mertes et Michael Balter, assistés et représentés par Me R. Fonteyn.

e. Par requête adressée à la Cour par lettre recommandée à la poste le 12 avril 2021 et parvenue au greffe le 14 avril 2021, un recours en annulation du décret de la Communauté

flamande du 2 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 autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano » (publié au *Moniteur belge* du 15 octobre 2020, deuxième édition) a été introduit par l'ASBL « Vivant Ostbelgien », Diana Stiel, Alain Mertes et Michael Balter, assistés et représentés par Me R. Fonteyn.

Ces affaires, inscrites sous les numéros 7555, 7556, 7557, 7558, 7559 et 7560 du rôle de la Cour, ont été jointes.

Des mémoires et mémoires en réplique ont été introduits par :

- le Conseil des ministres, assisté et représenté par Me M. Feys, avocat au barreau de Gand;

- le Gouvernement flamand, assisté et représenté par Me M. Feys;

- le Gouvernement wallon, assisté et représenté par Me M. Feys;

- le Collège réuni de la Commission communautaire commune, assisté et représenté par Me M. Feys;

- le Gouvernement de la Communauté germanophone, assisté et représenté par Me M. Feys.

Les parties requérantes dans les affaires n^{os} 7555, 7556, 7558, 7559 et 7560 ont introduit un mémoire en réponse.

Par ordonnance du 18 mai 2022, la Cour, après avoir entendu les juges-rapporteurs T. Detienne et W. Verrijdt, a :

- décidé que les affaires étaient en état et fixé l'audience au 29 juin 2022;

- invité les parties à répondre préalablement aux questions suivantes par un mémoire complémentaire à introduire par pli recommandé à la poste le 17 juin 2022 au plus tard et à communiquer dans le même délai aux autres parties, ainsi qu'au greffe de la Cour par courriel envoyé à l'adresse « griffie@const-court.be » :

« 1. Pouvez-vous expliquer l'articulation de l'article 6, §§ 5 et 6, de l'article 7 et de l'article 10, § 1er, de l'accord de coopération du 25 août 2020 ? Pourquoi certaines catégories de données de la base de données I qui sont communiquées par les centres de contact à Sciensano conformément à l'article 6, §§ 5 et 6, de l'accord de coopération du 25 août 2020

sont-elles identiques aux catégories de données de la base de données III qui sont communiquées par Sciensano aux centres de contact conformément à l'article 7 ?

2. Comment les données à caractère personnel visées à l'article 6, §§ 5 et 6, de l'accord de coopération sont-elles communiquées par les centres de contact à Sciensano en vue de leur enregistrement dans la base de données I ? Les centres de contact enregistrent-ils dans la base de données I les données qu'ils recueillent et si oui, en vertu de quelle disposition ?

3. Pouvez-vous expliquer la référence faite par l'article 3, § 1er, 4°, et par l'article 10, § 2, de l'accord de coopération du 25 août 2020 aux personnes de catégorie V et/ou VI ' visées à l'article 6 ' ? Les données à caractère personnel relatives aux personnes de catégories V et VI sont-elles collectées dans la base de données I, et si oui, en vertu de quelle disposition ? ».

Des mémoires complémentaires ont été introduits par :

- le Conseil des ministres;

- le Gouvernement flamand;

- le Gouvernement wallon;

- le Collège réuni de la Commission communautaire commune;

- le Gouvernement de la Communauté germanophone.

À l'audience publique du 29 juin 2022 :

- ont comparu :

. Me R. Fonteyn, pour les parties requérantes dans les affaires n^{os} 7555, 7556, 7558, 7559 et 7560;

. Me R. Fonteyn, qui comparaissait également *loco* Me C. Forget et Me S. Najmi, pour la partie requérante dans l'affaire n° 7557;

. Me M. Feys et Me A. Vandeburie, avocat au barreau de Bruxelles, pour le Conseil des ministres, le Gouvernement flamand, le Gouvernement wallon, le Collège réuni de la Commission communautaire commune et le Gouvernement de la Communauté germanophone;

- les juges-rapporteurs T. Detienne et W. Verrijdt ont fait rapport;

- les avocats précités ont été entendus;

- les affaires ont été mises en délibéré.

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 -

Quant à l'intérêt

A.1.1. La première partie requérante dans les affaires n^{os} 7555, 7556, 7558, 7559 et 7560 expose qu'elle est un parti politique à portée territoriale spécifique qui a vocation à défendre les intérêts particuliers des habitants de la Communauté germanophone. Elle justifie son intérêt à demander l'annulation de l'ensemble des actes 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'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 (ci-après : l'accord de coopération du 25 août 2020) par le fait que cet accord de coopération vise notamment les habitants de la Communauté germanophone. Elle soutient en outre que les actes attaqués ont une incidence sur les recours en annulation qu'elle a introduits devant le Conseil d'État contre l'arrêté royal n° 18 du 4 mai 2020 « portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 », contre l'arrêté royal n° 25 du 28 mai 2020 « modifiant l'arrêté royal n° 18 du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 », contre l'arrêté royal n° 44 du 26 juin 2020 « concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano » et contre l'arrêté du Gouvernement wallon de pouvoirs spéciaux n° 35 du 5 mai 2020 « organisant le tracing socio-sanitaire dans le cadre de la lutte contre l'épidémie COVID-19 ». Elle se réfère à ses écrits de procédure devant le Conseil d'État.

Les deuxième à quatrième parties requérantes dans les affaires précitées sont des députés du Parlement de la Communauté germanophone. Elles justifient leur intérêt par le fait qu'en vertu des actes attaqués, des éléments essentiels de leur vie privée sont susceptibles d'être collectés et communiqués à des banques de données dont elles contestent la légalité.

La partie requérante dans l'affaire n° 7557 est une association sans but lucratif qui a pour but de combattre l'injustice et toute atteinte arbitraire aux droits d'un individu ou d'une collectivité.

A.1.2. Les parties requérantes dans les affaires n^{os} 7555, 7556, 7558, 7559 et 7560 estiment disposer de l'intérêt requis pour attaquer non seulement le décret de la Communauté germanophone du 12 octobre 2020 mais aussi les autres actes qui portent assentiment à l'accord de coopération du 25 août 2020, puisque cet accord de coopération vise notamment les habitants de la Communauté germanophone.

A.2.1. Le Conseil des ministres, le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté germanophone et le Collège réuni de la Commission communautaire commune (ci-après : les autorités défenderesses) contestent l'intérêt de la première partie requérante dans les affaires n^{os} 7555, 7558, 7559 et 7560, au motif que celle-ci ne démontre pas en quoi les recours présentement examinés sont susceptibles d'influencer les recours qu'elle a introduits devant le Conseil d'État. Les autorités défenderesses observent que ces recours sont dirigés contre l'arrêté royal n° 18 du 4 mai 2020, contre l'arrêté royal n° 25 du 28 mai 2020 et contre l'arrêté royal n° 44 du 26 juin 2020, précités, qui ont perdu leur objet du fait de leur retrait par les articles 3 à 5 de la loi du 9 octobre 2020. Elles se réfèrent en outre à l'article 7 de la loi du 27 mars 2020 « habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus COVID-19 (II) ».

Selon les autorités défenderesses, la première partie requérante n'établit pas que les actes attaqués sont susceptibles d'affecter son but statutaire, qui s'apparente du reste à la défense de l'intérêt général. Enfin, le caractère territorial de son but statutaire ne lui permet pas de justifier d'un intérêt à l'annulation du décret de la

Région wallonne du 30 septembre 2020, de l'ordonnance de la Commission communautaire commune du 1er octobre 2020 et du décret de la Communauté flamande du 2 octobre 2020.

Les autorités défenderesses contestent également l'intérêt à agir des deuxième à quatrième parties requérantes dans les mêmes affaires au motif, d'une part, que leur qualité de parlementaire ne leur confère pas un intérêt fonctionnel suffisant et, d'autre part, qu'elles ne disposent pas d'un intérêt direct à l'annulation du décret de la Région wallonne du 30 septembre 2020, de l'ordonnance de la Commission communautaire commune du 1er octobre 2020 et du décret de la Communauté flamande du 2 octobre 2020.

A.2.2. Les autorités défenderesses contestent l'intérêt au recours des première à quatrième parties requérantes dans l'affaire n° 7556 pour les mêmes motifs que ceux qui sont exposés en A.2.1 ainsi qu'en raison de l'absence d'identification, par ces parties requérantes, de la disposition dont elles demandent l'annulation. Elles observent sur ce point que les articles 2 à 11 du décret de la Communauté germanophone du 12 octobre 2020 ne concernent pas l'assentiment à l'accord de coopération du 25 août 2020.

A.2.3. Les autorités défenderesses font valoir que l'intérêt de la partie requérante dans l'affaire n° 7557 doit toujours être apprécié au cas par cas et que cette dernière n'établit pas que les actes attaqués sont susceptibles d'affecter son but statutaire, qui s'apparente du reste à la défense de l'intérêt général.

Quant au moyen unique

A.3.1. Le moyen unique est pris de la violation des articles 10, 11 et 22 de la Constitution, lus en combinaison ou non avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne, avec les articles 4, point 7), 5, paragraphe 1), 6, 9, 14, 35 et 36 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). Il est divisé en dix branches.

A.3.2. Les parties requérantes dans les affaires n^{os} 7555, 7556, 7558, 7559 et 7560 soutiennent que leurs requêtes sont dirigées contre les actes attaqués en ce qu'ils portent assentiment à l'accord de coopération du 25 août 2020 et que les autorités défenderesses font une application erronée de l'arrêt n° 171/2015 du 3 décembre 2015. Elles font valoir que la manière dont les articles 10 et 11 de la Constitution, l'article 7 de la Charte des droits fondamentaux et les articles 4, point 7), 35 et 36 du RGPD sont violés, est exposée avec la précision requise.

A.3.3. Dans leurs mémoires en réponse, les parties requérantes dans les affaires n^{os} 7555, 7556, 7558, 7559 et 7560 invitent la Cour à poser à la Cour de justice de l'Union européenne la question préjudicielle suivante :

« Le droit de l'Union, et particulièrement les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne et les articles 4.7, 5.1, 6, 9, 14, 35 et 36 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 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, lus isolément ou en combinaison avec les dispositions du 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, s'oppose-t-il à l'application d'une règlementation nationale qui, à l'instar 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'inspection d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID19 se fondant sur une base de données auprès de Sciensano :

1° centralise les données auprès d'un seul opérateur public;

2° ne distingue pas les données collectées et les bases de données dans lesquelles elles sont enregistrées en fonction des différentes finalités poursuivies par cette collecte de données;

3° organise la collecte des données concernant les personnes présumées infectées suivant les modalités que cette réglementation nationale précise;

4° organise la collecte des données concernant les ‘ contacts ’ des personnes (présumées) infectées (personne de catégorie IV) suivant les modalités que cette réglementation nationale précise;

5° fait le choix d’une pseudonymisation (et non d’une anonymisation) des données traitées à des fins de recherche;

6° autorise que le ‘ Comité de sécurité de l’information ’ détermine les éléments essentiels liés au transfert de données à des tiers, tels que l’identité du responsable du traitement, les catégories de personnes concernées et la nature exacte des données pouvant être communiquées;

7° autorise que le médecin traitant soit informé du test visé sans l’accord de la personne concernée ? ».

A.4.1. Les autorités défenderesses soulèvent l’irrecevabilité du moyen unique en ce qu’il serait exclusivement dirigé contre l’accord de coopération du 25 août 2020. Elles se réfèrent à l’arrêt n° 171/2015. Selon les autorités défenderesses, le moyen unique serait par ailleurs irrecevable à défaut d’exposé, en ce qu’il vise la violation de l’article 7 de la Charte des droits fondamentaux de l’Union européenne et des articles 4, point 7), 35 et 36 du RGPD. Enfin, le moyen unique serait irrecevable en ce qu’il est pris de la violation des articles 10 et 11 de la Constitution, à défaut de préciser la différence de traitement contestée et les catégories de personnes à comparer.

A.4.2. À titre principal, les autorités défenderesses soutiennent que le moyen unique est non fondé. À titre subsidiaire, elles soutiennent que seule une annulation partielle des actes attaqués pourrait intervenir, dès lors qu’aucune critique n’est formulée contre les articles 1, 4, 5, 10, 13 et 16 à 19 de l’accord de coopération du 25 août 2020. À titre infiniment subsidiaire, les autorités défenderesses demandent, en cas d’annulation, le maintien des effets des actes attaqués « de façon définitive pour l’ensemble de la période comprise entre le 4 mai 2020 et la publication de l’arrêté royal proclamant la fin de l’épidémie du coronavirus COVID-19 ou à tout le moins jusqu’à l’adoption d’un nouvel accord de coopération et à son assentiment, sans préjudice du maintien des effets des mesures visées par l’accord de coopération pour le futur conformément à l’article 15 et 19 de l’accord de coopération ». Elles font valoir que le suivi des contacts est l’un des moyens les plus efficaces pour lutter contre la propagation d’une maladie contagieuse telle que le COVID-19. Elles exposent que la détection précoce des personnes qui ont été en contact avec des personnes infectées par cette maladie ou sérieusement suspectées d’en être infectées est primordiale pour pouvoir formuler les recommandations nécessaires, pour éviter la recrudescence de la maladie ainsi que des mesures de confinement plus attentatoires aux droits et libertés, pour adopter des décisions adaptées à l’ampleur de la crise sanitaire, pour faciliter les avancées de la recherche scientifique concernant une maladie encore largement méconnue et pour assurer la continuité de la politique de lutte contre celle-ci. Se référant sur ce dernier point aux recommandations formulées par le Centre européen de prévention et de contrôle dans son rapport du 21 juin 2021, les autorités défenderesses observent que l’arrêt soudain de la politique belge en matière de traçage de contacts pourrait mettre en péril l’ensemble de la politique de l’Union européenne de lutte contre le virus.

Les autorités défenderesses soutiennent également qu’une annulation non modulée créerait un vide juridique qui serait source d’insécurité juridique et exposerait les personnes visées par l’accord de coopération du 25 août 2020 à des risques de poursuites pour violation du secret professionnel. Se référant aux arrêts de la Cour n^{os} 1/2005, 134/2012 et 66/2013, les autorités défenderesses ajoutent qu’une annulation non modulée entraînerait une charge administrative et judiciaire intenable pour les administrations ainsi que la remise en cause des nombreuses décisions et contrats visant à mettre en œuvre le traçage des contacts. Selon les autorités défenderesses, il ressort des délais de suppression des données visés à l’article 15 de l’accord de coopération du 25 août 2020 qu’une annulation des actes attaqués ne peut produire aucun effet utile, dès lors que les mesures de l’accord de coopération auront déjà été consommées. Les autorités défenderesses soutiennent que, comme la Cour l’a déjà jugé par son

arrêt n° 104/2006 du 21 juin 2006, l'épuisement des effets d'une disposition transitoire peut conduire au maintien des effets pour la période considérée. Enfin, elles exposent que les parties requérantes n'ont pas demandé la suspension des actes attaqués et qu'une annulation de ceux-ci causerait des désagréments incommensurables pour les administrations et entités concernées mais n'apporterait qu'un avantage purement théorique aux parties requérantes.

Les autorités défenderesses exposent que le système d'une base de données centralisée sert de support aux accords de coopération du 14 juillet 2021 et du 27 septembre 2021 ainsi qu'aux accords de coopération d'exécution du 14 juillet 2021, du 23 juillet 2021, du 20 septembre 2021 et du 27 septembre 2021 « 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 ». Elles soulignent que l'annulation des actes attaqués aura des conséquences indésirables sur la stratégie de vaccination et de suivi des contacts, sur le certificat COVID numérique de l'Union européenne et sur le COVID Safe Ticket. Tant que ces deux derniers outils sont utilisés, les résultats des vaccinations et des tests doivent rester accessibles sur le plan financier et organisationnel. Elles ajoutent que la base de données centralisée est déjà appliquée par le secteur concerné et qu'elle est connue du grand public.

En ce qui concerne la création de la base de données I auprès de Sciensano (article 2 de l'accord de coopération du 25 août 2020)

A.5.1. Dans la première branche du moyen unique, les parties requérantes font valoir que l'article 2 de l'accord de coopération du 25 août 2020 est contraire aux principes de légalité, de prévisibilité, de nécessité et de proportionnalité en ce qu'il prévoit la centralisation de données médicales sensibles auprès de Sciensano, alors qu'il existe d'autres moyens moins intrusifs d'atteindre l'objectif poursuivi, tels que la fourniture, par les centres de contacts, des données nécessaires aux acteurs chargés de la recherche scientifique. Les parties requérantes se réfèrent aux avis de l'Autorité de protection des données n^{os} 34/2020 et 42/2020.

A.5.2. Les parties requérantes dans les affaires n^{os} 7555, 7556, 7558, 7559 et 7560 soutiennent que la communauté scientifique conteste la nécessité et l'efficacité d'une centralisation des données. Elles se réfèrent à la recommandation (UE) n° 2020/518 de la Commission européenne du 8 avril 2020 « concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées », au règlement (UE) n° 2021/953 du Parlement européen et du Conseil du 14 juin 2021 « relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19 », aux avis n^{os} 36/2020 et 138/2020 de l'Autorité de protection des données et à des sites internet.

A.6.1. Les autorités défenderesses soutiennent que le grief pris de la violation des principes de légalité et de prévisibilité n'est pas fondé, à défaut d'exposé. Elles font valoir que la création d'une base de données centrale auprès de Sciensano est nécessaire et proportionnée au regard des objectifs de protection des données, de sécurité et de maniabilité. Premièrement, un système décentralisé nécessiterait des mesures de protection différenciées et il serait inadapté à la mobilité du citoyen. Il entraînerait des problèmes logistiques et de protection des données et il ralentirait le traçage des contacts, au détriment de la lutte contre la propagation du virus. Deuxièmement, l'avis de l'Autorité de protection des données n° 42/2020 portait sur l'arrêté royal n° 44 du 26 juin 2020, et non sur l'accord de coopération du 25 août 2020. Dans son avis n° 64/2020 du 20 juillet 2020, l'Autorité de protection des données a confirmé la nécessité et la proportionnalité de la création d'une base de données centrale auprès de Sciensano. Troisièmement, les parties requérantes sous-estiment les répercussions de la crise sanitaire et les risques de fuites de données qui sont inhérents à un système décentralisé. Si les centres de contact devaient fournir eux-mêmes les données nécessaires aux acteurs de la recherche scientifique, cela entraînerait un énorme surplus de travail pour ces centres au détriment de l'accomplissement de leur mission d'information. La transmission et le traitement continus de données sensibles sur différentes banques de données entraîneraient par ailleurs un risque important en matière de sécurité de l'information et de fuites des données. À l'inverse, une base de données centrale contribue à respecter le principe de minimisation des données et à un traçage manuel des contacts plus sûr et plus efficace.

A.6.2. En réponse aux questions posées par la Cour dans son ordonnance du 18 mai 2022, les autorités défenderesses indiquent que la base de données I contient les données nécessaires à la mise en œuvre de la politique de traçage, de testing, d'isolement et de quarantaine. Il s'agit des données à caractère personnel relatives aux personnes de catégories I à IV. La base de données I est mise à jour continuellement. La base de données III contient uniquement les données qui sont nécessaires aux collaborateurs des centres de contact et aux enquêteurs de terrain pour effectuer le traçage des contacts. Ces données sont reprises dans la base de données III sur une base temporaire puisqu'elles sont effacées chaque jour.

En réponse à la première question, les autorités défenderesses exposent que, premièrement, l'article 6, § 5, de l'accord de coopération du 25 août 2020 prévoit que les données émanant notamment des hôpitaux et de Sciensano sont fournies à la base de données I. Deuxièmement, l'article 6, § 6, prévoit que les données collectées par les centres de contact dans la base de données III retournent à la base de données I. Troisièmement, l'article 7 régit aussi l'échange de données entre la base de données I et la base de données III. Quatrièmement, l'article 10 prévoit que les centres de contact d'une entité fédérée peuvent contacter les citoyens qui y sont domiciliés. Cinquièmement, l'échange de données entre la base de données I et la base de données III est justifié, d'une part, par le fait que les centres de contact n'ont pas besoin d'avoir accès à toutes les données de la base de données I pour effectuer le traçage manuel des contacts et, d'autre part, par le fait que les données enregistrées dans la base de données III doivent pouvoir être attribuées, dans la base de données I, à la bonne personne. Les informations introduites par les centres de contact dans la base de données III sont utilisées pour mettre à jour la base de données I. Elles permettent de faire le suivi des personnes qui ont déjà été contactées par les centres de contact et de celles qui doivent encore l'être.

En réponse à la deuxième question, les autorités défenderesses exposent que les données visées à l'article 6, §§ 5 et 6, de l'accord de coopération sont les données qui sont collectées par les centres de contact et enregistrées dans la base de données III et qui sont automatiquement enregistrées dans la base de données I. Les centres de contact n'enregistrent jamais directement des données dans la base de données I car ils n'y ont pas accès. Ils peuvent uniquement consulter les données qui leur sont nécessaires dans la base de données III.

En réponse à la troisième question, les autorités défenderesses indiquent que les personnes de catégories V et/ou VI « visées à l'article 6 » de l'accord de coopération sont le médecin traitant et le médecin de référence dont les données à caractère personnel sont traitées dans la base de données I.

En ce qui concerne la nécessité de collecter certaines catégories de données (articles 6 à 9 de l'accord de coopération du 25 août 2020)

A.7. Dans la deuxième branche du moyen unique, les parties requérantes soutiennent que les articles 6 à 9 de l'accord de coopération du 25 août 2020 ne satisfont pas aux principes et dispositions visés dans le moyen, en ce que (1) les données collectées et les bases de données dans lesquelles elles sont enregistrées ne sont pas distinguées en fonction des finalités poursuivies, (2) la collecte des données concernant les personnes présumées infectées (personnes de catégorie III) et les personnes en contact avec une personne infectée ou avec une personne présumée infectée (personnes de catégorie IV) n'est pas nécessaire ni proportionnée, (3) le choix de pseudonymiser les données traitées à des fins de recherche scientifique n'est pas justifié et (4) certains concepts ne sont pas suffisamment clairs. Les parties requérantes se réfèrent à l'avis n° 64/2020 de l'Autorité de protection des données.

1. La nécessité de distinguer les données et les bases de données selon la finalité poursuivie

A.8. Les parties requérantes font valoir que le numéro d'identification de sécurité sociale, le registre national, les résultats du « CT-scan » et la langue de la personne concernée ne sont pas nécessaires au regard de l'objectif poursuivi. Puisque les centres de contacts ont accès au numéro d'identification de sécurité sociale et aux informations contenues dans le registre national, la finalité d'identifier la personne concernée peut être atteinte sans enregistrer ces informations dans la base de données I. Le traitement du numéro d'identification de sécurité sociale entraîne une ingérence particulièrement grave dans le droit au respect de la vie privée des personnes concernées en raison des informations sensibles qu'il contient. Le traitement des résultats du « CT-scan » poursuit une finalité de recherche scientifique. Il n'est ni nécessaire ni proportionné à la finalité de traçage des contacts. Enfin, l'enregistrement de la langue des personnes concernées dans la banque de données I n'apparaît pas

nécessaire dès lors qu'il est possible de diriger automatiquement les personnes concernées vers un interlocuteur qui parle leur langue via un choix de langue automatique proposé au début du contact téléphonique.

A.9. Les autorités défenderesses soutiennent, premièrement, que la recherche scientifique n'est pas une finalité en soi de l'accord de coopération du 25 août 2020, lequel a pour unique finalité de « régler le flux de données entre les bases de données I et II afin de faciliter la recherche scientifique ». Deuxièmement, le fait de distinguer les bases de données selon la finalité de la collecte conduirait à un système décentralisé qui entraînerait une charge administrative supplémentaire pour les prestataires de soins de santé et des risques en matière de sécurité. Les données devraient en effet être scindées par les prestataires de soins de santé, avant leur enregistrement, selon la finalité de leur collecte. Ces prestataires de soins de santé devraient également anonymiser ou pseudonymiser les données destinées à la recherche scientifique avant que celles-ci soient incluses dans la base de données y relative. Troisièmement, la pseudonymisation des données destinées à la recherche scientifique depuis la base de données I avant leur partage avec la base de données II, et non avant leur enregistrement dans la base de données I, permet de ne pas alourdir la charge administrative des médecins et de confier la pseudonymisation des données à la plateforme eHealth qui dispose de l'expertise requise. Quatrièmement, la collecte du numéro d'identification de sécurité sociale et l'accès au registre national sont nécessaires en vue de l'identification univoque des personnes concernées. Les autorités défenderesses se réfèrent à l'exposé général de l'accord de coopération du 25 août 2020 et à l'arrêt n° 29/2010 du 18 mars 2010. Elles soulignent que l'accès des centres de contact au numéro d'identification de sécurité sociale et au registre national découle précisément de l'inscription de ces informations dans la base de données I, qui alimente la base de données III à laquelle ces centres ont accès. Cinquièmement, l'utilisation ultérieure des « CT-scans » à des fins de recherche scientifique ne signifie pas que l'enregistrement de ces données n'est pas nécessaire ni proportionné. Sixièmement, l'enregistrement de la langue des personnes concernées est un élément essentiel du traçage des contacts. Le système proposé par les parties requérantes n'est pas envisageable, dès lors que c'est le centre de contact qui appelle la personne concernée et non l'inverse.

2. Le traitement des données concernant les personnes présumées infectées et les personnes en contact avec une personne infectée ou avec une personne présumée infectée

A.10. Selon les parties requérantes, le traitement des données concernant les personnes présumées infectées (personnes de catégorie III) poursuit une finalité de recherche scientifique. Il n'est ni nécessaire ni proportionné à la finalité de traçage des contacts. Le traitement des données concernant les personnes en contact avec une personne infectée ou avec une personne présumée infectée (personnes de catégorie IV) n'est pas non plus nécessaire ni proportionné.

A.11. Se référant à l'exposé général de l'accord de coopération du 25 août 2020, les autorités défenderesses soutiennent que le traitement des données des personnes présumées infectées est nécessaire et proportionné. Il s'agit d'un diagnostic présumé posé par un médecin sur la base d'un examen médical qui constitue une donnée exacte au sens de l'article 5, paragraphe 1, point d), du RGPD. Les autorités défenderesses ajoutent qu'en vertu de l'article 3, § 2, du même accord de coopération, les données des personnes présumées infectées servent au traçage des contacts et non à la recherche scientifique.

Selon les autorités défenderesses, le traitement des données concernant les personnes en contact avec une personne infectée ou avec une personne présumée infectée est également nécessaire et proportionné. Premièrement, l'avis n° 64/2020 de l'Autorité de protection des données concerne le projet d'accord de coopération. Deuxièmement, la collecte de la date de naissance de ces personnes résulte de la collecte du numéro d'identification de sécurité sociale, et sa finalité ressort de l'exposé général de l'accord de coopération du 25 août 2020. Troisièmement, il ressort de l'article 6, § 5, 7°, de cet accord de coopération que « les données nécessaires permettant au centre de contact de prendre tout contact utile » englobent le code postal et la langue. Quatrièmement, il ressort de l'exposé général du même accord de coopération que la prise de contact ne s'étend pas aux contacts des personnes en contact avec une personne infectée ou avec une personne présumée infectée. Cinquièmement, l'enregistrement du refus de voir un médecin a également été justifié dans cet exposé général.

3. Le choix de pseudonymiser les données traitées à des fins de recherche scientifique

A.12. Les parties requérantes soutiennent que le législateur ne justifie pas la nécessité de pseudonymiser les données traitées à des fins de recherche scientifique et que l'anonymisation entraînerait moins de risque de réidentification.

A.13. Les autorités défenderesses font valoir que, dans son avis n° 64/2020, l'Autorité de protection des données n'a pas dénoncé l'absence de justification quant au choix de la pseudonymisation. Elles soutiennent que ce choix est justifié dans l'exposé général de l'accord de coopération du 25 août 2020 et que l'anonymisation complète rendrait impossible toute recherche de contact.

4. L'absence de clarté de certains concepts

A.14. Les parties requérantes se réfèrent à l'avis n° 64/2020 dans lequel l'Autorité de protection des données s'interroge sur la portée des termes « le numéro d'identification provenant d'une source authentique » et « personne à contacter en cas d'urgence ».

A.15. Les autorités défenderesses exposent qu'à la suite de cet avis, ces notions ont été clarifiées à l'article 8, § 1er, 1°, de l'accord de coopération du 25 août 2020 et dans son exposé général.

En ce qui concerne l'habilitation conférée au Comité de sécurité de l'information d'autoriser la communication de données à caractère personnel à des tiers (articles 11 et 12 de l'accord de coopération du 25 août 2020)

A.16. Dans la troisième branche du moyen unique, les parties requérantes font valoir que les articles 11 et 12 de l'accord de coopération du 25 août 2020 violent les dispositions et principes visés dans le moyen en habilitant le Comité de sécurité de l'information à déterminer les éléments essentiels liés à la communication de données à des tiers, tels que l'identité du responsable du traitement, les catégories de personnes concernées et la nature exacte des données pouvant être communiquées. Elles font valoir que le Comité de sécurité de l'information ne peut pas être considéré comme une autorité de contrôle au sens de l'article 51 du RGPD et que la compétence d'autorisation de ce Comité ne peut dès lors pas être justifiée sur la base de l'article 36, paragraphes 4 et 5, du RGPD. Elles se réfèrent aux critiques formulées par la section de législation du Conseil d'État.

A.17. Selon les autorités défenderesses, les parties requérantes n'exposent pas concrètement en quoi les compétences du Comité de sécurité de l'information violeraient le RGPD. Se référant à l'exposé général de l'accord de coopération du 25 août 2020 et à 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 », les autorités défenderesses exposent que le Comité de sécurité de l'information est un organe indépendant qui est chargé d'autoriser la communication de données à caractère personnel dans le secteur social et des soins de santé et de promouvoir la protection des données et la sécurité de l'information, et non une autorité de contrôle au sens de l'article 51 du RGPD. La compétence du Comité de sécurité de l'information d'accepter ou de refuser des échanges de données par voie de délibération favorise le respect du droit à la vie privée puisqu'elle permet d'effectuer un contrôle préventif préalable à l'échange de données afin de garantir un échange de données licite et correct. Cette compétence ne porte pas préjudice à celles de l'Autorité de la protection des données, qui peut demander au Comité de sécurité de l'information de reconsidérer sa décision en cas de non-respect des normes juridiques supérieures. En se fondant sur les articles 6, paragraphe 2, et 9, paragraphe 4, du RGPD, les autorités défenderesses soutiennent que l'article 36 du même règlement n'exclut pas qu'un contrôle préalable soit effectué par une instance autre que l'autorité de contrôle. Elles soutiennent que les observations de la section de législation du Conseil d'État ont été prises en compte dans les articles 11 et 12 de l'accord de coopération du 25 août 2020. Elles font valoir que les compétences du Comité de sécurité de l'information ne concernent pas des éléments essentiels du traitement tels que les instituts susceptibles de relever de la collectivité, les « informateurs » qui sont tenus de communiquer des données à Sciensano ou les catégories de données qui sont traitées dans les bases de

données I à IV. Ces éléments doivent être déterminés par un accord de coopération d'exécution. Le rôle du Comité de sécurité de l'information garantit la flexibilité nécessaire à l'adoption de mesures efficaces et adaptées à la réalité évolutive de la lutte contre le virus. Les autorités défenderesses concluent que les articles 11, alinéa 3, et 12, alinéa 1er, de l'accord de coopération du 25 août 2020 ne règlent pas des éléments essentiels du traitement des données à caractère personnel.

En ce qui concerne l'information fournie par les centres de contacts aux médecins traitants (article 3, § 1er, 2°, B, de l'accord de coopération du 25 août 2020)

A.18. Dans la quatrième branche du moyen unique, les parties requérantes font valoir que l'article 3, § 1er, 2°, B, de l'accord de coopération du 25 août 2020 viole l'article 5, paragraphe 1, point b), du RGPD et l'article 22 de la Constitution en ce qu'il prévoit que les médecins traitants sont informés de la condition médicale des personnes qui ont peut-être été contaminées, des personnes qui ont réalisé un test de dépistage (personnes de catégorie II) et des personnes présumées infectées (personnes de catégorie III) sans le consentement des personnes concernées.

A.19. À titre principal, les autorités défenderesses soutiennent que la quatrième branche du moyen unique repose sur une lecture erronée de l'article 3, § 1er, 2°, B, de l'accord de coopération du 25 août 2020. Cette disposition prévoit uniquement que les médecins de référence (personnes de catégorie VI), et non les médecins traitants (personnes de catégorie V), peuvent être contactés par les centres de contact afin d'être informés de la contamination présumée. L'accord de coopération a été modifié sur ce point après l'avis de l'Autorité de protection des données.

À titre subsidiaire, les autorités défenderesses soutiennent que les finalités du traitement visé à l'article 3, § 1er, 2°, B, de l'accord de coopération du 25 août 2020 sont déterminées et explicites, conformément au principe de limitation des finalités.

En ce qui concerne la finalité de recherche scientifique (article 3, § 1er, 4°, de l'accord de coopération du 25 août 2020)

A.20. Dans la cinquième branche du moyen unique, les parties requérantes soutiennent que l'article 3, § 1, 4°, de l'accord de coopération du 25 août 2020 viole le principe de finalité, en ce que la finalité de recherche scientifique devrait être considérée comme un traitement ultérieur de données, et non comme une finalité primaire, dès lors que les données sont collectées initialement à d'autres fins. La distinction entre une recherche scientifique fondée sur l'utilisation primaire ou secondaire de données de santé a une incidence sur la base juridique du traitement et sur le principe de minimisation des données. Elles se réfèrent aux avis n° 42/2020 et n° 43/2020 de l'Autorité de protection des données.

Quant à la base juridique du traitement, les parties requérantes soutiennent qu'à défaut de demander le consentement des personnes concernées conformément à l'article 6, paragraphe 1, point a), et à l'article 9, paragraphe 2, point a), du RGPD, l'article 3, § 3, de l'accord de coopération du 25 août 2020 viole l'article 6, paragraphe 1, point e), du RGDP.

Quant au principe de minimisation des données, les parties requérantes font valoir qu'en faisant de la finalité de recherche scientifique une finalité primaire au même titre que les finalités de « recherche de contacts » et de « prévention de l'extension des effets néfastes causés par les maladies infectieuses », le responsable du traitement peut traiter davantage de données, ce qui est contraire à l'article 5, paragraphe 1, point b), du RGPD.

A.21. Les autorités défenderesses font valoir, premièrement, qu'un traitement ultérieur est un traitement pour une finalité qui n'avait pas été envisagée au départ et à propos de laquelle les personnes concernées, non informées de manière adéquate, doivent être informées (article 13, paragraphe 3, du RGPD). Deuxièmement, si la finalité du traitement secondaire est compatible avec celle du traitement primaire, le traitement peut s'appuyer sur la base juridique de la finalité du traitement primaire (article 6, paragraphe 4, du RGPD). Troisièmement, l'article 3, § 1er, 4°, de l'accord de coopération du 25 août 2020 prévoit uniquement de faciliter la recherche scientifique afin de permettre un traitement secondaire de données pour la recherche scientifique, sans faire de la recherche scientifique

une finalité en soi. La finalité primaire consiste en la gestion des flux de données entre les bases de données I et II afin de permettre la recherche scientifique. Cette finalité figurant dans l'accord de coopération, elle ne saurait être considérée comme une finalité autre que celle pour laquelle les données ont été collectées. L'Autorité de protection des données n'a d'ailleurs émis aucune réserve sur ce point dans son avis n° 64/2020. Quatrièmement, les traitements aux fins de recherche scientifique sont conformes au principe de minimisation des données puisque seules les données pseudonymisées sont échangées avec la base de données II. Selon les autorités défenderesses, le principe de minimisation des données doit toujours être évalué à la lumière de la recherche spécifique envisagée et les données qui peuvent être utilisées ou non dans le cadre de la finalité de recherche scientifique ne peuvent pas être délimitées *a priori*.

En ce qui concerne les liens entre la base de données I et la base de données V et la notion de « contacts à risque » (article 14 de l'accord de coopération du 25 août 2020)

A.22. Dans les sixième et septième branches du moyen unique, les parties requérantes font valoir que l'article 14 de l'accord de coopération du 25 août 2020 est contraire aux dispositions et principes visés dans le moyen en ce qu'il ne limite pas l'utilisation des données contenues dans la base de données I au suivi manuel des contacts et en ce qu'il ne définit pas la notion de « contacts à risque ». Elles font référence à l'avis n° 43/2020 de l'Autorité de protection des données.

A.23. Selon les autorités défenderesses, la sixième branche du moyen unique repose sur des textes antérieurs à celui de l'accord de coopération du 25 août 2020 et sur une mauvaise compréhension des différentes bases de données. Elles exposent que les données de contact et de santé de personnes présumées infectées collectées dans la base de données I sont traitées par les hôpitaux, les laboratoires et les collaborateurs du centre de contact. La base de données I alimente les bases de données II, III et VI. La base de données V contient les données du journal des enregistrements de l'application numérique de traçage des contacts, les données de contamination et la date probable de la contamination, sans identifier l'utilisateur. Aucune donnée de la base de données I n'est transférée directement vers la base de données V. La séparation des banques de données I et V est assurée à la fois par des mesures techniques et organisationnelles prises par Sciensano et par la création de la banque de données VI. Créée par l'accord de coopération d'exécution du 13 octobre 2020 entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92*bis*, § 1er, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980 (ci-après : l'accord de coopération d'exécution du 13 octobre 2020), la base de données VI permet de sécuriser l'authentification du statut d'infection.

Selon les autorités défenderesses, la septième branche du moyen unique repose sur une lecture erronée de l'article 14, § 9, 2°, de l'accord de coopération du 25 août 2020. Conformément à cette disposition, la notion de « contact à risque » a été définie à l'article 1er, 10°, de l'accord de coopération d'exécution du 13 octobre 2020.

En ce qui concerne la notion de « visite physique » (article 3 de l'accord de coopération du 25 août 2020)

A.24. Dans la huitième branche du moyen unique, les parties requérantes font valoir que l'article 3, § 1er, 2°, A, et § 2, 2°, A, de l'accord de coopération du 25 août 2020 ne satisfait pas au principe de finalité en ce qu'il ne définit pas la notion de « visite physique ». Elles font référence à l'avis n° 64/2020 de l'Autorité de protection des données.

A.25. Se référant à l'exposé général de l'accord de coopération, les autorités défenderesses soutiennent que les règles spécifiques relatives à la mise en œuvre du traçage, dont celles relatives aux visites à domicile, relèvent de la compétence des entités fédérées. Il ressort de l'article 1er, § 1er, 20°, de l'accord de coopération du 25 août 2020 et de son exposé général que les visites physiques peuvent être effectuées par les collaborateurs du centre de contact lorsque le contact téléphonique ou par courrier électronique est impossible. Il ressort par ailleurs de l'article 3, § 2, du même accord de coopération que ces trois modalités de contact poursuivent des finalités identiques et que le centre de contact ne peut traiter les données obtenues dans le cadre d'une visite domiciliaire qu'aux fins définies par cette disposition. Les autorités défenderesses exposent qu'à la suite de l'avis n° 64/2020

de l'Autorité de protection de données, les termes « entre autres » ont été supprimés et le terme « suivi » a été défini dans l'exposé général de l'accord de coopération. Selon les autorités défenderesses, le principe de transparence visé à l'article 12 du RGPD n'oblige pas à définir les circonstances spécifiques du traitement dans un instrument législatif. En se fondant sur l'article 16 de l'accord de coopération du 25 août 2020 et à son exposé général, les autorités défenderesses concluent que la personne concernée est informée de manière transparente du traitement de ses données à caractère personnel pendant la prise de contact et par le site web http://corona-tracking.info.

En ce qui concerne l'obligation de secret des collaborateurs des centres de contact

A.26. Dans la neuvième branche du moyen unique, les parties requérantes soutiennent qu'en omettant de prévoir que les collaborateurs des centres de contact sont soumis au secret professionnel, l'accord de coopération du 25 août 2020 est contraire à l'article 9, paragraphe 2, point i), du RGPD. Elles se réfèrent aux avis n^{os} 34/2020 et 64/2020 de l'Autorité de protection des données.

A.27. Les autorités défenderesses soutiennent que la soumission des collaborateurs des centres de contact au secret professionnel relève de la compétence des entités fédérées et est réglée, respectivement, par l'article 3, alinéa 3, du décret de la Communauté flamande du 29 mai 2020 « portant organisation du suivi des contacts centralisé par une structure de coopération de partenaires externes, du suivi des contacts local par les administrations locales ou les conseils des soins et portant organisation des équipes COVID-19 dans le cadre du COVID-19 », par l'article 5 de l'arrêté du Gouvernement wallon de pouvoirs spéciaux n° 35 du 5 mai 2020 « organisant le tracing socio-sanitaire dans le cadre de la lutte contre l'épidémie COVID-19 », par l'article 10.18 du décret de la Communauté germanophone du 1er juin 2004 « relatif à la promotion de la santé et à la prévention médicale » et par l'article 4, § 2, de l'arrêté de pouvoirs spéciaux du Collège réuni de la Commission communautaire commune n° 2020/006 du 18 juin 2020 « organisant le suivi sanitaire des contacts dans le cadre de la lutte contre la pandémie COVID-19 ».

En ce qui concerne la durée de conservation des données enregistrées dans la base de données II (article 15 de l'accord de coopération du 25 août 2020)

A.28. Dans la dixième branche du moyen unique, les parties requérantes reprochent à l'article 15 de l'accord de coopération de ne pas préciser la durée de conservation des données pseudonymisées qui sont enregistrées dans la base de données II.

A.29. Les autorités défenderesses exposent qu'à la suite de l'avis n° 64/2020 de l'Autorité de protection des données, un délai de conservation de trente ans concernant ces données a été prévu à l'article 15, § 2, de l'accord de coopération du 25 août 2020. Elles ajoutent que ce délai est proportionné aux finalités poursuivies puisqu'il correspond au délai généralement accepté pour la conservation de données de santé à des fins de recherche scientifique.

- B -

Quant au contexte des actes attaqués

B.1.1. Les parties requérantes demandent l'annulation du décret de la Région wallonne du 30 septembre 2020 (affaire n° 7555), de l'ordonnance de la Commission communautaire commune du 1er octobre 2020 (affaire n° 7559), du décret de la Communauté flamande du 2 octobre 2020 (affaire n° 7560), de l'article 2 de la loi du 9 octobre 2020 (affaires n^{os} 7557 et 7558) et du décret de la Communauté germanophone du 12 octobre 2020 (affaire n° 7556)

« 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'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 » (ci-après : l'accord de coopération du 25 août 2020).

Par cet accord de coopération, l'autorité fédérale, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune conviennent de créer plusieurs bases de données en vue d'organiser le traçage manuel et le traçage numérique des personnes infectées par le COVID-19, des personnes présumées l'être et de leurs contacts, afin de limiter la propagation du virus.

B.1.2. La section de législation du Conseil d'État a, dans son avis n° 67.719/VR du 15 juillet 2020 sur l'avant-projet de loi devenu la loi attaquée du 9 octobre 2020, décrit le projet d'accord de coopération. Cette description est applicable par analogie au texte définitif de l'accord de coopération, moyennant certaines adaptations indiquées entre crochets :

« 5.1. L'accord de coopération crée auprès de Sciensano quatre bases de données (Bases de données I, III, IV et V), à côté de la base de données existante, dont les modalités sont définies au regard de la lutte contre le COVID-19 (Base de données II). L'article 1er, § 1er, [6° à 10°], de l'accord de coopération décrit ces cinq bases de données.

- La Base de données I est la base de données centrale générale créée auprès de Sciensano pour le traitement et l'échange de données aux fins de traitement fixées dans l'accord de coopération. […]

- La Base de données II est la base de données existante auprès de Sciensano créée en exécution d'un accord de coopération [lire : une convention de collaboration] conclu avec l'Institut national d'assurance maladie-invalidité (ci-après : INAMI) […]. Les données […] doivent permettre aux institutions de recherche, dont Sciensano, d'effectuer des études scientifiques ou statistiques en rapport avec la propagation du coronavirus COVID-19 et de soutenir la politique de lutte contre le coronavirus par l'échange des données avec la Base de données I [article 1er, § 2, 3°].

- La Base de données III est la base de données [des instructions d'appel et des instructions] pour le personnel du centre de contact.

- La Base de données IV est la base de données contenant les coordonnées des collectivités.

- La Base de données V est le journal central des enregistrements qui permet de contrôler le fonctionnement de l'application numérique de traçage des contacts et qui, au sein de Sciensano, est séparée des Bases de données I et II. Une application numérique de traçage des contacts sur la base du DP3T se compose en effet d'une application mobile qui peut être, sur une base volontaire, installée et utilisée par l'utilisateur en local sur son appareil, et d'un journal central des enregistrements conservés dans la Base de données V [article 14, § 3, 1° et 2°, et § 5].

5.2. Le chapitre Ier de l'accord de coopération contient des dispositions générales. L'article 1er comporte un certain nombre de définitions (paragraphe 1er), mentionne les objectifs de l'accord de coopération (paragraphe 2), indique qu'il n'est pas porté préjudice à la réglementation des autorités compétentes en matière de suivi des contacts pour la détection des maladies contagieuses (paragraphe 3), requiert que les parties doivent prendre les mesures nécessaires à la mise en œuvre de l'accord de coopération et à l'harmonisation de leurs initiatives existantes avec cet accord (paragraphe 4), prévoit la possibilité d'accords de coopération d'exécution (paragraphe 5) et dispose que les prestataires des soins de santé et les personnes contactées sont relevées de leur secret professionnel (paragraphe 6). L'article 2 crée la Base de données I (paragraphe 1er), inscrit la Base de données II dans le cadre de cet accord de coopération (paragraphe 2), crée les Bases de données III et IV (paragraphe 3), désigne Sciensano comme responsable du traitement des Bases de données I et II (paragraphe 4) et dispose que les entités fédérées [ou leurs agences] désigneront les responsables du traitement des Bases de données III et IV (paragraphe 5).

Le chapitre II contient l'article 3, qui règle les finalités du traitement concernant la mise à disposition des données à caractère personnel par la Base de données I (paragraphe 1er), ainsi que le traitement des données à caractère personnel [par les entités fédérées] ou les agences compétentes (paragraphe 2) et par les équipes mobiles et les inspections d'hygiène des communautés (paragraphe 3). Une interdiction générale de traitement des données à caractère personnel à d'autres fins est énoncée (paragraphe 4).

Le chapitre III contient l'article 4, qui définit les catégories de personnes dont les données à caractère personnel sont traitées dans le cadre de l'accord de coopération à l'examen. Ces catégories sont définies à l'article 1er, § 1er, [13° à 18°].

- Personnes de catégorie I : les personnes pour lesquelles le médecin a prescrit un test de dépistage du COVlD-19;

- Personnes de catégorie II : les personnes qui ont été soumises à un test de dépistage du COVID-19;

- Personnes de catégorie III : les personnes [pour lesquelles] le médecin [a une présomption sérieuse qu'elles sont] infectées, sans qu'un test de dépistage du COVID-19 ait été effectué ou prescrit, ou dont le test de dépistage du COVID-19 a révélé qu'elles n'étaient pas infectées;

- Personnes de catégorie IV : les personnes avec lesquelles soit (i) les Personnes de catégorie II dans la mesure où le test de dépistage du COVID-19 a révélé qu'elles sont infectées, soit (ii) les Personnes de catégorie III ont été en contact pendant une période de quatorze jours avant et après les premiers signes d'infection;

- Personnes de catégorie V : les médecins traitants des Personnes de catégories I, II et III;

- Personnes de catégorie VI : le médecin de référence ou – en l'absence d'un médecin de référence au sein de la collectivité concernée – le responsable administratif des collectivités avec lesquelles les Personnes des catégories I, II et III ont été en contact pendant une période de quatorze jours avant et après les premiers symptômes de l'infection.

Le chapitre IV détermine les catégories de données à caractère personnel qui sont traitées dans le cadre de l'accord de coopération. L'article 5 prescrit que le traitement des données doit être effectué conformément au RGPD et à la loi du 30 juillet 2018 ' relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel '. L'article 6 requiert que les déclarations obligatoires en vertu de la réglementation communautaire soient faites auprès de la Base de données I (paragraphe 1er) et définit les catégories de données à caractère personnel qui sont traitées dans cette base de données, respectivement, pour les Personnes de catégorie I, les Personnes de catégorie II, les Personnes de catégorie III et les Personnes de catégorie IV (paragraphes 2 à 5). Les paragraphes 6 et 7 définissent les données à caractère personnel supplémentaires à traiter pour certaines catégories de personnes et de clusters, qui sont collectées ou fournies par [les centres de contact,] les équipes mobiles ou les inspections d'hygiène compétentes. L'article 7 définit les catégories de données à caractère personnel qui sont traitées dans la Base de données III, à savoir les données à caractère personnel qui sont communiquées par Sciensano à partir de la Base de données I aux centres de contact (paragraphe 1er), les données à caractère personnel pour la Base de données III en ce qui concerne les Personnes de catégorie II qui, après avoir effectué un test de dépistage du COVID-19, se sont avérées infectées, et les Personnes de catégorie III (paragraphe 2), les Personnes de catégorie IV (paragraphe 3) et les Personnes de catégorie VI (paragraphe 4). L'article 8 définit les catégories de données à caractère personnel qui sont traitées dans la Base de données IV en ce qui concerne les Personnes de catégorie V et de catégorie VI. L'article 9 définit les catégories de données à caractère personnel qui, après pseudonymisation, sont traitées dans la Base de données II en ce qui concerne les Personnes de catégorie I, de catégorie II et de catégorie III (paragraphe 1er) et les Personnes de catégorie IV (paragraphe 2).

Le chapitre V comporte l'article 10 qui règle l'accès aux données à caractère personnel par les centres de contact (paragraphe 1er) et par les équipes mobiles et les services d'inspection d'hygiène (paragraphe 2) ainsi que la transmission des données à caractère personnel, après pseudonymisation, de la Base de données I à la Base de données II (paragraphe 3).

Le chapitre VI concerne la compétence du Comité de sécurité de l'information. L'article 11 règle la délibération préalable, dans certains cas, au sein de ce comité (paragraphes 1er et 2) et la compétence de ce comité de préciser des données (paragraphe 3). Il est également prévu de régler certains aspects de l'accord de coopération dans un accord de coopération d'exécution

(paragraphe 4). L'article 12 définit les modalités que le Comité de sécurité de l'information peut fixer (paragraphe 1er) et règle l'accès au Registre national et aux registres de la Banque-carrefour de la sécurité sociale (paragraphe 2), ainsi que la délibération préalable au sein du Comité de sécurité de l'information pour la communication [à la Base de données I] de données à caractère personnel provenant d'autres sources authentiques […] (paragraphe 3).

Le chapitre VII contient l'article 13, qui concerne les mesures de sécurité que Sciensano [et les entités fédérées compétentes ou leurs agences doivent] prendre afin de garantir un niveau de sécurité adapté au risque.

Le chapitre VIII concerne les applications numériques de traçage des contacts. L'article 14 définit leur objectif (paragraphe 1er) et règle les limites du traitement des données à caractère personnel au moyen de ces applications (paragraphe 2), ainsi que les conditions minimales auxquelles ces applications doivent répondre (paragraphe 3). Celles-ci doivent respecter les principes énoncés [aux articles 5 et 25] du RGPD (paragraphe 4) et doivent se faire sur une base volontaire (paragraphe 5). Le délai de conservation des données relatives aux contacts est réglé (paragraphe 6), ainsi que les objectifs du traitement des données (paragraphe 7). Une analyse d'impact relative à la protection des données doit être établie et publiée (paragraphe 8). Il est également prévu de préciser certains aspects des applications numériques de traçage des contacts dans un accord de coopération d'exécution (paragraphe 9).

Le chapitre IX contient l'article 15, qui règle le délai de conservation maximal des données à caractère personnel pour les Bases de données I, III, IV et V (paragraphe 1er) et II (paragraphe 2).

Le chapitre X concerne la transparence et les droits des personnes concernées. L'article 16 énonce l'obligation pour Sciensano en tant que responsable du traitement de prendre des mesures appropriées en matière de communication des droits des personnes concernées (paragraphe 1er), créer et à assurer la maintenance d'un site internet (paragraphe 2), gérer et assurer la maintenance d'un système pour l'exercice des droits prévus dans le RGPD (paragraphe 3) et conclure un accord avec les [entités fédérées] et leurs agences en ce qui concerne leurs responsabilités en matière d'exercice des droits des personnes concernées et la fourniture d'informations (paragraphe 4).

Le chapitre [XI] contient diverses dispositions finales. L'article 17 organise le règlement des litiges entre les parties par une juridiction de coopération. L'article 18 charge la Conférence interministérielle Santé publique de surveiller la mise en œuvre et le respect des dispositions de l'accord de coopération, […] de proposer des adaptations [et d'exercer une fonction de médiation]. L'article 19 règle l'entrée en vigueur rétroactive de l'accord de coopération (paragraphe 1er) et prévoit [que ses mesures prennent fin le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie de COVID-19 (paragraphe 2) ainsi que] la possibilité de sa résiliation par un nouvel accord de coopération (paragraphe [3]) » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, pp. 31-35).

B.1.3. Conformément à son article 1er, § 2, l'accord de coopération du 25 août 2020 a pour triple objet (1) d'encadrer le suivi manuel des contacts et le déploiement des équipes mobiles, (2) d'encadrer le suivi numérique des contacts au moyen d'une application numérique

de traçage des contacts et (3) de permettre aux instituts de recherche et aux administrations, dont Sciensano, de mener des études scientifiques ou statistiques sur la lutte contre la propagation du COVID-19 et/ou de soutenir des politiques dans ce domaine.

Il ressort de l'exposé général de l'accord de coopération que le traçage numérique des contacts a vocation à compléter le suivi manuel (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, p. 72).

L'accord de coopération vise notamment à donner des recommandations aux personnes infectées par le COVID-19 et aux personnes potentiellement infectées ou présumées l'être, de façon à rompre la chaîne de contamination. Il ressort de l'article 1er, § 2, 1°, *f*, de l'accord de coopération que ces recommandations n'ont pas de caractère obligatoire pour les personnes concernées.

B.1.4. Avant l'accord de coopération du 25 août 2020, la création d'une banque de données visant à permettre le traçage manuel des contacts dans le cadre de la lutte contre le COVID-19 a été organisée par l'arrêté royal n° 18 du 4 mai 2020 « portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 » (ci-après : l'arrêté royal n° 18 du 4 mai 2020). D'une durée de validité fixée au départ jusqu'au 4 juin 2020 (article 6), cet arrêté a été prolongé jusqu'au 30 juin 2020 par l'article 2 de l'arrêté royal n° 25 du 28 mai 2020 « modifiant l'arrêté royal n° 18 du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 » (ci-après : l'arrêté royal n° 25 du 28 mai 2020).

Le 14 mai 2020, une proposition de loi « portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 » a été introduite à la Chambre avec le même objectif (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1249/001). Une seconde proposition de loi « relative à l'utilisation d'applications numériques de traçage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population », introduite la veille, visait, elle, à encadrer le traçage numérique des contacts au moyen d'applications numériques (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1251/001). Par ses avis n^{os} 67.425/3-67.426/3-67.427/3 et 67.424/3 du 26 mai 2020 rendus sur

ces deux propositions de lois, la section de législation du Conseil d'État a conclu à la nécessité de conclure un accord de coopération entre l'autorité fédérale et les communautés, compte tenu du lien étroit existant entre les compétences fédérales et les compétences communautaires concernées par les mesures envisagées (*Doc. parl*., Chambre, 2019-2020, DOC 55-1249/006, pp. 6-9; *Doc. parl*., Chambre, 2019-2020, DOC 55-1251/003, pp. 5-8). Elle a réitéré cette conclusion dans son avis n° 67.482/3 du 3 juin 2020 rendu à propos d'un amendement global à la première proposition de loi précitée qui visait à remplacer celle-ci (*Doc. Parl*., Chambre, 2019-2020, DOC 55-1249/009, pp. 5-7).

Le 25 juin 2020, le Comité de concertation a adopté le projet d'accord de coopération à l'origine de l'accord de coopération du 25 août 2020.

Dans l'attente de l'aboutissement des procédures législatives d'assentiment au projet d'accord de coopération, l'arrêté royal n° 44 du 26 juin 2020 « concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano » (ci-après : l'arrêté royal n° 44 du 26 juin 2020) a repris en substance le contenu du projet d'accord de coopération. Cet arrêté est entré en vigueur le 1er juillet 2020. Selon son article 17, il devait cesser ses effets le jour de l'entrée en vigueur de l'accord de coopération et, au plus tard, le 15 octobre 2020.

L'arrêté royal n° 18 du 4 mai 2020, l'arrêté royal n° 25 du 28 mai 2020 et l'arrêté royal n° 44 du 26 juin 2020 ont été retirés par les articles 3 à 5 de la loi attaquée du 9 octobre 2020.

B.1.5. Conformément à son article 19, § 1er, alinéa 1er, les dispositions de l'accord de coopération du 25 août 2020 correspondant en substance à celles de l'arrêté royal n° 18 du 4 mai 2020 sont entrées en vigueur rétroactivement à la date de l'entrée en vigueur de cet arrêté royal, le 4 mai 2020. Conformément à son article 19, § 1er, alinéa 2, l'article 14 de l'accord de coopération du 25 août 2020 et les dispositions du même accord de coopération relatives aux

applications numériques de traçage des contacts sont entrés en vigueur rétroactivement le 29 juin 2020 « en ce qui concerne les dispositions correspondant en substance à l'arrêté royal nº 44 du 26 juin 2020 ».

L'article 19, § 2, de l'accord de coopération du 25 août 2020 prévoit que, sous réserve de ce qui est dit dans son article 15, §§ 2 et 3, ses mesures prennent fin le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie de COVID-19.

Quant à l'intérêt des parties requérantes

B.2.1. Le Conseil des ministres, le Gouvernement wallon, le Gouvernement flamand, le Gouvernement de la Communauté germanophone et le Collège réuni de la Commission communautaire commune (ci-après : les autorités défenderesses) soutiennent que les recours en annulation sont irrecevables pour absence d'intérêt.

B.2.2. La Constitution et la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle 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 les actes attaqués.

B.2.3. Les deuxième à quatrième parties requérantes dans les affaires nos 7555, 7556, 7558, 7559 et 7560 invoquent leur qualité de personne physique à l'appui de leur intérêt.

Les actes attaqués portent assentiment à l'accord de coopération du 25 août 2020 qui crée un cadre juridique pour le traçage manuel et numérique des contacts des personnes infectées par le coronavirus en vue d'en éviter la propagation. Cet accord de coopération prévoit la collecte de nombreuses données à caractère personnel y compris des données sensibles concernant la santé relatives notamment aux personnes ayant été en contact avec une personne testée positive au coronavirus ou avec une personne présumée infectée.

Cet accord de coopération, tel qu'il a été approuvé par les actes attaqués, affecte donc directement et défavorablement la situation de toute personne physique se trouvant sur le territoire belge.

Un accord de coopération qui nécessite un assentiment législatif ne produit entièrement ses effets qu'après avoir reçu l'assentiment de l'ensemble des assemblées législatives concernées.

Les deuxième à quatrième parties requérantes dans les affaires n^{os} 7555, 7556, 7558, 7559 et 7560 justifient dès lors d'un intérêt à demander l'annulation de l'ensemble des actes d'assentiment à l'accord de coopération du 25 août 2020.

Il n'est pas nécessaire d'examiner l'intérêt de la première partie requérante dans ces affaires.

B.2.4. Le recours dans l'affaire n° 7557 porte sur l'article 2 de la loi du 9 octobre 2020 qui est aussi l'acte attaqué dans l'affaire n° 7558, et se fonde sur un moyen analogue à celui qui a été allégué dans cette affaire. Dès lors que les deuxième à quatrième parties requérantes dans l'affaire n° 7558 justifient d'un intérêt à l'annulation de l'article 2 de la loi du 9 octobre 2020, il n'est pas nécessaire d'examiner l'intérêt de la partie requérante dans l'affaire n° 7557.

B.2.5. L'exception est rejetée.

Quant à la recevabilité du moyen unique

B.3.1. Selon les autorités défenderesses, le moyen unique est irrecevable parce qu'il est en réalité uniquement dirigé contre l'accord de coopération du 25 août 2020.

B.3.2. La Cour est compétente pour statuer, par voie d'arrêt, sur les recours en annulation des lois, décrets et ordonnances. Entrent dans cette compétence les actes portant assentiment à un accord de coopération. La Cour n'est cependant pas compétente pour annuler un accord de coopération.

Les parties requérantes ne peuvent toutefois pas utilement attaquer, et la Cour contrôler, les actes portant assentiment à un accord de coopération sans impliquer dans leur critique ou dans leur examen le contenu des dispositions pertinentes de l'accord de coopération approuvé.

B.3.3. En ce qu'il est dirigé, formellement, contre les actes portant assentiment à l'accord de coopération du 25 août 2020 et, matériellement, contre les dispositions de cet accord de coopération, le moyen unique est recevable.

B.4.1. Les autorités défenderesses soutiennent que le moyen unique est irrecevable en ce qu'il est pris de la violation des articles 10 et 11 de la Constitution, à défaut pour les parties requérantes d'identifier les deux catégories de personnes que les actes attaqués traiteraient d'une manière discriminatoire.

B.4.2. Lorsqu'une violation du principe d'égalité et de non-discrimination est invoquée en combinaison avec un autre droit fondamental garanti par la Constitution ou par une disposition de droit international, ou découlant d'un principe général de droit, la catégorie des personnes à l'égard desquelles ce droit fondamental est violé doit être comparée à la catégorie des personnes auxquelles ce droit fondamental est garanti.

B.4.3. Dès lors que les articles 10 et 11 de la Constitution sont invoqués en combinaison avec plusieurs dispositions garantissant le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, l'exception est rejetée.

B.5.1. Dans l'affaire n° 7556, les autorités défenderesses soutiennent que le moyen unique est irrecevable en ce que les parties requérantes n'identifient pas la disposition du décret de la Communauté germanophone du 12 octobre 2020 dont elles demandent l'annulation.

Dans toutes les affaires, les autorités défenderesses soutiennent que le moyen unique est irrecevable en ce qu'il est pris de la violation de l'article 7 de la Charte des droits fondamentaux

de l'Union européenne (ci-après : la Charte) et des articles 4, point 7), 35 et 36 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). Selon elles, les parties requérantes négligent d'indiquer en quoi ces dispositions seraient violées.

B.5.2. L'article 6 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle dispose :

« La requête indique l'objet du recours et contient un exposé des faits et moyens ».

Pour satisfaire aux exigences de cette disposition, 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. Ces exigences sont dictées, d'une part, par la nécessité pour la Cour d'être à même de déterminer, dès le dépôt de la requête, la portée exacte du recours en annulation et, d'autre part, par le souci d'offrir aux autres parties au procès la possibilité de répliquer aux arguments des parties requérantes, de sorte qu'il est indispensable de disposer d'un exposé clair et univoque des moyens.

B.5.3. Il peut être déduit de la requête dans l'affaire n° 7556 que les parties requérantes dirigent uniquement leurs griefs contre l'article 1er du décret de la Communauté germanophone du 12 octobre 2020 en tant que cette disposition porte assentiment à l'accord de coopération du 25 août 2020. La Cour n'examine dès lors pas les autres dispositions de ce décret.

B.5.4. Les parties requérantes soutiennent que l'accord de coopération du 25 août 2020, tel qu'il a été approuvé par les actes attaqués, porte atteinte au droit au respect de la vie privée et au droit à la protection des données à caractère personnel garantis par l'article 22 de la

Constitution, par l'article 8 de la Convention européenne des droits de l'homme et par l'article 7 de la Charte, qui ont une portée analogue.

Le moyen unique est dès lors recevable.

B.5.5. L'article 4, point 7), du RGPD définit le responsable du traitement.

Lorsqu'elles critiquent, dans la première branche du moyen unique, la création de la base de données I auprès de Sciensano au motif, entre autres, que cette institution n'est pas chargée des opérations manuelles de traçage des contacts, les parties requérantes exposent en quoi l'article 4, point 7), du RGDP serait violé.

Le moyen unique est dès lors recevable.

B.5.6. Lorsque, dans la troisième branche du moyen unique, les parties requérantes observent que la compétence d'autorisation du Comité de sécurité de l'information ne saurait être justifiée sur la base de l'article 36, paragraphe 5, du RGPD, dès lors que ce Comité ne peut pas être considéré comme une autorité de contrôle, elles exposent en quoi cette disposition serait violée.

Les parties requérantes n'exposent en revanche pas en quoi l'article 36, paragraphe 4, du RGPD, qui concerne la consultation de l'autorité de contrôle dans le cadre de l'élaboration d'une proposition législative ou d'une mesure réglementaire, ni en quoi l'article 35 du RGPD et l'article 36, paragraphes 1 à 3, du RGPD, qui concernent l'analyse d'impact préalable des opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et la consultation préalable de l'autorité de contrôle dans ce cadre, seraient violés.

En ce qu'il est pris de la violation des articles 35 et 36, paragraphes 1 à 4, du RGPD, le moyen unique est irrecevable.

B.5.7. La reproduction, même intégrale, des avis d'une instance consultative ne satisfait pas aux exigences, précitées, de l'article 6 de la loi spéciale du 6 janvier 1989 sur la Cour

constitutionnelle. Les griefs développés dans la deuxième branche du moyen unique concernant la nécessité de distinguer les données et les bases de données selon la finalité poursuivie, la nécessité de la collecte dans la base de données I des données à caractère personnel relatives aux personnes de catégorie IV et l'absence de clarté de certains concepts sont dès lors irrecevables.

Quant au fond

B.6. Le moyen unique est pris de la violation des articles 10, 11 et 22 de la Constitution, lus en combinaison ou non avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte et avec les articles 4, point 7), 5, paragraphe 1, 6, 9, 14 et 36, paragraphe 5, du RGPD.

Les parties requérantes font essentiellement valoir que plusieurs dispositions de l'accord de coopération du 25 août 2020, telles qu'elles ont été approuvées par les actes attaqués, violent le droit au respect de la vie privée et le droit à la protection des données à caractère personnel.

B.7.1. 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.7.2. 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.7.3. 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.7.4. Le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelle et conventionnelle précitées, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée.

La proposition qui a précédé l'adoption de l'article 22 de la Constitution insistait sur « la protection de la personne, la reconnaissance de son identité, l'importance de son épanouissement et celui de sa famille », et elle soulignait la nécessité de protéger la vie privée et familiale « des risques d'ingérence que peuvent constituer, notamment par le biais de la modernisation constante des techniques de l'information, les mesures d'investigation, d'enquête et de contrôle menées par les pouvoirs publics et organismes privés, dans l'accomplissement de leurs fonctions ou de leurs activités » (*Doc. parl.*, Sénat, S.E. 1991-1992, n° 100-4/2°, p. 3). Cette proposition indiquait également que le législateur « ne pourrait en aucun cas vider de sa substance le droit au respect de la vie privée et familiale, sous peine d'enfreindre la règle constitutionnelle, en plus des règles internationales » (*ibid*.).

Le droit au respect de la vie privée a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles. 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*, §§ 47-48; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, §§ 66-68; 17 décembre 2009, *B.B. c. France*, § 57; 10 février 2011, *Dimitrov-Kazakov c. Bulgarie*, §§ 29-31; 18 octobre 2011,

Khelili c. Suisse, §§ 55-57; 9 octobre 2012, *Alkaya c. Turquie*, § 29; 18 avril 2013, *M.K. c. France*, § 26; 18 septembre 2014, *Brunet c. France*, § 31; 13 octobre 2020, *Frâncu c. Roumanie*, § 51).

B.7.5. 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*, § 31; grande chambre, 12 novembre 2013, *Söderman c. Suède*, § 78).

La protection des données à caractère personnel, et en particulier des données médicales, joue un rôle fondamental pour le droit au respect de la vie privée d'une personne et pour préserver sa confiance dans les services de santé (CEDH, 25 février 1997, *Z. c. Finlande*, § 95). 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*, § 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*, § 95; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 103; 26 janvier 2017, *Surikov c. Ukraine*, § 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*, § 74).

B.7.6. 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, alors que l'article 8 de cette Charte vise spécifiquement la protection des données à caractère personnel.

B.7.7. 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 et Eifert*, point 52; 16 janvier 2019, C-496/17, *Deutsche Post AG*, point 54).

B.7.8. L'article 52, paragraphe 1, de la Charte dispose :

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont

nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

B.7.9. L'article 4, points 1), 2), 5), 7), et 15), du RGPD dispose :

« Définitions

Aux fins du présent règlement, on entend par :

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

2) ' traitement ', toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

[…]

5) ' pseudonymisation ', le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

[…]

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

[…]

15) ' données concernant la santé ', 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 ».

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 14 du RGPD, intitulé « Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée », dispose :

« 1. Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable du traitement fournit à celle-ci toutes les informations suivantes:

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement;

b) le cas échéant, les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) les catégories de données à caractère personnel concernées;

e) le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel;

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une

organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition;

2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée les informations suivantes nécessaires pour garantir un traitement équitable et transparent à l'égard de la personne concernée :

a) la durée pendant laquelle les données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

b) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;

c) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ainsi que du droit de s'opposer au traitement et du droit à la portabilité des données;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer le consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci;

e) le droit d'introduire une réclamation auprès d'une autorité de contrôle;

f) la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public;

g) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

3. Le responsable du traitement fournit les informations visées aux paragraphes 1 et 2 :

a) dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées;

b) si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne; ou

c) s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

4. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont

été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

5. Les paragraphes 1 à 4 ne s'appliquent pas lorsque et dans la mesure où :

a) la personne concernée dispose déjà de ces informations;

b) la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve des conditions et garanties visées à l'article 89, paragraphe 1, ou dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles;

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

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

L’article 24 du RGPD, intitulé « Responsabilité du responsable du traitement », dispose:

« 1. Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.

2. Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement ».

L’article 26 du RGPD, intitulé « Responsables conjoints du traitement », dispose:

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

2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

3. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement ».

L'article 36 du RGPD, intitulé « Consultation préalable », dispose, en ses paragraphes 1 et 5 :

« 1. Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

[…]

5. Nonobstant le paragraphe 1, le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique ».

B.8. Les griefs des parties requérantes portent sur les aspects suivants :

I. la création de la base de données I auprès de Sciensano, visée à l'article 2 de l'accord de coopération du 25 août 2020, et la durée de conservation des données enregistrées dans la base de données II, visée à l'article 15 (première et dixième branches) (B.9-B.26);

II. la nécessité de collecter certaines catégories de données, visées aux articles 6 à 9 (deuxième branche) (B.27-B.34);

III. l'habilitation conférée au Comité de sécurité de l'information d'autoriser la communication de données à caractère personnel à des tiers, visée aux articles 11 et 12 (troisième branche) (B.35.1-B.40);

IV. l'information fournie par les centres de contacts aux médecins traitants, visée à l'article 3, § 1er, 2°, B (quatrième branche) (B.41-B.43);

V. la finalité de recherche scientifique, visée à l'article 3, § 1er, 4° (cinquième branche) (B.44-B.48);

VI. les liens entre la base de données I et la base de données V et la notion de « contacts à risque », visés à l'article 14 (sixième et septième branches) (B.49-B.52.3);

VII. la notion de « visite physique », visée à l'article 3 (huitième branche) (B.53-B.55.4);

VIII. l'obligation de secret des collaborateurs des centres de contact (neuvième branche) (B.56-B.62).

I. En ce qui concerne la création de la base de données I auprès de Sciensano et la durée de conservation des données enregistrées dans la base de données II (première et dixième branches)

B.9. Dans la première branche du moyen unique, les parties requérantes font valoir que la création de la base de données I auprès de Sciensano prévue à l'article 2 de l'accord de coopération du 25 août 2020, tel qu'il a été approuvé par les actes attaqués, entraîne une ingérence disproportionnée dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel, dès lors que Sciensano n'est pas chargé des opérations manuelles de traçage des contacts et qu'il existe d'autres moyens d'atteindre l'objectif poursuivi, par exemple, en demandant aux centres de contact de fournir eux-mêmes les données nécessaires aux acteurs chargés de la recherche scientifique. Les parties requérantes

soutiennent également que la disposition attaquée viole les principes de légalité et de prévisibilité car elle ne permettrait pas de comprendre en quoi la création d'une base de données centrale est nécessaire et proportionnée.

Dans la dixième branche du moyen unique, les parties requérantes soutiennent qu'à défaut de préciser la durée de conservation des données pseudonymisées qui sont enregistrées dans la base de données II, l'article 15 de l'accord de coopération ne satisfait pas au principe de légalité.

La Cour examine ensemble ces griefs qui portent notamment sur le respect du principe de légalité par des dispositions connexes.

B.10.1. Comme il est dit en B.7.4, le droit au respect de la vie privée englobe la protection des données à caractère personnel et des informations personnelles dont relèvent, notamment, les données de santé.

En ce qu'elle prévoit la centralisation d'un grand nombre de données à caractère personnel, y compris des données sensibles concernant la santé, la disposition attaquée entraîne une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel, garantis par les dispositions citées en B.7 à B.8.

B.10.2. Comme il est dit en B.7.5, une telle ingérence n'est admissible que si elle est prévue par une disposition législative suffisamment précise, si elle répond à un besoin social impérieux dans une société démocratique et si elle est proportionnée à l'objectif légitime qu'elle poursuit.

Dès lors que les données figurant dans la base de données I sont notamment des données concernant la santé, au sens de l'article 4, point 15), du RGPD, et que la disposition attaquée suppose l'accomplissement de plusieurs traitements de ces données, au sens de l'article 4, point 2), du même RGPD, l'ingérence doit également satisfaire aux conditions fixées par 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 ».

B.11.1. En ce qu’elles déduisent une violation des principes de légalité et de prévisibilité du caractère non nécessaire et disproportionné de la disposition attaquée, les parties requérantes confondent des étapes distinctes du contrôle que doit effectuer la Cour quant au respect du droit à la vie privée et du droit à la protection des données à caractère personnel.

B.11.2. 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 des traitements de données à caractère personnel doivent être fixés dans la loi elle-même. À cet égard, quelle que soit la matière concernée, les éléments suivants présentent en principe un caractère essentiel : 1°) les catégories de données traitées; 2°) les catégories de personnes concernées; 3°) la finalité poursuivie par le traitement; 4°) les catégories de personnes ayant accès aux données traitées et 5°) le délai maximal de conservation des données (voyez dans ce sens l'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.11.3. 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, 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*, § 57; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 99). À cet égard, la Cour européenne des droits de l'homme a souligné qu'il existe plusieurs étapes cruciales au cours desquelles des questions de protection des données peuvent se poser au regard de l'article 8 de la Convention européenne des droits de l'homme, notamment lors de la collecte, de la conservation, de l'utilisation et de la communication des données (CEDH, 24 janvier 2019, *Catt. c. Royaume-Uni*, § 95).

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.11.4. Partant, la Cour examine d'abord si, eu égard aux différents éléments contenus dans la disposition attaquée et dans les dispositions liées à celle-ci, toute personne dont les données à caractère personnel sont collectées et enregistrées dans la base de données I et, le cas échéant, dans les autres bases de données alimentées par celle-ci peut savoir de manière suffisamment précise dans quelles conditions s'effectue le traitement de ses données.

1. La légalité et la prévisibilité de l'ingérence

B.12. L'article 2 de l'accord de coopération du 25 août 2020 dispose :

« § 1. Afin d'atteindre les objectifs visés à l'article 1er, § 2, une Base de données I, qui contient les catégories de données décrites à l'article 6, est créée au sein de Sciensano. Ces données sont traitées conformément aux finalités telles que définies à l'article 3, pour la durée déterminée à l'article 15. Ces données seront communiquées par les personnes autorisées ou au nom des personnes autorisées des hôpitaux et des laboratoires, ainsi que par les médecins et le personnel du centre de contact, des services d'inspection d'hygiène et des équipes mobiles.

§ 2. La Base de données I est créée sans préjudice de la Base de données II déjà existante.

Pour atteindre l'objectif visé à l'article 1er, § 2, 1°, *h*, et 3°, les données de la Base de données I seront pseudonymisées avant d'être incluses dans la Base de données II conformément aux dispositions des articles 9 et 10.

§ 3. Pour atteindre les objectifs visés à l'article 1er, § 2, 1° *b*, *e*, *f* et *g*, et parallèlement à la Base de données I, les bases de données temporaires suivantes sont également créées, entre lesquelles les catégories de données définies à l'article 6 seront échangées, mais uniquement pour les finalités de traitement définies à l'article 3 et conformément aux dispositions de l'article 10, pour la durée déterminée à l'article 15 :

1° la Base de données III;

2° la Base de données IV.

§ 4. Sciensano est le responsable du traitement des Bases de données I et II.

§ 5. Les entités fédérées compétentes ou les agences désignées par les autorités compétentes, chacune pour sa compétence, agissent en tant que responsables du traitement des Bases de données III et IV, en ce qui concerne les données à caractère personnel collectées et utilisées par les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes et prennent les mesures appropriées pour que les personnes visées à

l'article 4 reçoivent les informations visées aux articles 13 et 14 du Règlement Général sur la Protection des Données et les communications visées aux articles 15 à 22 et à l'article 34 du Règlement Général sur la Protection des Données en ce qui concerne les finalités de traitement visées à l'article 3, § 2. Ces informations doivent être fournies dans un langage simple et clair et de manière concise, transparente, compréhensible et facilement accessible ».

B.13.1. Selon l'article 1er, § 1er, 6°, de l'accord de coopération du 25 août 2020, la base de données I est « la base de données de Sciensano qui sera créée en vertu du présent accord de coopération pour le traitement et l'échange de données aux finalités de traitement prévues à l'article 3 ». Sciensano est désigné responsable du traitement de cette base de données (article 2, § 4, de l'accord de coopération du 25 août 2020). Il s'agit de l'institution publique dotée de la personnalité juridique qui a notamment pour missions légales de rendre des avis aux autorités de santé, de traiter des données à caractère personnel relatives à la santé publique ou en lien avec la santé et de réaliser des analyses scientifiques sur la base des informations traitées en vue de soutenir la politique de santé (articles 3 et 4, § 1er, 1°, et § 4, de la loi du 25 février 2018 « portant création de Sciensano »). Depuis le 17 juin 2021, l'article 4/1 de la loi du 25 février 2018, introduit par l'article 63 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 que « dans le cadre de la gestion des crises touchant la santé publique, Sciensano a pour mission de coordonner et d'implémenter les aspects scientifiques qui y sont liés, de surveiller et d'évaluer les risques au moyen d'analyses spécifiques des données collectées, de fournir des avis et recommandations aux différentes autorités de santé du pays et d'organiser la communication au profit des autorités, des prestataires des soins de santé et du public ». Cette disposition vise à clarifier les missions légales de Sciensano et à renforcer l'autorité et le rôle de cette institution dans le cadre de la gestion des crises sanitaires (*Doc. parl.*, Chambre, 2020-2021, DOC 55-1929/001, p. 60).

Il ressort du dispositif de l'accord de coopération et de son exposé général que la base de données I est une base de données centrale créée auprès de Sciensano afin de collecter les données à caractère personnel fournies, d'une part, par les médecins, les laboratoires et les hôpitaux et, d'autre part, par le personnel des centres de contact et par les équipes mobiles (article 2, § 1er, troisième phrase, de l'accord de coopération du 25 août 2020; *Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, pp. 65 et 73). Le « centre de contact » est l'« instance

désignée par les entités fédérées compétentes ou par les agences compétentes pour contacter la personne concernée par tout moyen de communication, y compris par téléphone, par courrier électronique ou au moyen d'une visite physique dans le cadre des objectifs fixés à l'article 3, § 2, et qui partage ensuite les données collectées avec la base de données I » (article 1er, § 1er, 4°). Les « équipes mobiles » sont les « collaborateurs de l'équipe de soutien COVID (Outbreak Support team) organisée par les inspections d'hygiène qui prennent des mesures sur place dans le cas d'un cluster » (article 1er, § 1er, 12°). Un « cluster » est « une concentration de personnes infectées ou potentiellement infectées par le coronavirus COVID–19 dans des collectivités » (article 1er, § 1er, 2°). Une « collectivité » est « une communauté de personnes pour lesquelles les inspections d'hygiène compétentes estiment qu'il existe un risque accru de propagation du coronavirus COVID–19 » (article 1er, § 1er, 3°), par exemple : un hôpital, une école, un centre d'asile, une prison, une maison de repos et de soins, un lieu de travail, une institution pour personnes handicapées, une garderie, un centre de revalidation ou une caserne (*Doc. parl*., Chambre, 2019-2020, DOC 55-1490/001, p. 76).

B.13.2. La base de données I est créée à côté d'une autre base de données qui existe déjà auprès de Sciensano (la base de données II). Les données à caractère personnel de la base de données I sont enregistrées, après pseudonymisation, dans la base de données II en vue d'être utilisées à des fins de recherche scientifique (article 2, § 2). L'exposé général de l'accord de coopération mentionne que la plateforme « e-Health » est responsable de cette pseudonyimsation, qui intervient après l'enregistrement des données dans la base de données I et avant le partage de celles-ci avec la base de données II (*Doc. parl*., Chambre, 2019-2020, DOC 55-1490/001, pp. 69-74, spécialement p. 71).

B.13.3. L'accord de coopération crée en outre trois autres bases de données : une base de données commune aux centres de contact qui contient les instructions et les instructions d'appel destinées au personnel des centres de contact (la base de données III), une base de données contenant les coordonnées de collectivités (la base de données IV) (article 1er, § 1er, 8° et 9°, et article 2, § 3) et le journal central des enregistrements de l'application numérique de traçage des contacts (la base de données V) (article 1er, § 1er, 10°, et article 14, § 3, 2°).

Les bases de données III et IV « échangent des données entre elles et avec la Base de données I dans le cadre du suivi des contacts » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, p. 75; voir article 2, § 3). Les entités fédérées compétentes ou leurs agences sont désignées responsables du traitement des bases de données III et IV (article 2, § 5). Il s'agit, selon l'exposé général de l'accord de coopération, de l'Agence flamande « Zorg en Gezondheid », de l'Agence wallonne pour une vie de qualité, du Ministère de la Communauté germanophone et de la Commission communautaire commune (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, p. 74).

Sciensano est le responsable du traitement de la base de données V (article 14, § 3, 3°), laquelle est, chez Sciensano, séparée des bases de données I et II (article 1er, § 1er, 10°).

B.13.4. Il en résulte que la base de données I constitue la source des données à caractère personnel qui sont transmises à la base de données II utilisée pour la recherche scientifique. Elle constitue par ailleurs la source et le destinataire des données à caractère personnel qui sont collectées dans la base de données III et dans la base de données IV. Il ressort en effet de l'article 1er, § 1er, 4°, précité, de l'accord de coopération et de son exposé général que la base de données I comprend notamment les informations recueillies, par les centres de contacts, auprès des personnes infectées et des personnes présumées infectées concernant les personnes avec lesquelles celles-ci ont été en contact et les informations recueillies, par les équipes mobiles, auprès des collectivités :

« Afin de rendre le suivi manuel des contacts aussi efficace que possible, la Base de données I doit intervenir en tant que base de données centrale dans la lutte contre la propagation du coronavirus COVID-19. Sciensano, en tant que responsable du traitement, gère la Base de données I qui contient des données à caractère personnel fournies par les prestataires de soins et les établissements de soins. Toutefois, aux fins énoncées dans le présent accord de coopération, il sera également nécessaire que le personnel des centres de contact (y compris les enquêteurs de terrain) et les équipes mobiles partagent avec la Base de données I les données qu'ils ont recueillies. L'objectif est d'organiser un suivi manuel de contacts qui soit aussi efficace et complet que possible » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, p. 73).

« Les données collectées par les équipes mobiles peuvent en outre être transférées à Sciensano pour être stockées dans la Base de données I en vue de leur traitement et de leur communication ultérieur(e)s, mais uniquement pour les finalités de traitement fixées dans le présent accord de coopération » (*ibid.*, p. 89).

B.13.5. En revanche, la base de données I est sans lien avec la base de données V.

a) Les finalités du traitement

B.14.1. L'article 3 de l'accord de coopération du 25 août 2020 énonce les finalités du traitement des données à caractère personnel collectées dans la base de données I « et de l'échange ultérieur de [ces] données vers les Bases de données II, III et IV » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, p. 76).

B.14.2. Comme l'a observé l'Autorité de la protection des données dans son avis n° 64/2020 du 20 juillet 2020 sur le projet d'accord de coopération devenu l'accord de coopération du 25 août 2020, ces finalités peuvent être rassemblées en trois catégories (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/002, pp. 11-12).

La première finalité est de permettre aux centres de contact de procéder au traçage manuel des personnes (présumées) infectées et de leurs contacts (ci-après : la finalité de traçage manuel des contacts). À cette fin, les centres de contacts reçoivent, au moyen d'un échange de données entre la base de données I et la base de données III, les catégories de données à caractère personnel relatives aux personnes de catégorie II « dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles étaient infectées » (ci-après : les personnes de catégorie II testées positives) et aux personnes présumées infectées (personnes de catégorie III) afin de leur donner des recommandations éventuelles mais surtout de leur demander de fournir des informations concernant les personnes avec lesquelles elles ont eu des contacts (article 3, § 1er, 1°, lu en combinaison avec l'article 1er, § 1er, 14° et 15°; voir aussi l'article 3, § 2, 1°, et l'article 10, § 1er). Ces informations doivent permettre ensuite aux centres de contact de contacter les personnes avec lesquelles les personnes testées positives et les personnes présumées infectées ont été en contact au cours d'une période de quatorze jours avant à quatorze jours après les premiers signes d'infection (personnes de catégorie IV) pour leur fournir des recommandations en matière d'hygiène et de prévention, leur proposer une quarantaine ou les inviter à se soumettre à un test de dépistage (article 3, § 1er, 2°, A, lu en combinaison avec l'article 1er, § 1er, 16°; voir aussi l'article 3, § 2, 2°, A). Ces informations doivent également permettre aux centres de contact de contacter le médecin de référence ou le responsable administratif des collectivités avec lesquelles ces personnes testées positives et présumées

infectées ont été en contact au cours d'une période de quatorze jours avant à quatorze jours après les premiers symptômes de l'infection par le coronavirus COVID–19 (personnes de catégorie VI) pour les informer de la contamination (présumée) des personnes précitées (article 3, § 1er, 2°, B, lu en combinaison avec l'article 1er, § 1er, 18°; voir aussi l'article 3, § 2, 2°, B, et l'article 10, § 1er).

La deuxième finalité est de permettre aux équipes mobiles et aux services d'inspection d'hygiène des autorités fédérées de prendre des initiatives visant à prévenir la propagation des effets nocifs causés par le COVID-19 dans le cadre de l'accomplissement de leurs missions réglementaires (ci-après : la finalité de prévention). À cette fin, les équipes et services visés par le décret flamand du 21 novembre 2003 « relatif à la politique de santé préventive », par le décret de la Communauté germanophone du 1er juin 2004 « relatif à la promotion de la santé et à la prévention médicale » et ses arrêtés d'exécution, par l'ordonnance de la Région de Bruxelles-Capitale du 19 juillet 2007 « relative à la politique de prévention en santé », par le décret de la Région wallonne du 2 mai 2019 « modifiant le Code wallon de l'Action sociale et de la Santé en ce qui concerne la prévention et la promotion de la santé », par l'arrêté du Collège réuni de la Commission communautaire commune du 23 avril 2009 « relatif à la prophylaxie des maladies transmissibles » et par l'arrêté du Gouvernement flamand du 19 juin 2009 « relatif aux initiatives visant à prévenir l'extension des effets néfastes causés par des facteurs biotiques » ont accès aux données à caractère personnel collectées dans la base de données I concernant les personnes de catégories I à IV (article 3, § 1er, 3°; article 3, § 3, et article 10, § 2).

La troisième finalité consiste à permettre aux institutions de recherche, dont Sciensano, d'effectuer des études scientifiques ou statistiques sur la lutte contre la propagation du COVID–19 et/ou de soutenir la politique dans ce domaine (ci-après : la finalité de recherche scientifique). À cette fin, les données à caractère personnel relatives aux personnes de catégories I à V contenues dans la base de données I sont mises à la disposition de la base de données II sous une forme pseudonymisée, puis, des institutions de recherche, dont Sciensano, sous une forme anonymisée ou au moins pseudonymisée (article 3, § 1er, 4°; voir aussi : article 1er, § 2, 1°, *h*; article 1er, § 2, 3°, et article 10, § 3, première phrase).

B.14.3. L'article 3, § 4, mentionne que les données collectées dans le cadre de l'accord de coopération ne peuvent pas être utilisées à d'autres fins « notamment mais pas exclusivement à des fins policières, commerciales, fiscales, pénales ou de sécurité de l'État ».

b) Les catégories de données à caractère personnel collectées et les catégories de personnes concernées

B.15.1. L'article 6, §§ 2 à 7, de l'accord de coopération du 25 août 2020 détermine les catégories de données à caractère personnel contenues dans la base de données I pour chaque catégorie de personnes concernées.

B.15.2. Pour les personnes disposant d'une prescription (personnes de catégorie I), la base de données I contient les catégories suivantes de données à caractère personnel : « 1° le numéro NISS; 2° le nom et le prénom; 3° le sexe; 4° la date de naissance et, le cas échéant, la date de décès; 5° l'adresse; 6° les coordonnées, y compris le numéro de téléphone et l'adresse électronique de la personne concernée et de la personne à contacter en cas d'urgence ou du représentant légal, et l'indication du lien qu'ont ces personnes avec la personne concernée (parent, tuteur, médecin généraliste, …); 7° la date de l'apparition des symptômes; 8° le numéro INAMI du prescripteur du test de dépistage […]; 9° les données relatives au test de dépistage prescrit, en ce compris la date et le type de test […]; 10° l'indication de l'exercice ou du non-exercice de la profession de prestataire de soins; 11° le service hospitalier, le numéro d'identification et les coordonnées de l'hôpital, si la personne concernée est hospitalisée; 12° éventuellement, le résultat du CT-scan, si la personne concernée est hospitalisée; 13° la collectivité éventuelle dont la personne concernée fait partie ou avec laquelle elle est entrée en contact » (article 6, § 2, alinéa 1er). Les nom et prénom, date de naissance, sexe et adresse sont extraits du Registre national ou des registres de la Banque-carrefour de la sécurité sociale (article 6, § 2, alinéa 2).

B.15.3. Pour les personnes testées (personnes de catégorie II), la base de données I contient, outre les données précitées en B.15.2, « 2° la date, le résultat, le numéro d'échantillon et le type de test de dépistage […]; 3° le numéro INAMI du laboratoire qui a effectué le test de dépistage […]; 4° si le résultat du test de dépistage n'a pas permis de constater une

contamination, l'éventuelle décision d'annulation prise par un médecin; 5° si le résultat du test de dépistage n'a pas permis de constater une contamination, le numéro INAMI du médecin qui a pris la décision d'annulation » (article 6, § 3, alinéa 1er).

Ces données sont fournies par « les personnes autorisées ou sur ordre des personnes autorisées du laboratoire, de l'hôpital ou de l'autre établissement de soins ou du prestataire de soins qui a effectué le test de dépistage », sauf la décision éventuelle d'annulation prise par un médecin en cas de résultat négatif du test de dépistage et le numéro INAMI de ce médecin, qui sont communiqués par le médecin concerné (article 6, § 3, alinéa 2).

B.15.4. Pour les personnes présumées infectées (personnes de catégorie III), la base de données I contient, outre les données visées au 1° à 7°, 10° et 13°, précitées en B.15.2, « 7° le diagnostic présumé de contamination […]; 8° le numéro INAMI du médecin qui émet la forte suspicion […]; 12° les données nécessaires permettant au centre de contact de prendre tout contact utile avec la personne concernée, en ce compris le code postal et la langue » (article 6, § 4, alinéa 1er). Les nom et prénom, date de naissance, sexe et adresse sont extraits du Registre national ou des registres de la Banque-carrefour de la sécurité sociale (article 6, § 4, alinéa 2, deuxième phrase).

Ces données sont fournies par le médecin qui soupçonne la contamination (article 6, § 4, alinéa 2, première phrase).

B.15.5. Pour les personnes ayant eu un contact avec une personne testée positive ou avec une personne présumée infectée (personnes de catégorie IV) et, le cas échéant, pour les personnes de catégorie II testées positives et pour les personnes présumées infectées (personnes de catégorie III), la base de données I contient : « 1° le numéro NISS; 2° le nom et le prénom; 3° le sexe; 4° la date de naissance et, le cas échéant, la date du décès; 5° l'adresse; 6° les coordonnées, en ce compris le numéro de téléphone et l'adresse électronique; 7° les données nécessaires permettant au centre de contact de prendre tout autre contact utile avec la personne visée au présent paragraphe et la liste des personnes avec lesquelles la personne visée au présent paragraphe a eu des contacts récents, en ce compris le code postal et la langue, ainsi que le risque estimé de contagion de la personne visée au présent paragraphe; 8° la liste des collectivités dont la personne visée au présent paragraphe fait partie ou avec lesquelles elle est entrée en contact, dont les données sont communiquées par la base de données IV; 9° les

critères pertinents permettant d'évaluer si le risque d'infection est élevé ou faible et de donner des conseils, en ce compris les symptômes éventuels, le moment où les symptômes sont apparus, le type de test de dépistage prescrit […], la visite chez le médecin, l'enregistrement du refus éventuel de voir un médecin; 10° les informations pertinentes communiquées au centre de contact par la personne visée au présent paragraphe concernant les déplacements effectués, les symptômes et le suivi des mesures d'isolement, de prévention et d'hygiène; 11° le simple fait qu'il y ait eu contact entre les personnes de catégorie IV et les personnes de catégories I, II, III, y compris l'appartenance au ménage des personnes de catégorie IV; 12° la réponse à la question de savoir si (i) les [personnes de catégorie II testées positives]; (ii) les personnes de catégorie III; ou (iii) les personnes de catégorie IV utilisent ou non une application numérique de traçage des contacts » (article 6, § 5).

La même disposition prévoit que ces données sont fournies par les centres de contacts.

B.15.6. Pour les personnes de catégorie II testées positives, pour les personnes de catégories III et IV ainsi que pour les personnes faisant partie d'un *cluster*, la base de données I contient également « toutes les données nécessaires à l'organisation et au suivi du contact avec la personne concernée par le personnel du centre de contact, telles que la langue de la personne concernée, le statut de contact de la personne concernée, les numéros de ticket des enregistrements de prise de contact ou des tentatives de prise de contact, les types de contact, l'heure des tickets, l'heure et la durée de la prise de contact, le résultat de la prise de contact » (article 6, §§ 6 et 7).

Pour les personnes de catégorie II testées positives et pour les personnes de catégories III et IV, ces données sont fournies par les centres de contacts (article 6, § 6). Pour les personnes faisant partie d'un *cluster*, ces données sont fournies par les équipes mobiles ou par les services d'inspections d'hygiène compétents (article 6, § 7).

B.16.1. Les catégories de données à caractère personnel contenues dans les bases de données II, III et IV sont énumérées aux articles 7 à 9 de l'accord de coopération du 25 août 2020.

B.16.2. La base de données II contient ainsi, pour les personnes de catégories I, II et III, « les données à caractère personnel […] énumérées à l'article 6 mais uniquement après

pseudonymisation », à savoir « 1° un numéro unique qui ne permet pas d'identifier la personne; 2° l'année de naissance et, le cas échéant, l'année et le mois du décès; 3° le sexe; 4° le code postal; 5° le numéro INAMI du prescripteur du test de dépistage du coronavirus COVID–19; 6° le type, la date, le numéro d'échantillon et le résultat du test de dépistage du coronavirus COVID–19 ou le diagnostic présumé en l'absence de test de dépistage du coronavirus COVID–19; 7° le numéro INAMI du laboratoire qui a effectué le test de dépistage du coronavirus COVID–19; 8° en cas de résultat de test de dépistage du coronavirus COVID–19 négatif, une éventuelle décision d'annulation par un médecin; 9° en cas de décision d'annulation d'un résultat de test négatif, le numéro INAMI du médecin qui a pris la décision d'annulation; 10° le cas échéant, le type et le code postal de la collectivité dont la personne fait partie ou avec laquelle elle est entrée en contact; 11° le résultat des examens médicaux, y compris le résultat du CT-scan; 12° l'indication de l'exercice ou non de la profession de prestataire de soins; 13° les données pertinentes pour le traçage des contacts, en ce compris les symptômes, la date des premiers symptômes, les déplacements, le suivi des mesures d'isolement et d'hygiène; 14° le simple fait qu'il y ait eu contact, y compris le fait de faire partie du ménage, entre les Personnes de catégorie IV et, d'une part, les Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé que ces personnes sont infectées, et, d'autre part les Personnes de catégorie III » (article 9, § 1er).

Pour les personnes de catégorie IV, la base de données II contient « les données à caractère personnel […] énumérées à l'article 6 mais uniquement après pseudonymisation », à savoir : « 1° un numéro unique qui ne permet pas d'identifier la personne; 2° l'année de naissance et, le cas échéant, l'année et le mois du décès; 3° le sexe; 4° les symptômes; 5° le contact ou l'absence de contact avec des personnes vulnérables; 6° le résultat et la date du test de dépistage du coronavirus COVID–19 prescrit; 7° l'exercice de la profession de prestataire de soins; 8° les données strictement nécessaires relatives à la prise de contact, en ce compris la date du ticket et le résultat général de la prise de contact sous la forme d'un code; 9° tous les critères pertinents pour estimer le risque élevé ou faible; 10° le code postal de l'adresse » (article 9, § 2).

B.16.3. La base de données III contient les catégories suivantes de données à caractère personnel concernant les personnes de catégorie II testées positives et les personnes de catégorie III : « 1° le numéro NISS; 2° le nom et le prénom; 3° le sexe; 4° la date de naissance; 5° les coordonnées, en ce compris l'adresse, le numéro de téléphone et l'adresse électronique, de la personne concernée, ainsi que des personnes à contacter en cas d'urgence; 6° les données

nécessaires permettant au centre de contact de prendre tout contact utile avec la personne concernée, en ce compris le code postal et la langue; 7° l'indication que la personne doit être appelée par téléphone en tant que personne (présumée) infectée afin de retracer ses contacts; 8° le cas échéant, le résultat du test de dépistage du coronavirus COVID–19 et la date du test; 9° le numéro du ticket, la date, l'heure et le résultat de la prise de contact » (article 7, § 2).

Pour les personnes de catégorie IV, la base de données III contient : « 1° le numéro NISS; 2° le nom et le prénom; 3° le sexe; 4° la date de naissance et, le cas échéant, la date du décès; 5° l'adresse; 6° les coordonnées, en ce compris le numéro de téléphone et l'adresse électronique; 7° les données nécessaires permettant au centre de contact de prendre tout autre contact utile avec la personne visée au présent paragraphe et la liste des personnes avec lesquelles la personne visée au présent paragraphe a eu des contacts récents, en ce compris le code postal et la langue de la personne visée au présent paragraphe; 8° la liste des collectivités dont la personne visée au présent paragraphe fait partie ou avec lesquelles elle est entrée en contact, dont les données sont communiquées par la Base de données IV; 9° les critères pertinents permettant d'évaluer si le risque d'infection est élevé ou faible et de donner des conseils, en ce compris les symptômes éventuels, le moment où les symptômes sont apparus, le type de test de dépistage du coronavirus COVID–19 prescrit, la visite chez le médecin, l'enregistrement du refus éventuel de voir un médecin; 10° les données pertinentes communiquées au centre de contact et aux équipes mobiles par la personne visée au présent paragraphe concernant les déplacements effectués, les symptômes et le suivi des mesures d'isolement, de prévention et d'hygiène; 11° le simple fait qu'il y ait eu contact entre la Personne de catégorie IV, en ce compris l'appartenance au ménage de celle-ci, et d'une part, les Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a montré que ces personnes sont infectées, et, d'autre part, les Personnes de catégorie III » (article 7, § 3).

Pour les personnes de catégorie VI, la base de données III contient : « 1° le nom, le type, les coordonnées de la collectivité; 2° les coordonnées du médecin de référence et/ou de la personne responsable de la collectivité, en ce compris ses nom, prénom et numéro de téléphone » (article 7, § 4).

B.16.4. La base de données IV contient les catégories suivantes de données à caractère personnel relatives aux personnes de catégories V et VI : « 1° le numéro d'identification

provenant d'une source authentique, en particulier le Registre national et la Banque-carrefour de la sécurité sociale, et le numéro d'identification interne; 2° les nom, le type, l'adresse, le numéro figurant dans la Banque-carrefour des Entreprises, de la collectivité à laquelle la personne appartient ou avec laquelle elle a eu des contacts; 3° les coordonnées du médecin de référence et/ou de la personne responsable de la collectivité, en ce compris le nom, prénom et le numéro de téléphone » (article 8).

c) Les catégories de personnes ayant accès aux données

B.17.1. Il ressort de l'article 2, §§ 4 et 5, de l'accord de coopération du 25 août 2020 que les bases de données I à IV sont accessibles par leur responsable du traitement respectif, à savoir Sciensano pour les bases de données I et II, et les entités fédérées compétentes ou leurs agences pour les bases de données III et IV.

B.17.2. Par ailleurs, selon l'article 10, § 1er, alinéa 1er, de l'accord de coopération, les centres de contact ont accès uniquement « aux catégories de données à caractère personnel visées à l'article 7, § 2, § 3 et § 4 », c'est-à-dire aux données à caractère personnel de la base de données III relatives aux personnes de catégorie II testées positives et aux personnes de catégories III, IV et VI.

Selon l'article 10, § 1er, alinéa 2, l'accès des centres de contact aux données de la base de données III poursuit « les finalités mentionnées à l'article 3, § 1er, 1° à 3° et à l'article 3, § 2 », c'est-à-dire la finalité de traçage manuel des contacts et la finalité de prévention.

B.17.3. Selon l'article 10, § 2, de l'accord de coopération, les équipes mobiles et les services d'inspection d'hygiène compétents ont accès « aux catégories de données à caractère personnel relatives aux Personnes de catégories I, II, III, IV et si nécessaire des Personnes de catégories V et VI, visées à l'article 6, dans la Base de données I », uniquement « aux fins mentionnées à l'article 3, § 1er, 3° », c'est-à-dire pour la finalité de prévention.

B.17.4. L'article 10, § 3, première phrase, de l'accord de coopération dispose que les données à caractère personnel de la base de données I sont transmises ultérieurement, après

pseudonymisation, à la base de données II « aux fins définies à l'article 3, § 1er, 4°, », c'est-à-dire pour la finalité de recherche scientifique.

B.17.5. Il résulte de ce qui précède qu'à côté de l'accès dont dispose leur responsable du traitement respectif, la base de données I est accessible, en outre, aux équipes mobiles et aux services d'inspection d'hygiène compétents, tandis que la base de données III est accessible aux centres de contact.

d) La durée maximale de conservation des données

B.18.1. 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.18.2. Selon l'article 15, § 1er, de l'accord de coopération du 25 août 2020, les données contenues dans la base de données I sont supprimées au plus tard soixante jours après leur enregistrement. La même disposition prévoit que les données enregistrées dans la base de données III sont supprimées quotidiennement.

L'article 15, § 3, dispose que les bases de données I et III sont « désactivées, supprimées ou effacées » par le responsable du traitement au plus tard cinq jours après le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie de COVID–19.

B.19.1. En ce qui concerne le délai de conservation maximal des données à caractère personnel pseudonymisées enregistrées dans la base de données II, l'article 15, § 2, du projet d'accord de coopération prévoyait que ces données seraient supprimées « conformément aux dispositions de la loi du 10 avril 2014 portant des dispositions diverses en matière de santé et de l'accord de coopération conclu en exécution de celle-ci entre l'INAMI et Sciensano ».

À la suite de l'avis de l'Autorité de protection des données n° 64/2020 du 20 juillet 2020 (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/002, p. 23), l'article 15, § 2, de l'accord de coopération du 25 août 2020 finalement adopté prévoit que ces données sont supprimées « conformément au délai généralement accepté pour la conservation des dossiers concernant la santé et dans le cadre de la recherche scientifique en matière de santé, à savoir trente ans ».

B.19.2. Lorsque, dans la dixième branche du moyen unique, les parties requérantes font grief à l'article 15, § 2, de l'accord de coopération du 25 août 2020 de ne pas préciser avec la clarté requise le délai de conservation des données pseudonymisées enregistrées dans la base de données II, ils se réfèrent au projet d'accord de coopération et non à l'accord de coopération. Dès lors qu'il repose sur une prémisse erronée, le moyen unique, en sa dixième branche, n'est pas fondé.

B.20.1. Selon l'article 15, § 1er et § 3, deuxième phrase, de l'accord de coopération, les données à caractère personnel enregistrées dans la base de données IV sont transférées aux entités fédérées compétentes en matière de détection des maladies infectieuses au plus tard cinq jours après le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie de COVID–19.

Aucun délai maximal de conservation n'est fixé pour les données à caractère personnel enregistrées dans la base de données IV.

B.20.2. L'article 15, § 1er, du projet d'accord de coopération disposait :

« […] Les données à caractère personnel de la Base de données IV sont soit mises à jour tous les 10 ans, soit supprimées […] ».

Dans son avis n° 67.719/VR du 15 juillet 2020 sur l'avant-projet de loi devenue la loi attaquée du 9 octobre 2020, la section de législation du Conseil d'État avait indiqué à propos de cette disposition que l'absence d'un délai maximal de conservation des données à caractère personnel contenues dans la base de données IV n'était pas conforme au RGPD :

« L'article 15, § 1er, alinéa 1er, de l'accord de coopération prévoit que les données à caractère personnel de la Base de données IV sont soit mises à jour tous les dix ans, soit supprimées. Interrogés à cet égard, les délégués ont répondu ce qui suit :

' Na een termijn van 10 jaar worden de gegevens ofwel gewist, ofwel nagekeken op hun accuraatheid en indien nodig geüpdatet. Indien in geval van niet-accurate gegevens updaten onmogelijk is of niet opportuun, zullen de gegevens gewist worden. Zolang ze niet gewist zijn, zijn ze accuraat en zijn dit de gegevens van de contactpersonen van de collectiviteiten. In geval van uitbraken van andere infectieziekten, zal dit immers zeer nuttig zijn '.

Cette absence de délai maximal de conservation pour ces données à caractère personnel n'est toutefois pas conforme à l'article 5, paragraphe 1, e), du RGDP, qui prescrit que ' les données à caractère personnel doivent être […] conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées '.

39.2. Interrogés quant aux motifs justifiant l'exception envisagée au paragraphe 1er, alinéa 2, pour ce qui concerne les données des Bases de données IV et V, les délégués ont répondu ce qui suit :

' Het komt opportuun voor om deze Gegevensbank [IV] te en voortbestaan na de COVID19 crisis. Immers, deze Gegevensbank zal ook haar nut in de toekomst bewijzen. Daarenboven bevat het merendeel van deze gegevens geen persoonsgegevens, maar gegevens over de collectiviteiten zelf '.

Le dispositif sera revu de manière à rendre celui-ci conforme au principe selon lequel il appartient au législateur de fixer les délais de conservation des données à caractère personnel » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, pp. 55-56).

B.20.3. Dans l'exposé général de l'accord de coopération du 25 août 2020, il est mentionné :

« Les données à caractère personnel de la Base de données III seront supprimées quotidiennement et celles de la Base de données IV sont soit mises à jour, soit supprimées en permanence. Dans l'hypothèse où la mise à jour de données inexactes est impossible ou inappropriée, les données seront supprimées. Tant qu'elles ne sont pas supprimées, elles sont exactes et constituent les données des personnes de contact des collectivités qui seront sauvegardées. Les données à caractère personnel de la Base de données IV seront transférées au plus tard cinq jours après le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus COVID-19 aux entités fédérées pour l'exécution de leur compétence en matière de détection des maladies infectieuses et contagieuses dans le cadre de leur compétence matérielle en matière de médecine préventive les soins de santé préventifs. En cas d'apparition d'autres maladies infectieuses, la conservation des données à caractère personnel exactes dans la Base de données IV sera en effet très utile. En outre, la Base de données IV ne contient des données à caractère personnel que dans une mesure limitée » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, p. 105).

B.20.4. La base de données IV contient plusieurs catégories de données à caractère personnel relatives aux personnes de catégories V et VI. Ces données sont énumérées à l'article 8, précité, de l'accord de coopération du 25 août 2020.

En ne prévoyant pas le délai maximal de conservation de ces données à caractère personnel, les articles 2, § 3, et 15, § 1er et § 3, deuxième phrase, de l'accord de coopération du 25 août 2020, tels qu'ils ont été approuvés par les actes attaqués, violent les articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 5, paragraphe 1, point e), du RGPD.

B.21. Sous réserve de l'annulation partielle mentionnée en B.20.4, l'article 2 de l'accord de coopération du 25 août 2020, lu en combinaison avec ses articles 1er, 3, 6 à 10, et 15, détermine les catégories de données traitées dans la base de données I et les bases de données II, III et IV liées à celle-ci, les catégories de personnes concernées, les finalités poursuivies par le traitement, les catégories de personnes ayant accès aux données traitées et le délai maximal de conservation des données. Conformément à l'article 3, § 4, l'utilisation des données récoltées à d'autres fins que celles qui sont mentionnées en B.14.2 est par ailleurs interdite.

Les personnes dont les données à caractère personnel sont collectées dans la base de données I et les bases de données liées à celle-ci peuvent dès lors connaître de manière suffisamment précise les conditions dans lesquelles leurs données sont traitées.

2. La nécessité et la proportionnalité de l'ingérence

B.22. La Cour examine maintenant la nécessité et la proportionnalité de l'ingérence.

Dans le cadre de cet examen, il y a lieu de vérifier si l'ingérence ne va pas au-delà de ce qui est nécessaire à la réalisation des objectifs poursuivis et, en particulier, s'il existe des mesures qui sont moins attentatoires aux droits concernés, tout en contribuant de manière efficace au but de la réglementation en cause (CJUE, 17 octobre 2013, C-291/12, *Schwarz c. Stadt Bochum*, points 46 et 47). La protection du droit fondamental au respect de la vie privée au niveau de l'Union exige, conformément à la jurisprudence constante de la Cour de justice,

que les dérogations à la protection des données à caractère personnel et les limitations de celle- ci s'opèrent dans les limites du strict nécessaire (CJUE, 16 décembre 2008, C-73/07, *Satakunnan Markkinapörssi et Satamedia*, point 56; 8 avril 2014, C-293/12 et C-594/12, *Digital Rights* Ireland e.a., points 51 et 52; 6 octobre 2015, C-362/14, *Schrems*, point 92, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige et Watson e.a*., points 96 et 103; 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a*., point 130).

Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient de tenir compte notamment de leur caractère automatisé, des techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées et de la présence ou de l'absence de garanties visant à éviter l'usage inapproprié et abusif, par les services publics, des données à caractère personnel traitées (arrêt n° 108/2016 du 14 juillet 2016, B.12.2; arrêt n° 29/2018 du 15 mars 2018, B.14.4; arrêt n° 27/2020 du 20 février 2020, B.8.3; CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 59; décision, 29 juin 2006, *Weber et Saravia c. Allemagne*, § 135; 28 avril 2009, *K.H. e.a. c. Slovaquie*, §§ 60-69; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, §§ 101-103, 119, 122 et 124; 18 avril 2013, *M.K. c. France*, §§ 37 et 42-44; 18 septembre 2014, *Brunet c. France*, §§ 35-37; 12 janvier 2016, *Szabó et Vissy c. Hongrie*, § 68; CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd* et C-594/12, *Kärntner Landesregierung e.a*., points 56-66).

B.23. Comme il est dit en B.1.1. et B.1.3, l'accord de coopération du 25 août 2020 vise à protéger la santé publique au moyen d'un traçage manuel et numérique des contacts dans le cadre de la lutte contre la propagation du COVID-19.

Cet objectif constitue un but légitime susceptible de justifier des ingérences dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel. Au

demeurant, la protection de la santé publique contribue également à la protection des droits et des libertés d'autrui.

B.24.1. En vertu du principe de 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.24.2. Dans son avis n° 42/2020 du 25 mai 2020 relatif à la proposition de loi « portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 », citée en B.1.4, l'Autorité de protection des données a observé que la centralisation d'une quantité importante de données relatives à la santé « dans une banque de données unique constituée, détenue et gérée par un acteur qui ne ferait office que d'intermédiaire » n'était pas conforme à ce principe :

« Rien n'indique qu'il soit requis d'effectuer une centralisation de ces données dans une banque de données détenue par un tiers (Sciensano), une telle centralisation n'étant dès lors pas conforme aux principes de nécessité, proportionnalité et minimisation et donc pas acceptable.

[…]

L'Autorité rappelle que la désignation de Sciensano en tant que responsable du traitement […] implique qu'elle soit en charge du respect de toutes les obligations qui s'imposent aux responsables du traitement en vertu du GDPR (fourniture de l'information adéquate aux personnes concernées, mise en place d'un système de gestion des droits des personnes concernées, mise en œuvre de mesures de sécurité appropriées, analyse de risques etc). La portée de cette désignation devrait par ailleurs être précisée. Sciensano n'agit en effet en tant que responsable du traitement que pour ce qui concerne les opérations précitées de collecte, enregistrement dans la banque de données et communication des données à des tiers. Pas pour ce qui concerne les opérations dites ' de traçage ' (prise de contact avec les personnes infectées et leurs contacts) proprement dites.

En ce qui concerne ces opérations, ce sont les agences régionales (qui chapeautent les centres de contact) qui sont responsables de traitement et l'Autorité rappelle également qu'ils sont tenus, à ce titre, de mettre en place les mesures de sécurité, le droit d'accès du citoyen, d'effectuer une analyse de risques etc (article 35).

[…]

La proposition de loi prévoit une centralisation d'une grande quantité de données, essentiellement médicales et donc sensibles, entre les mains d'un acteur unique qui n'est

pourtant pas l'acteur qui se chargera de l'accomplissement des trois finalités prévues; Sciensano n'est en effet :

a. pas en charge des opérations visant à contacter les personnes infectées (ou présumées infectées), opérations effectuées par des centres de contact sous la responsabilité des agences régionales compétentes en matière de santé;

b. pas en charge de la réalisation des études épidémiologiques visées à l'article 1§ 2°;

c. et pas non plus mandaté pour effectuer des ' initiatives visant à combattre la propagation des effets nocifs causés par les maladies infectieuses '

L'Autorité se demande pourquoi chacun des acteurs chargés de l'accomplissement de ces finalités ne pourrait pas lui-même collecter et enregistrer les données nécessaires à ces opérations, quitte à les fournir directement aux organismes de recherche épidémiologiques et de santé publique visés par la proposition de loi.

Par ailleurs, l'Autorité ne saisit pas la raison pour laquelle les données relatives aux ' malades ' (personnes présumées infectées par le virus, ayant effectué un test, s'étant vu prescrire un test ou hospitalisées avec un diagnostic confirmé) et celles relatives aux personnes avec lesquelles elles sont entrées en contact doivent être consignées dans la même banque de données (sachant que les secondes sont ' communiquées par les centres de contact ' qui détiennent donc déjà ces données pour contacter ces personnes et n'ont donc pas besoin qu'elles soient enregistrées chez Sciensano – art 2 § 4 de la proposition de loi).

Cette centralisation d'une quantité importante de données relatives à la santé dans une banque de données unique constituée, détenue et gérée par un acteur qui ne ferait office que d'intermédiaire […] n'est pas conforme aux principes de nécessité et de minimisation […] » (pp. 8-10; dans le même sens : avis n° 34/2020 du 28 avril 2020 « concernant un avant-projet d'arrêté royal n° XXX portant exécution de l'article 5, § 1, 1°, de la loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus COVID-19 (II), dans le cadre de l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population », p. 5; avis n° 36/2020 du 29 avril 2020 relatif à l'avant-projet d'arrêté royal devenu l'arrêté royal n° 18 du 4 mai 2020, pp. 5 et 11).

B.24.3. Il ressort de l'exposé général de l'accord de coopération du 25 août 2020 que la création d'une base de données centrale auprès de Sciensano a été justifiée par la nécessité d'assurer un suivi manuel uniforme dans toute la Belgique compte tenu de la mobilité des citoyens, par la volonté de ne pas ralentir le fonctionnement des centres de contact et par celle de réduire le risque de fuites de données :

« Afin de rendre le traitement des données de ce suivi manuel des contacts uniforme dans toute la Belgique, Sciensano, l'Institut belge de santé publique, a été chargé de rassembler les

données de santé et les coordonnées des patients auprès des médecins, des laboratoires et des hôpitaux dans une base de données centrale unique.

Une base de données centrale est nécessaire compte tenu de la mobilité des citoyens à travers les différentes entités fédérées. La tenue de différentes bases de données par entité fédérée impliquerait donc une interaction entre ces bases de données dès que de tels déplacements auraient lieu. Sur le plan pratique, cette interaction pourrait ralentir le fonctionnement des centres de contact puisqu'ils devraient attendre les contributions des autres entités fédérées. En outre, le transfert régulier de données à caractère personnel entre différentes bases de données décentralisées comporte un risque beaucoup plus élevé de fuites des données. Dans l'optique d'une politique plus sûre et plus efficace, l'objectif du présent accord de coopération est avant tout de fournir la base juridique pour cette base de données centrale.

Cette base de données centrale au sein de Sciensano, qui sera mise en place sur la base du présent accord de coopération (ci-après ' Base de données I '), permettra l'échange de données avec les bases de données qui seront créées pour soutenir les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes. Ces dernières, également des bases de données centralisées (ci-après dénommées ' Base de données III et IV '), seront également créées dans le cadre du présent accord de coopération.

L'organisation des bases de données repose sur les principes de protection des données dès la conception et par défaut sur la minimisation des données. Le stockage multiple des mêmes données à caractère personnel dans des bases de données de différentes entités fédérées est évité.

Du point de vue de la technologie de l'information, chaque base de données dispose naturellement de son propre modèle de données sous-jacent. Différents modèles de données donnent lieu à différentes bases de données.

La Base de données I est nécessairement une base de données commune à toutes les entités fédérées car le suivi des contacts ne peut se limiter aux personnes ressortant d'une seule entité fédérée. L'organisation d'une base de données par entité fédérée aurait pour conséquence que chaque région ou communauté devrait gérer sa propre duplication de l'ensemble de la base de données, et il faudrait une synchronisation permanente, avec le risque de fuites de données que cela implique. Ceci est contraire aux principes de minimisation des données et de sécurité des informations prévus dans le Règlement Général sur la Protection des Données.

L'organisation d'une base de données par entité fédérée aurait une incidence négative fondamentale sur le délai d'exécution de l'ensemble du suivi manuel des contacts. En effet, les différentes opérations visant à organiser l'échange de données entre les différentes bases de données des entités fédérées prendraient tellement de temps que cela ralentirait l'ensemble du processus (du suivi des personnes devant passer un test de dépistage du coronavirus COVID-19 à la prise de contact avec les Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID-19 a révélé qu'elles sont infectées, et les Personnes de catégorie III).

La Base de données III est une banque de données distincte qui ne contient que les instructions (d'appel) destinées au personnel des centres de contact. Cette base de données dispose d'un modèle de données différent de la Base de données I et constitue donc une base

de données distincte. Du reste, la distinction entre les Bases de données I et III constitue une mesure de protection des données dès la conception qui permet d'éviter que le personnel des centres de contact ne dispose d'un accès indu aux données de santé contenues dans la Base de données I. La Base de données III est une base de données commune aux centres de contact pour la même raison que la Base de données I est une base de données commune aux entités fédérées.

La base de données IV est une base de données distincte contenant des informations sur les collectivités et les personnes de contact des collectivités. Cette base de données dispose d'un modèle de données différent de celui des Bases de données I et III et constitue donc une base de données distincte.

Afin de permettre aux services d'inspection d'hygiène et aux équipes mobiles de remplir correctement les tâches qui leur sont confiées (notamment l'identification et la détection des foyers du coronavirus COVID-19 et clusters, la prise de mesures sur place pour contenir les foyers du coronavirus COVID-19 et les clusters), il est également nécessaire de prévoir un échange de données entre la Base de données I et les services d'inspection d'hygiène, ainsi qu'avec les équipes mobiles » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, pp. 65-69).

B.24.4. Dans son avis n° 64/2020 du 20 juillet 2020 sur le projet d'accord de coopération devenu l'accord de coopération du 25 août 2020, l'Autorité de protection des données a indiqué que la création d'une base de données centrale auprès de Sciensano semblait nécessaire et proportionnée au regard de ces justifications :

« À ce stade, les justifications avancées dans le commentaire général accompagnant le présent projet semblent justifier la nécessité et la proportionnalité de la création d'une base de données centrale auprès de Sciensano (du moins dans son principe) » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/002, p. 8).

B.24.5. La centralisation des données à caractère personnel relatives aux contaminations par le coronavirus, pour les besoins de la lutte contre la propagation du COVID-19, est justifiée en l'espèce pour des motifs de sécurité et d'intégrité des données et de rapidité du traçage manuel des personnes potentiellement contaminées. La centralisation des données, au lieu de leur enregistrement dans des bases de données séparées gérées par les centres de contacts, offre davantage de garanties en ce qui concerne leur sécurité et leur intégrité. Le risque d'abus ainsi que le risque de retard seraient plus élevés si les données à caractère personnel relatives aux contaminations par le COVID-19 étaient intégrées dans une banque de données séparée gérée par chaque centre de contact du pays.

B.25. Selon l’article 4, point 7), du RGPD, le responsable du traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

Le responsable du traitement est donc celui qui a la capacité de déterminer les finalités et les moyens du traitement des données.

Sciensano satisfait à ce double critère en ce qui concerne le traitement, pour la finalité de recherche scientifique, des données à caractère personnel pseudonymisées de la base de données II qui sont issues de la base de données I, compte tenu des missions légales qui lui sont confiées par l’article 4, précité, de la loi du 25 février 2018 « portant création de Sciensano ».

Il ressort en revanche de ce qui a été dit en B.14.2 et B.17 que les centres de contact désignés par les entités fédérées ou leurs agences effectuent le traitement des données à caractère personnel de la base de données III qui sont en partie issues de la base de données I pour la finalité de traçage manuel des contacts et pour la finalité de prévention, tandis que les équipes mobiles et les services d’inspection d’hygiène des autorités fédérées effectuent le traitement des données de la base de données I pour la finalité de prévention.

L’article 26 du RGPD prévoit que, lorsque les finalités et les moyens du traitement sont déterminés par plusieurs responsables du traitement, ceux-ci sont les responsables conjoints du traitement. Les obligations respectives des responsables conjoints du traitement sont définies dans un accord (paragraphe 1) dont les « grandes lignes » sont mises à la disposition de la personne concernée (paragraphe 2). Celle-ci peut exercer les droits que lui confère le RGPD à l’égard de chacun des responsables du traitement (paragraphe 3).

Dès lors que les équipes mobiles et les services d’inspection d’hygiène traitent les données à caractère personnel de la base de données I, les entités fédérées compétentes ou leurs agences

sous l'autorité desquelles travaillent ces équipes et services doivent être désignés responsables conjoints du traitement de la base de données I, aux côtés de Sciensano au sens de l'article 26 du RGPD. Compte tenu des liens étroits entre les bases de données I et III, les entités fédérées compétentes ou leurs agences sous l'autorité desquelles travaillent les centres de contact doivent également être désignées responsables conjoints du traitement de la base de données I au sens de l'article 26 du RGPD.

B.26. Le moyen unique, en sa première branche, est fondé dans la mesure visée en B.20.4. et dans la mesure visée en B.25.

Les actes attaqués doivent être annulés en tant qu'ils portent assentiment, d'une part, aux articles 2, § 3, et 15, § 1er et § 3, deuxième phrase, de l'accord de coopération du 25 août 2020, en ce que ces dispositions ne prévoient pas un délai maximal de conservation des données à caractère personnel enregistrées dans la base de données IV et, d'autre part, à l'article 2, § 4, du même accord de coopération en ce que cette disposition ne prévoit pas que les entités fédérées compétentes ou leurs agences sous l'autorité desquelles travaillent les centres de contact, les équipes mobiles et les services d'inspection d'hygiène sont responsables conjoints du traitement de la base de données I.

II. En ce qui concerne la nécessité de collecter certaines catégories de données (deuxième branche)

B.27. Dans la deuxième branche du moyen unique, les parties requérantes font valoir que les articles 6 à 9 de l'accord de coopération du 25 août 2020 entraînent une ingérence disproportionnée dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel dès lors que ces dispositions prévoient la collecte de certaines données à caractère personnel non nécessaires au regard de la finalité de traçage manuel des contacts (premier grief). Par ailleurs, le choix de pseudonymiser les données traitées à des fins de recherche ne serait pas justifié (second grief).

B.28. Les parties requérantes font valoir que la collecte, dans la base de données I, du numéro d'identification à la sécurité sociale (ci-après : le NISS), des données à caractère personnel issues du registre national, du résultat du CT-scan et de la langue de la personne concernée n'est pas nécessaire pour la finalité de traçage manuel des contacts. Il en irait de même pour les données à caractère personnel collectées dans la base de données I concernant les personnes de catégorie III.

B.29.1. L'accord de coopération du 25 août 2020 prévoit la collecte du NISS dans la base de données I pour les personnes de catégories I à IV (article 6, § 2, alinéa 1er, 1°, § 3, 1°, § 4, alinéa 1er, 1°, et § 5, 1°).

Comme le précise l'article 1er, § 1er, 11°, de l'accord de coopération, le NISS est le numéro d'identification visé à l'article 8, § 1er, 1° ou 2°, de la loi du 15 janvier 1990 « relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale ». Il s'agit, pour les personnes physiques enregistrées dans le registre national, du numéro d'identification du registre national et, pour les personnes physiques non enregistrées dans le registre national, du numéro d'identification de la Banque-carrefour de la sécurité sociale.

Le choix d'utiliser le NISS est justifié dans l'exposé général de l'accord de coopération comme suit :

« En vue de l'identification univoque des personnes concernées (c'est-à-dire les patients hospitalisés, les personnes infectées ou les personnes sérieusement suspectées d'être infectées) et de la mise en relation des données collectées, il est absolument indispensable de conserver également le numéro d'identification de sécurité sociale des personnes concernées dont les données sont traitées dans la base de données I et de permettre un accès général au Registre national. Cela soulage également les médecins, les hôpitaux et les laboratoires qui mettent les informations à disposition (c'est-à-dire les fournisseurs d'information), car ils n'ont à fournir que les données qui ne figurent pas dans le Registre national. Étant donné que l'ensemble du système de soins de santé en Belgique repose sur l'utilisation du numéro de Registre national pour identifier effectivement un patient, ce numéro est également essentiel pour le traitement dans le cadre du suivi manuel des contacts, en vue d'identifier correctement la personne index ainsi que les personnes avec lesquelles la personne index est entrée en contact. L'inclusion du numéro d'identification de sécurité sociale entraîne nécessairement l'enregistrement de la date de naissance des personnes concernées dont les données sont sauvegardées dans la Base de données I.

L'utilisation obligatoire du numéro d'identification à la sécurité sociale comme numéro d'identification unique dans le secteur des soins de santé est également régie par l'article 8 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth. Dans son arrêt 29/2010 du 18 mars 2010, la Cour constitutionnelle a estimé que ' [compte] tenu des garanties prévues par la loi du 21 août 2008 quant à la confidentialité des données à caractère personnel relatives à la santé au cours de leur traitement par la plate-forme eHealth, le choix de recourir au numéro du Registre national comme clé d'identification est raisonnablement justifié » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, pp. 82-84).

La collecte du NISS dans la base de données I comme clé d'identification des personnes de catégories I à IV est ainsi raisonnablement justifiée.

B.29.2. L'article 6, § 2, alinéa 2, § 3, 1°, et § 4, alinéa 2, de l'accord de coopération prévoit en outre que les noms et prénom, date de naissance, sexe et adresse des personnes de catégories I à III sont collectées dans la base de données I à partir du registre national ou des registres de la Banque-carrefour de la sécurité sociale.

Il en résulte que l'accès à ces registres doit permettre de recueillir uniquement des données à caractère personnel visant à identifier les personnes (potentiellement) infectées ou présumées l'être, ce qui est nécessaire à la poursuite de la finalité de traçage manuel des contacts.

B.30.1. L'accord de coopération prévoit également que « le résultat du CT-scan » peut être enregistré dans la base de données I pour la personne de catégorie I qui est hospitalisée (article 6, § 2, alinéa 1er, 12°), le « CT scan » désignant une technique d'imagerie médicale. Selon les parties requérantes, la collecte de cette catégorie de données poursuit uniquement la finalité de recherche scientifique, et non celle de traçage manuel des contacts.

B.30.2. En vertu du principe de 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). Conformément au principe de minimisation des données,

ces données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies (article 5, paragraphe 1, point c), du RGPD).

B.30.3. L'exposé général de l'accord de coopération indique :

« Les catégories de données à caractère personnel collectées sont les suivantes : des données d'identification et de contact, données relatives aux tests de dépistage, prescriptions, résultats des examens par CT-scans et diagnostics présumés des personnes, d'une part, et des données relatives aux personnes infectées ou sérieusement suspectées d'être infectées ainsi qu'aux patients hospitalisés dont le diagnostic du coronavirus COVID-19 a été confirmé dans les hôpitaux, d'autre part. […]

En ce qui concerne les tests de dépistage du coronavirus COVID-19, non seulement les résultats des tests de dépistage du coronavirus COVID-19 sont importants, mais le type de test de dépistage du coronavirus COVID-19 prescrit et/ou effectué, ainsi que la date du test de dépistage du coronavirus COVID-19, sont également indispensables. D'une part, pour déterminer si un patient est infecté ou non et, d'autre part, pour permettre aux chercheurs de mener des recherches qualitatives et statistiques supplémentaires sur les tests de dépistage du coronavirus COVID-19. Une infection par le coronavirus COVID-19 peut également être déduite des résultats des examens des CT-scans. La collecte de ces données permet d'obtenir plus de clarté sur l'évolution générale de la maladie du coronavirus COVID-19 chez un patient infecté » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, pp. 81-82).

B.30.4. Il en ressort que le résultat d'un examen réalisé par CT-scan est un élément d'imagerie médicale qui permet de constater de l'infection au coronavirus chez un patient. Sous réserve de l'interprétation selon laquelle le CT-scan visé à l'article 6, § 2, alinéa 1er, 12°, de l'accord de coopération est un CT-scan dont on peut déduire une infection au COVID-19, il peut être admis que l'enregistrement de cette donnée dans la base de données I est nécessaire à la poursuite de la finalité de traçage des contacts, laquelle suppose d'établir au préalable le statut des personnes infectées par le COVID-19.

B.31. L'accord de coopération prévoit en outre l'enregistrement, dans la base de données I, de la langue des personnes présumées infectées (personnes de catégorie III) (article 6, § 4, 12°), des personnes avec lesquelles les personnes testées positives et les personnes présumées infectées ont été en contact (personnes de catégorie IV), des personnes de catégorie II testées positives (article 6, § 5, 7°, et § 6) et des personnes faisant partie d'un *cluster* (article 6, § 7).

Il peut être admis que la mention de la langue de la personne concernée est nécessaire pour permettre aux centres de contact de contacter cette personne dans sa langue.

B.32.1. Selon l'article 1er, § 1er, 15°, de l'accord de coopération, les personnes de catégorie III sont « les personnes pour lesquelles le médecin a une présomption sérieuse d'infection par le coronavirus COVID–19, sans qu'un test de dépistage du coronavirus COVID–19 n'ait été effectué ou prescrit, ou lorsque le test de dépistage du coronavirus COVID–19 a révélé qu'elles n'étaient pas infectées ».

Comme il est dit en B.15.4, l'article 6, § 4, de l'accord de coopération détermine les données à caractère personnel relatives aux personnes de catégorie III qui sont enregistrées dans la base de données I par le médecin qui soupçonne la contamination.

B.32.2. Dans son avis n° 64/2020 du 20 juillet 2020 précité, l'Autorité de protection des données a observé :

« 42. Le projet prévoit la collecte et l'enregistrement, dans la Base de données I, de données à caractère personnel concernant des personnes présumées infectées (personnes de catégorie III). Si, dans un premier temps, au vu de la pénurie de tests permettant de confirmer une infection au coronavirus, il a pu sembler justifié de se contenter d'une forte présomption pour établir l'existence d'une infection au COVID-19, l'Autorité se demande si tel est toujours le cas aujourd'hui alors que les capacités de testing ont été très largement augmentées depuis le début de l'épidémie et qu'il apparait qu'aujourd'hui toutes les personnes pour lesquelles on suspecte une infection au COVID-19 devraient pouvoir être testées. L'Autorité se demande dès lors pourquoi le projet prévoit une collecte et un enregistrement de nombreuses données concernant les personnes présumées infectées dans la base de données I (et III).

43. Par ailleurs, comme l'Autorité a déjà eu l'occasion de le souligner dans ses avis n° 36/2020 et n° 42/2020, la donnée ' diagnostic présumé de contamination par le coronavirus COVID-19 ' peut difficilement être considérée comme une donnée exacte au sens de l'article 5.1.d) du RGPD » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/002, p. 17).

B.32.3. L'exposé général de l'accord de coopération indique :

« Un patient pour lequel il existe un soupçon sérieux qu'il est infecté par le coronavirus COVID-19, est un patient dont le médecin a déclaré que même sans test le patient présente des symptômes suffisants pour supposer l'infection ou dont le test de dépistage du coronavirus COVID-19 a montré que le patient n'est pas infecté, mais que le médecin ignore cette décision. Comme les deux diagnostics de soupçon de contamination sont établis par un

médecin et sont donc suffisamment fiables, il est nécessaire d'également désigner ces personnes présumées infectées en tant que personnes infectées et de les inclure dans la recherche de contacts. Le terme de personnes présumées infectées fait donc référence aux personnes désignées par un médecin comme personnes index mais qui n'ont pas été officiellement désignées comme infectées par un test » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, p. 84).

B.32.4. L'inclusion des personnes présumées infectées dans le système de traçage manuel des contacts a ainsi été justifiée par la fiabilité du diagnostic établi par le médecin. Afin de protéger la santé publique lors de la pandémie de COVID-19, les législateurs ont pu inclure dans le traçage manuel des contacts les personnes pour lesquelles un médecin a une forte suspicion clinique qu'elles sont infectées, en l'absence de test ou malgré un résultat négatif au test de dépistage.

Il découle par ailleurs de l'article 3, § 1er, 1°, et § 2, 1°, de l'accord de coopération que, contrairement à ce que soutiennent les parties requérantes, le traitement dans la base de données I des données à caractère personnel concernant les personnes de catégorie III poursuit bien la finalité de traçage manuel de contacts, et non uniquement la finalité de recherche scientifique.

B.33. En ce qui concerne le choix de pseudonymiser les données traitées à des fins de recherche, l'article 9 de l'accord de coopération énumère les catégories de données à caractère personnel de la base de données I qui sont enregistrées, après pseudonymisation, dans la base de données II en vue d'être utilisées à des fins de recherche scientifique.

Sur ce point, l'exposé général de l'accord de coopération mentionne :

« Il convient de continuer à garantir les fonctions de recherche épidémiologique existante. Il importera donc, sur la base des données fournies dans le cadre du suivi manuel des contacts de permettre aux institutions de recherche, y compris Sciensano, d'effectuer des études scientifiques ou statistiques liées à la propagation du coronavirus COVID-19 et/ou de soutenir la politique de lutte contre le coronavirus, grâce à l'échange de données entre la Base de données I et la base de données déjà en place au sein de Sciensano, laquelle est utilisée actuellement pour la recherche scientifique (ci-après ' Base de données II '). C'est une tâche qui relève de la compétence matérielle de l'État fédéral en matière de recherche scientifique. Le traitement des données à caractère personnel dans la Base de données I s'inscrit également dans le cadre des compétences fédérales en matière de recherche scientifique, comme il ressort de l'article 1er, § 2 de l'accord de coopération. À ce titre, il s'inscrit dans le cadre des missions

confiées à Sciensano par l'article 4 de la loi du 25 février 2018 ' portant création de Sciensano '. Seul l'échange de données à caractère personnel pseudonymisées dans le cadre de la recherche scientifique avec la base de données déjà existante de Sciensano (Base de données II) est donc régi par l'accord de coopération. L'établissement de règles relatives à la mise en œuvre de la recherche scientifique même ne relève donc pas du champ d'application de l'accord de coopération.

En ce qui concerne cet échange de données, on opte pour la pseudonymisation plutôt que pour l'anonymisation car il n'est pas possible de déterminer préalablement quelles données sont nécessaires pour mener une recherche scientifique particulière. Il semble donc approprié de ne pas priver les données de leur valeur potentielle lorsqu'elles sont enregistrées dans la Base de données II, mais aussi de protéger autant que possible les données à caractère personnel des personnes concernées. Comme l'a souligné le Comité européen de la protection des données, le nouveau concept de pseudonymisation tel que défini pour la première fois dans le Règlement Général sur la Protection des Données constitue un mécanisme de protection approprié. Ce concept de pseudonymisation impose également de prendre des mesures techniques et organisationnelles appropriées, conformes à la minimisation des données et à la protection des données dès la conception. La plateforme eHealth sera responsable dans ce cadre de la pseudonymisation des données à caractère personnel. Cette pseudonymisation a lieu lorsque et avant que les données à caractère personnel de la Base de données I sont partagées avec la Base de données II. Il n'est donc pas question de données pseudonymisées dans la Base de données I, parce que cela n'est pas techniquement faisable et parce qu'il convient toujours de satisfaire aux principes imposés par le Règlement Général sur la Protection des Données » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, pp. 69-71).

Il en ressort que le choix de pseudonymiser les données à caractère personnel enregistrées dans la base de données II plutôt que de les anonymiser est raisonnablement justifié.

B.34. Sous réserve de l'interprétation mentionnée en B.30.4, le moyen unique, en sa deuxième branche, n'est pas fondé.

III. En ce qui concerne l'habilitation conférée au Comité de sécurité de l'information d'autoriser la communication de données à caractère personnel à des tiers (troisième branche)

B.35.1. Dans la troisième branche du moyen unique, les parties requérantes font valoir que les articles 11 et 12 de l'accord de coopération du 25 août 2020 méconnaissent le principe de légalité contenu dans l'article 22 de la Constitution, en ce qu'ils habilitent le Comité de sécurité de l'information à déterminer les éléments essentiels liés à la communication de données à caractère personnel à des tiers. Selon les parties requérantes, les délibérations du Comité de sécurité de l'information ne peuvent pas être considérées comme une « loi » au sens de l'article 6, paragraphe 2, de l'article 9, paragraphe 2, point i), et de l'article 9, paragraphe 4, du

RGPD. Par ailleurs, la compétence d'autorisation du Comité de sécurité de l'information ne peut pas être justifiée sur la base de l'article 36, paragraphe 5, du RGPD dès lors que ce Comité ne peut pas être considéré comme une autorité de contrôle.

B.35.2. Le grief des parties requérantes porte uniquement sur la délégation accordée au Comité de sécurité de l'information quant à la communication de données à caractère personnel à des tiers. Cette mesure est visée à l'article 11, § 1er, de l'accord de coopération du 25 août 2020, lu en combinaison avec son article 10, § 3, seconde phrase.

La Cour limite son examen à ces dispositions.

B.36.1. L'article 11, § 1er, de l'accord de coopération du 25 août 2020 dispose :

« Dans la mesure où cela n'est pas repris dans le présent accord de coopération, tant la communication de données à caractère personnel par type d'acteur à Sciensano pour traitement dans la Base de données I que la communication ultérieure de ces données à caractère personnel par Sciensano à des tiers tels que prévus dans l'article 10 ont toujours lieu après délibération de la Chambre sécurité sociale et santé du Comité de sécurité de l'information visée dans 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 Général sur la Protection des Données ».

L'article 10, § 3, seconde phrase, dispose :

« Les données à caractère personnel telles que communiquées et conservées dans la Base de données II, ne peuvent être transmises à des tiers aux fins stipulées à l'article 3, § 1er, 4° qu'après la délibération, visée à l'article 11, de la Chambre sécurité sociale et santé du Comité de sécurité de l'information ».

L'article 3, § 1er, 4°, dispose :

« Le traitement des données à caractère personnel de la Base de données I vise les finalités de traitement suivantes :

[…]

4° la mise à disposition de données à caractère personnel pseudonymisées relevant des catégories de données à caractère personnel, relatives aux Personnes de catégories I à V, visées à l'article 6 conformément aux dispositions de l'article 10, à la base de données II déjà existante, afin de mettre les données pseudonymisées visées au présent alinéa après

anonymisation, ou au moins pseudonymisation dans le cas où l'anonymisation ne permettrait pas aux institutions de recherche d'effectuer leur étude scientifique ou statistique, à la disposition des institutions de recherche, dont Sciensano, selon la procédure prévue à cet effet afin de permettre aux institutions de recherche d'effectuer des études scientifiques ou statistiques sur la lutte contre la propagation du coronavirus COVID–19 et/ou, après pseudonymisation, de soutenir la politique dans ce domaine 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 ».

B.36.2. L'article 11, § 1er, de l'accord de coopération du 25 août 2020, lu en combinaison avec son article 10, § 3, seconde phrase, habilite la chambre « sécurité sociale et santé » du Comité de sécurité de l'information à autoriser, par voie de délibérations, la communication à des tiers des données à caractère personnel pseudonymisées enregistrées dans la base de données II « aux fins stipulées à l'article 3, § 1er, 4° », c'est-à-dire à des fins de recherche scientifique.

B.36.3. En ce qui concerne l'habilitation contenue dans les articles 10, § 3, et 11, § 1er, du projet d'accord de coopération, l'Autorité de protection des données a émis les observations suivantes :

« 58. L'article 10 § 3 du projet prévoit que ' […] Les données à caractère personnel telles que communiquées et conservées dans la Base de données II, ne peuvent être transmises à des tiers aux fins stipulées à l'article 3, § 1, 4° qu'après la délibération, visée à l'article 11, de la Chambre " Sécurité sociale et Santé " du Comité de sécurité de l'information '. L'Autorité rappelle qu'aux termes des principes de transparence et de légalité, la norme encadrant une communication de données – en tout cas lorsque celle-ci […] constitue une ingérence importante dans les droits et libertés des personnes concernées – doit déterminer les destinataires ou, en tout cas, les catégories de destinataires auxquelles ces données peuvent être communiquées. Les auteurs du projet devraient dès lors identifier, à tout le moins, les catégories de tiers auxquels ces données peuvent être communiquées.

59. L'article 11 § 1er du projet prévoit que ' Dans la mesure où cela n'est pas repris dans le présent accord de coopération, tant la communication de données à caractère personnel à Sciensano pour traitement dans la Base de données I que la communication ultérieure de ces données à caractère personnel par Sciensano à des tiers ont toujours lieu après délibération de la Chambre " Sécurité sociale et Santé " du Comité de sécurité de l'information visé dans 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 Général sur la Protection des Données '.

60. L'Autorité rappelle, comme elle l'a déjà fait dans ses avis n^{os} 36/2020 et 42/2020, que ni l'article 8 de la CEDH, ni l'article 22 de la Constitution, ni le RGPD, en particulier l'article 6.3, ne permettent un tel ' chèque en blanc '. Comme l'Autorité l'a déjà souligné plus haut, tout traitement (y compris donc toute communication) de données à caractère personnel

susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, comme c'est le cas, en l'espèce, doit être encadré spécifiquement par un texte législatif ou réglementaire (arrêté), et donc pas par une délibération du Comité de sécurité de l'information. L'Autorité rappelle que cette règlementation doit être précise et définir, au moins, les éléments essentiels du traitement, dont les finalités déterminées, explicites et légitimes; les (catégories de) données à caractère personnel qui sont pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités poursuivies; le délai de conservation maximal des données à caractère personnel enregistrées; la désignation du responsable du traitement; les destinataires ou catégories de destinataires auxquels les données sont communiquées et les circonstances dans lesquelles et les raisons pour lesquelles elles seront communiquées.

61. L'accord de coopération doit donc déterminer lui-même quels sont les ' tiers ' à qui Sciensano peut communiquer des données qu'il désigne et les raisons pour lesquelles ces données leur seront communiquées. Certainement au vu de la quantité et de la sensibilité des données en question (données relatives à la santé, données relatives à une présomption d'infection suite à un contact) et de la possibilité pour leurs destinataires potentiels d'effectuer des recoupements entre ces différents types de données » (*Doc. parl*., Chambre, 2019-2020, DOC 55-1490/002, pp. 21-22).

B.36.4. L'exposé général de l'accord de coopération du 25 août 2020 mentionne :

« Les données pseudonymisées contenues dans la Base de données II ne peuvent être transférées à des tiers que dans le cadre d'études scientifiques ou statistiques relatives à [la] lutte contre la propagation du coronavirus COVID-19 et/ou pour soutenir les politiques dans ce domaine. Ce transfert n'est possible qu'après délibération de la Chambre ' sécurité sociale et santé ' du Comité de sécurité de l'information » (*Doc. parl*., Chambre, 2019-2020, DOC 55-1490/001, pp. 93-94).

« Une délibération de la Chambre ' sécurité sociale et santé ' du Comité de sécurité de l'information est aussi requise pour l'échange des données de la Base de données II avec des tiers à des fins de recherche scientifique. Toutefois, l'octroi d'accès à des tiers pour la recherche scientifique ne relève pas du champ d'application de l'accord de coopération et ne sera donc pas traité plus en détail dans le présent accord de coopération » (*ibid*., pp. 96-97).

B.37.1. Comme il est dit en B.11.2, 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.37.2. 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 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.

L'article 36, paragraphe 5, dispose que le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la santé publique.

B.38.1. 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 11, § 1er, de l'accord de coopération du 25 août 2020, lu en combinaison avec son article 10, § 3, seconde phrase, (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.38.2. Il ressort de ce qui précède que 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.39. Comme la section de législation du Conseil d'État l'a observé dans son avis n° 63.202/2 du 26 avril 2018 sur l'avant-projet de loi devenu la loi du 5 septembre 2018, « le RGPD impose l'indépendance de l'autorité de contrôle et non celle des autorités publiques qui, ne recevant pas le statut d'une telle autorité de contrôle, traitent des données personnelles ou autorisent de tels traitements et doivent précisément être soumises au contrôle de l'autorité de contrôle » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3185/001, p. 129). 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 11, § 1er, de l'accord de coopération du 25 août 2020, lu en combinaison avec son

article 10, § 3, seconde phrase, 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.

Les législateurs ont en outre délégué des éléments essentiels de la communication à des tiers des données à caractère personnel mentionnée en B.36.2, en ne déterminant pas les destinataires de cette communication.

B.40. Les actes attaqués doivent être annulés en tant qu'ils portent assentiment à l'accord de coopération du 25 août 2020 en ce que son article 11, § 1er, contient les mots « tant » et « que la communication ultérieure de ces données à caractère personnel par Sciensano à des tiers tels que prévus dans l'article 10 » et en tant qu'ils portent assentiment à l'article 10, § 3, seconde phrase, du même accord de coopération.

IV. En ce qui concerne l'information fournie par les centres de contacts aux médecins traitants (quatrième branche)

B.41. Dans la quatrième branche du moyen unique, les parties requérantes font grief à l'article 3, § 1er, 2°, B, de l'accord de coopération du 25 août 2020 de prévoir que les médecins traitants sont informés de l'état de santé des personnes de catégories II et III sans le consentement des personnes concernées.

B.42. Les médecins traitants des personnes des catégories I, II et III sont les personnes de catégorie V au sens de l'article 1er, § 1er, 17°, de l'accord de coopération du 25 août 2020. Si cette catégorie de personnes était initialement visée par l'article 3, § 1er, 2°, B, du projet d'accord de coopération, elle ne figure plus dans l'article 3, § 1er, 2°, B, de l'accord de coopération du 25 août 2020 finalement adopté, qui dispose :

« Le traitement des données à caractère personnel de la Base de données I vise les finalités de traitement suivantes :

[…]

B. La mise à disposition par la Base de données I au centre de contact compétent des catégories de données à caractère personnel définies à l'article 7, § 4, au travers d'un échange

avec la Base de données III, en vue de contacter les Personnes de catégories VI par tout moyen de communication possible, y compris par téléphone, par courrier électronique ou par visite à la collectivité, afin de les informer de la contamination (présumée) des (i) Personnes de catégorie II dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles étaient infectées, et (ii) des Personnes de catégorie III ».

Les « personnes de catégorie VI » sont, conformément à l'article 1er, § 1er, 18°, du même accord de coopération « le médecin de référence - ou, en l'absence de médecin de référence au sein de la collectivité concernée - le responsable administratif des collectivités avec lesquelles les Personnes des catégories I, II et III ont été en contact au cours d'une période de quatorze jours avant à quatorze jours après les premiers symptômes de l'infection par le coronavirus COVID–19, une certaine marge d'appréciation pouvant être prise en compte sur la base des connaissances scientifiques ».

B.43. En ce qu'il repose sur une prémisse erronée, le moyen unique, en sa quatrième branche, n'est pas fondé.

V. En ce qui concerne la finalité de recherche scientifique (cinquième branche)

B.44. Dans la cinquième branche du moyen unique, les parties requérantes font valoir que l'article 3, § 1er, 4°, de l'accord de coopération du 25 août 2020 viole le principe de limitation des finalités et le principe de minimisation des données en ce que la finalité de recherche scientifique est erronément considérée comme une finalité primaire du traitement, et non comme une finalité ultérieure.

B.45. Le principe de limitation des finalités visé à l'article 5, paragraphe 1, point b), du RGPD a deux composantes. Il exige, d'une part, que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes et, d'autre part, que ces données ne soient pas « traitées ultérieurement d'une manière incompatible avec ces finalités ». La même disposition prévoit que « le traitement ultérieur […] à des fins de recherche scientifique […] n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales ».

B.46. L'article 3, § 1er, 4°, de l'accord de coopération du 25 août 2020 dispose :

« Le traitement des données à caractère personnel de la Base de données I vise les finalités de traitement suivantes :

[…]

4° la mise à disposition de données à caractère personnel pseudonymisées relevant des catégories de données à caractère personnel, relatives aux Personnes de catégories I à V, visées à l'article 6 conformément aux dispositions de l'article 10, à la base de données II déjà existante, afin de mettre les données pseudonymisées visées au présent alinéa après anonymisation, ou au moins pseudonymisation dans le cas où l'anonymisation ne permettrait pas aux institutions de recherche d'effectuer leur étude scientifique ou statistique, à la disposition des institutions de recherche, dont Sciensano, selon la procédure prévue à cet effet afin de permettre aux institutions de recherche d'effectuer des études scientifiques ou statistiques sur la lutte contre la propagation du coronavirus COVID–19 et/ou, après pseudonymisation, de soutenir la politique dans ce domaine conformément au titre IV de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ».

B.47.1. Comme il est dit en B.14.2, la recherche scientifique constitue la troisième finalité du traitement des données à caractère personnel collectées dans la base de données I. Il ressort de cette disposition et du dispositif de l'accord de coopération du 25 août 2020 que les données de la base de données I ne sont toutefois pas directement utilisées pour la recherche scientifique. Elles ne sont traitées à cette fin que dans un second temps après avoir été enregistrées dans la base de données II sous une forme pseudonymisée.

Le traitement des données à caractère personnel à des fins de recherche scientifique effectué en vertu de l'accord de coopération du 25 août 2020 constitue dès lors un « traitement ultérieur » de données au sens de l'article 5, paragraphe 1, point b), du RGPD. Conformément à la même disposition, ce traitement ultérieur est présumé être compatible avec les finalités initiales du traitement que sont, en l'espèce, la finalité de traçage manuel des contacts et la finalité de prévention.

B.47.2. Contrairement à ce que soutiennent les parties requérantes, la circonstance que le traitement de données à caractère personnel à des fins de recherche scientifique prévu par l'accord de coopération du 25 août 2020 est un traitement ultérieur de données n'emporte pas que ce traitement doive se fonder sur le consentement de la personne concernée.

Comme le considérant n° 50 du RGPD le mentionne, en cas de traitement ultérieur compatible avec les finalités initiales, « aucune base juridique distincte de celle qui a permis la collecte des données à caractère personnel n'est requise ». Il en découle que les bases de licéité qui fondent la collecte de données à caractère personnel dans la base de données I pour les finalités initiales de traçage manuel des contacts et de prévention servent également de bases de licéité au traitement ultérieur de ces données, après pseudonymisation, à des fins de recherche scientifique. En l'occurrence, ces bases de licéité peuvent être à la fois les intérêts vitaux de la personne concernée ou d'une autre personne physique (article 6, paragraphe 1, point d)), 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)), la médecine préventive (article 9, paragraphe 2, point h)) et des motifs d'intérêt public dans le domaine de la santé publique (article 9, paragraphe 2, point i)).

B.47.3. En ce qui concerne le grief des parties requérantes selon lequel le traitement de données à caractère personnel à des fins de recherche scientifique prévu par l'accord de coopération du 25 août 2020 aboutit à collecter des données à caractère personnel non nécessaires à la poursuite de la finalité de traçage manuel des contacts, il est renvoyé à l'examen de la deuxième branche du moyen unique.

B.48. Le moyen unique, en sa cinquième branche, n'est pas fondé.

VI. En ce qui concerne les liens entre la base de données I et la base de données V et la notion de « contacts à risque » (sixième et septième branches)

B.49. Dans les sixième et septième branches du moyen unique, les parties requérantes font valoir que l'article 14 de l'accord de coopération du 25 août 2020 méconnaît le droit au respect de la vie privée et le droit à la protection des données à caractère personnel en ce qu'il ne prévoit pas que les données contenues dans la base de données I sont uniquement destinées au traçage manuel des contacts à l'exclusion du traçage numérique de ceux-ci et en ce qu'il ne définit pas la notion de « contact à risque ».

B.50. Comme il est dit en B.1.2 et B.13.3, l'article 14 de l'accord de coopération du 25 août 2020, qui forme son chapitre VIII, fixe les règles relatives aux applications numériques de traçage des contacts. L'article 14, § 3, 2°, prévoit la création de la base de données V, définie à l'article 1er, § 1er, 10°, comme « le journal central des enregistrements de l'application numérique de traçage des contacts qui permet de contrôler le fonctionnement de l'application numérique de traçage des contacts, telle que décrite à l'article 14, et qui, à Sciensano, est séparée des Bases de données I et II ».

B.51.1. Les parties requérantes soutiennent d'abord que les liens entre la base de données I et la base de données V ne sont pas suffisamment clairs et que la base de données I viserait également l'objectif d'un traçage numérique des contacts.

B.51.2. Il résulte de l'article 1er, § 1er, 10°, précité, de l'accord de coopération du 25 août 2020 et de son exposé général que la base de données I est séparée de la base de données V et que Sciensano veille au respect de cette séparation. L'exposé général de l'accord de coopération indique :

« La question de savoir si une application numérique de traçage des contacts est utilisée ou non ne concerne que les données agrégées (c'est-à-dire la réponse affirmative ou négative à cette question) qui ne sont jamais reliées à l'application numérique de traçage des contacts elle-même. Si l'application numérique de traçage des contacts est utilisée par les personnes index et les personnes avec lesquelles ces personnes index ont été en contact, ces dernières ont déjà été informées concernant une contamination potentielle. Ces personnes ont en effet déjà été averties d'une contamination potentielle. L'enregistrement de ces données permet également de vérifier le fonctionnement de l'application numérique de traçage des contacts » ((*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, pp. 89-90).

« L'application mobile de l'application numérique de traçage des contacts enregistre les contacts entre les utilisateurs sans les identifier. La Base de données V permet à un utilisateur de transmettre volontairement et de manière contrôlée une infection identifiée et le moment probable de cette infection, afin que les autres utilisateurs puissent être informés s'ils ont été en contact avec l'utilisateur infecté pendant la période où il a été infecté, sans que l'identité de l'utilisateur infecté ou de l'autre utilisateur avec lequel il a été en contact puisse être identifiée » (*ibid.*, p. 115).

« Le présent accord de coopération prévoit que Sciensano est le responsable du traitement de la Base de données V. Sciensano doit s'assurer que les mesures techniques et organisationnelles nécessaires ont été prises pour cette base de données, et que les données de cette base de données ne sont pas croisées avec d'autres bases de données. Compte tenu de

l'expérience particulière de Sciensano en matière de protection des données lors du traitement de données de santé pour la recherche scientifique et de la mise en œuvre de telles méthodes de sécurisation et de pseudonymisation des données, Sciensano semble être le responsable le plus approprié pour effectuer ce traitement » (*ibid*., pp. 116-117).

Il peut par ailleurs être déduit des observations des autorités défenderesses que le renvoi, par l'article 2, § 1er, de l'accord de coopération du 25 août 2020, à l'article 1er, § 2, de celui-ci est erroné et qu'il doit se lire comme un renvoi à l'article 1er, § 2, 1° et 3°.

Comme il est dit en B.13.5, la base de données I est dès lors sans lien avec la base de données V.

B.51.3. Le moyen unique, en sa sixième branche, n'est pas fondé.

B.52.1. Les parties requérantes soutiennent ensuite que l'article 14 de l'accord de coopération ne définit pas la notion de « contact à risque ».

B.52.2. La notion de « contact à risque » est définie à l'article 1er, 10°, de l'accord de coopération d'exécution du 13 octobre 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts (ci-après : l'accord de coopération d'exécution du 13 octobre 2020), conformément à l'article 92*bis*, § 1er, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980, adopté en exécution de l'article 14, § 9, 2°, de l'accord de coopération du 25 août 2020.

L'article 14, § 9, 2°, de l'accord de coopération du 25 août 2020 dispose :

« Ce sont les entités fédérées qui décident quelle(s) application(s) mobile(s) sont mises à la disposition des utilisateurs dans le cadre du traçage de contacts par les autorités et qui en contrôlent la conformité avec la réglementation. Les procédures à cet égard, ainsi que la poursuite du fonctionnement de l'application numérique de traçage des contacts et les traitements de données utiles dans ce cadre sont réglés par un accord de coopération d'exécution visé à l'article 92*bis*, § 1er, alinéa 3, de la loi spéciale du 8 août 1980 de réformes institutionnelles, sans préjudice des dispositions du présent article. Cet accord de coopération d'exécution contient au minimum :

[…]

2° une description claire des traitements résultant de l'utilisation de l'application numérique de traçage des contacts et une définition claire des concepts importants tels que le contact à risque […] ».

L'article 1er, 10°, de l'accord de coopération d'exécution du 13 octobre 2020 dispose :

« Aux fins du présent accord, on entend par :

[…]

10° contact à risque: un contact pendant au moins quinze minutes à moins de deux mètres de distance avec une personne infectée; ce contact est établi lorsqu'un numéro de série temporaire non personnalisé correspondant à un numéro de série non personnalisé émis par le smartphone d'un utilisateur infecté est trouvé sur un smartphone ».

B.52.3. Le moyen unique, en sa septième branche, n'est pas fondé.

VII. En ce qui concerne la notion de « visite physique » (huitième branche)

B.53. Dans la huitième branche du moyen unique, les parties requérantes font valoir que l'article 3, § 1er, 2°, A, et § 2, 2°, A, de l'accord de coopération du 25 août 2020 ne satisfait pas au principe de finalité en ce qu'il ne définit pas la notion de « visite physique ».

B.54.1. L'article 3, § 1er, 2°, A, de l'accord de coopération du 25 août 2020 dispose :

« Le traitement des données à caractère personnel de la Base de données I vise les finalités de traitement suivantes :

[…]

2° A. la mise à disposition par la Base de données I au centre de contact compétent des catégories de données à caractère personnel définies à l'article 7, § 3, au travers d'un échange avec la Base de données III, en vue de contacter les Personnes de catégorie IV, par tout moyen de communication possible, en ce compris par téléphone, courrier électronique ou au moyen d'une visite physique, pour leur fournir des recommandations en matière d'hygiène et de prévention, leur proposer une quarantaine ou les inviter à se soumettre au test de dépistage du coronavirus COVID–19, en bénéficiant d'un suivi à ce niveau ».

L’article 3, § 2, 2°, A, dispose :

« Les centres de contact désignés par les entités fédérées ou les agences compétentes peuvent, dans la mesure où ils sont compétents et conformément à l’article 10, § 1er :

[…]

2° A. traiter les catégories de données à caractère personnel définies à l’article 7, § 3, aux fins de contacter les Personnes de catégorie IV par tout moyen de communication possible, y compris par téléphone, courrier électronique ou au moyen d’une visite physique, pour leur fournir, entre autres, des recommandations en matière d’hygiène et de prévention, leur proposer une quarantaine, ou les inviter à se soumettre au test de dépistage du coronavirus COVID–19, en bénéficiant d’un suivi ».

B.54.2. Comme il est dit en B.14.2, ces dispositions prévoient que les centres de contacts reçoivent, au moyen d’un échange de données entre la base de données I et la base de données III, les catégories de données à caractère personnel relatives aux personnes avec lesquelles les personnes testées positives et les personnes présumées infectées ont été en contact au cours d’une période de quatorze jours avant à quatorze jours après les premiers signes d’infection (personnes de catégorie IV) pour leur fournir des recommandations en matière d’hygiène et de prévention, leur proposer une quarantaine ou les inviter à se soumettre à un test de dépistage. Ces dispositions précisent que cette prise de contact peut intervenir « par tout moyen de communication possible, y compris par téléphone, courrier électronique ou au moyen d’une visite physique ».

L’article 3, § 1er, 1°, et § 2, 1°, de l’accord de coopération du 25 août 2020 autorise par ailleurs les centres de contacts à entrer en relation, notamment au moyen de visites physiques, avec les personnes de catégorie II testées positives et les personnes présumées infectées (personnes de catégorie III) pour leur donner d’éventuelles recommandations mais surtout pour leur demander de fournir des informations concernant les personnes avec lesquelles elles ont eu des contacts.

Selon l’article 1er, § 1er, 4°, du même accord de coopération, le centre de contact est l’« instance désignée par les entités fédérées compétentes ou par les agences compétentes pour contacter la personne concernée par tout moyen de communication, y compris par téléphone, par courrier électronique ou au moyen d’une visite physique dans le cadre des objectifs fixés à l’article 3, § 2, et qui partage ensuite les données collectées avec la base de données I ». Selon

son article 1er, § 1er, 20°, les enquêteurs de terrain sont « les collaborateurs des centres de contact qui peuvent effectuer des visites physiques dans le cadre du suivi des contacts ».

B.54.3. Dans son avis n° 64/2020 du 20 juillet 2020, précité, l'Autorité de protection des données a observé :

« 19. Tout d'abord, l'Autorité constate que le projet est beaucoup plus détaillé que les autres projets normatifs sur lesquels elle s'est déjà prononcée. L'Autorité remarque, en effet, que le projet cherche à clarifier, avec un grand degré de précision, les finalités qu'il poursuit, les données qui seront collectées et utilisées, ainsi que les flux de données qui seront mis en place.

20. Certains éléments doivent toutefois encore être clarifiés afin que l'accord de coopération encadre de manière suffisamment prévisible les traitements de données qu'il met en place. C'est, en particulier, le cas pour ce qui concerne les ' visites physiques ' qui pourront avoir lieu dans le contexte du suivi ' manuel ' des personnes (présumées) infectées et de leurs contacts.

21. Le projet entend, en effet, autoriser les ' centres de contact ' compétents à procéder à des ' visites physiques ' auprès des personnes de catégories II dont le test de dépistage du COVID-19 a révélé qu'elles étaient infectées, des personnes de catégories III [c.-à-d. les personnes présumées infectées] et des personnes de catégories IV [c.-à-d. les personnes ayant eu des contacts avec des personnes (présumées) infectées].

22. Actuellement, le projet n'apporte aucun encadrement spécifique de ces ' visites physiques ' qui constituent pourtant une ingérence importante dans le droit au respect de la vie privée des personnes concernées. Il conviendrait, afin que le projet réponde à l'exigence de prévisibilité qui s'impose à toute norme qui permet une interférence avec le droit au respect de la vie privée, que le projet détermine les conditions et les circonstances dans lesquelles une visite physique peut avoir lieu. Il faudrait, en particulier, que le projet détermine :

- les lieux dans lesquels ces visites peuvent avoir lieu (au domicile, sur le lieu de travail, …)

- les heures auxquelles elles peuvent avoir lieu

- les circonstances dans lesquelles elles peuvent avoir lieu, notamment, en indiquant si les centres de contacts doivent d'abord essayer de contacter les personnes concernées par des moyens moins intrusifs

- le caractère contraignant de telles visites. En d'autres termes, les personnes sont-elles contraintes d'ouvrir la porte aux personnes qui se rendraient chez elles (et si oui, des sanctions sont-elles prévues ?) ou ont-elles le choix de refuser d'ouvrir la porte si elles ne souhaitent pas donner des informations aux centres de contact ?

- le déroulement de ces visites et les données, y compris à caractère personnel, qui seront collectées à leur occasion (type de données, personnes concernées etc.)

23. Si la réponse à ces questions se trouvait dans d'autres législations, notamment régionales ou communautaires, il conviendrait de renvoyer explicitement et précisément aux dispositions qui encadrent ces ' visites physiques '. S'il n'existe aucune disposition de droit positif qui encadre de telles ' visites physiques ', il convient de prévoir un tel encadrement afin de permettre aux personnes concernées de connaitre les conditions et les circonstances dans lesquelles de telles visites peuvent avoir lieu.

24. L'Autorité estime que ces visites physiques ne peuvent être effectuées qu'afin de fournir à la personne visitée la même information que celle fournie aux personnes contactées par téléphone et que ces visites ne peuvent donner lieu à un contrôle du respect de recommandations précédemment fournies » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/002, pp. 9-10).

B.55.1. La visite physique effectuée par les enquêteurs de terrain en vertu de la disposition attaquée constitue une ingérence dans le droit au respect du domicile et de la vie privée.

B.55.2. Il ressort des dispositions mentionnées en B.54 et de l'exposé général de l'accord de coopération que la visite physique, qui exclut toute forme de contrainte, est un moyen subsidiaire dont disposent les enquêteurs de terrain pour contacter les personnes (présumées) infectées et leurs contacts afin de leur fournir des recommandations en matière d'hygiène et de prévention, de leur proposer une quarantaine ou de les inviter à se soumettre à un test de dépistage, lorsque le contact téléphonique ou électronique est impossible. Les modalités de mise en œuvre de ces visites sont par ailleurs déterminées par les réglementations des entités fédérées :

« Le centre de contact contacte non seulement les personnes dont les médecins ont de sérieux soupçons d'infection et celles dont le test de dépistage du coronavirus COVID-19 a révélé qu'elles étaient infectées, notamment les personnes index, mais aussi les personnes avec lesquelles elles ont eu des contacts étroits. Le centre de contact désigné par les entités fédérées compétentes ou par les agences compétentes reçoit ces données de la Base de données I auprès de Sciensano. En cas de contacts avec des personnes au sein d'une population fragile, le centre de contact prendra contact avec le médecin de référence ou, à défaut, avec le responsable administratif de cette collectivité pour un suivi complémentaire de la situation. Dans le cas de contacts avec des personnes individuelles, le centre de contact joint ces personnes par téléphone, leur donne ensuite les recommandations appropriées sur la base des informations qu'elles fournissent (rester chez soi, travailler à domicile, se faire tester, etc.) et confirme ces recommandations par voie électronique. Cet envoi électronique se résume à une confirmation des recommandations transmises oralement. Il est également possible que des enquêteurs de terrain effectuent des visites physiques aux personnes concernées lorsque le contact téléphonique ou électronique est impossible » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, pp. 91-92).

« Les règles spécifiques relatives à la mise en œuvre du traçage (comme […] les visites à domicile […]) ne relèvent […] pas du champ d'application de l'accord de coopération et sont régies par les réglementations applicables des autorités fédérées » (*ibid*., p. 64).

B.55.3. L'accord de coopération du 25 août 2020 vise uniquement à créer un cadre normatif pour le traitement conjoint de données par Sciensano, les centres de contact, les services d'inspections d'hygiène et les équipes mobiles dans le cadre du traçage des personnes (présumées) infectées par le COVID-19 et de leurs contacts. Eu égard à cet objectif, les précisions contenues dans l'accord de coopération et dans l'exposé général concernant le caractère subsidiaire de la visite physique par rapport au contact par téléphone et par courrier électronique et la finalité identique poursuivie par ces différentes modalités de contact rendent suffisamment prévisibles les circonstances dans lesquelles une telle visite peut être effectuée par les enquêteurs de terrain. Pour autant que, dans le cadre de leur compétence en matière de médecine préventive, les communautés aient omis de préciser les règles concernant l'exécution des visites physiques, cette omission ne résulterait pas des actes attaqués.

B.55.4. Compte tenu de ce qui est dit en B.55.2, le moyen unique, en sa huitième branche, n'est pas fondé.

VIII. En ce qui concerne l'obligation de secret des collaborateurs des centres de contact (neuvième branche)

B.56. Dans la neuvième branche du moyen unique, les parties requérantes soutiennent que l'accord de coopération du 25 août 2020 est contraire à l'article 9, paragraphe 2, point i), du RGPD en ce qu'il ne prévoit pas que les collaborateurs des centres de contact sont soumis au secret professionnel.

B.57. Comme il est dit en B.10.2, l'article 9, paragraphe 2, point i), du RGPD prévoit qu'en cas de traitement de données sensibles autorisé 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, le droit de l'Union ou celui de l'État membre prévoit des mesures appropriées

et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, « notamment le secret professionnel ».

B.58. Dans son avis n° 64/2020 du 20 juillet 2020 précité, l'Autorité de protection des données a observé :

« 25. Les traitements de données envisagés dans le projet portent, en partie, sur des données concernant la santé dont le traitement est, en principe, interdit (article 9.1 du RGPD). Toutefois, cette interdiction ne s'applique pas lorsque – comme c'est le cas en l'espèce – ' 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 ' (article 9.2.i) du RGPD).

26. À propos de cette exigence de secret, l'Autorité souligne que l'article 9.3°) de la LTD impose au responsable du traitement de données concernant la santé de veiller à ce que les personnes ayant accès aux données à caractère personnel concernant la santé, qu'il doit désigner, soient ' tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées '. Sauf erreur de l'Autorité, le projet ne crée, par contre, pas d'obligation spécifique de secret dans le chef des personnes (y compris celles travaillant dans les centres de contact) qui auront accès aux données relatives à la santé. Comme l'Autorité l'a déjà indiqué dans son avis n° 36/2020, l'Autorité estime qu'afin de préserver la confidentialité de l'identité et de l'état de santé des personnes identifiables dont les données à caractère personnel seront reprises dans les différentes bases de données créées par le projet, il est indiqué de prévoir dans le projet d'accord de coopération une disposition spécifique soumettant les personnes ayant accès à ces données au secret professionnel » (*Doc. parl*., Chambre, 2019-2020, DOC 55-1490/002, pp. 10-11).

B.59. Selon l'exposé général de l'accord de coopération du 25 août 2020, la soumission des collaborateurs des centres de contact au secret professionnel fait partie des règles relatives à la mise en œuvre du traçage manuel des contacts qui échappent au champ d'application de l'accord de coopération et qui sont régies par les réglementations des entités fédérées :

« Les règles spécifiques relatives à la mise en œuvre du traçage (comme […] la soumission des travailleurs des centres de contact au secret professionnel) ne relèvent […] pas du champ d'application de l'accord de coopération et sont régies par les réglementations applicables des autorités fédérées » (*Doc. parl.*, Chambre, 2019-2020, DOC 55-1490/001, p. 64).

B.60. Comme l’exposent les autorités défenderesses, les collaborateurs du centre de contact organisé auprès de l'Agence wallonne de la santé, de la protection sociale, du handicap et des familles sont soumis au secret professionnel en vertu de l’article 5 de l’arrêté du Gouvernement wallon de pouvoirs spéciaux n° 35 du 5 mai 2020 « organisant le tracing socio-sanitaire dans le cadre de la lutte contre l'épidémie COVID-19 ». Les collaborateurs du centre de contact central créé par la structure désignée par le Gouvernement flamand sont soumis au secret professionnel en vertu de l’article 3 du décret de la Communauté flamande du 29 mai 2020 « portant organisation du suivi des contacts centralisé par une structure de coopération de partenaires externes, du suivi des contacts local par les administrations locales ou les conseils des soins et portant organisation des équipes COVID-19 dans le cadre du COVID-19 ». Les collaborateurs du centre de contact créé par le Gouvernement de la Communauté germanophone sont soumis au secret professionnel en vertu de l’article 10.18, § 2, du décret de la Communauté germanophone du 1er juin 2004 « relatif à la promotion de la santé et à la prévention médicale », tel qu’il a été introduit par l’article 18 du décret du 20 juillet 2020 « relatif au suivi des chaines d'infection dans le cadre de la lutte contre la crise sanitaire provoquée par le coronavirus (COVID-19) ».

L’article 4, § 2, de l’arrêté de pouvoirs spéciaux du Collège réuni de la Commission communautaire commune n° 2020/006 du 18 juin 2020 « organisant le suivi sanitaire des contacts dans le cadre de la lutte contre la pandémie COVID-19 » interdit aux membres du centre de contact organisé auprès des services du Collège réuni de la Commission communautaire commune de divulguer les données à caractère personnel auxquelles ils ont accès ou de les utiliser à une autre fin. En vertu de l’article 13 du même arrêté, un manquement à cette interdiction est passible des sanctions pénales prévues à l’article 15 de l'ordonnance de la Commission communautaire commune du 19 juillet 2007 « relative à la politique de prévention en santé ».

Il en résulte que les collaborateurs des centres de contact sont tous soumis à une obligation légale de secret dont la méconnaissance est sanctionnée pénalement.

B.61. Dans l’interprétation selon laquelle les collaborateurs des centres de contact visés à l’article 1er, § 1er, 4°, de l’accord de coopération du 25 août 2020, y compris les enquêteurs de terrain visés dans son article 1er, § 1er, 20°, ont l’obligation de garder secrètes les données à caractère personnel dont ils ont connaissance dans l’exercice de leur mission conformément aux réglementations mentionnées en B.60, l’accord de coopération du 25 août 2020 ne viole pas le droit au respect de la vie privée et le droit à la protection des données à caractère personnel.

B.62. Sous réserve de l’interprétation mentionnée en B.61, le moyen unique, en sa neuvième branche, n’est pas fondé.

En ce qui concerne la demande de poser une question préjudicielle à la Cour de justice de l’Union européenne

B.63. Les parties requérantes suggèrent de poser à la Cour de justice une question préjudicielle sur l'interprétation du droit de l’Union.

L'examen des griefs invoqués n'a pas soulevé de doute concernant l'interprétation des dispositions du droit de l’Union applicables en l'espèce, si bien qu'il n'y a pas lieu d'accéder à la demande précitée.

En ce qui concerne la demande de maintien des effets

B.64. Les autorités défenderesses demandent le maintien des effets des actes attaqués en cas d’annulation.

B.65.1. 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 sur la Cour constitutionnelle (ci-après : la loi spéciale), le pouvoir d’annuler l’acte attaqué en tout ou en partie.

Lorsqu'elle annule, comme en l'espèce, une norme législative au motif que le législateur a omis de manière inconstitutionnelle de légiférer, 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.65.2. 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.

Toutefois, lorsque la Cour constate, au regard des moyens examinés, qu'un ensemble de mesures législatives est conforme à la Constitution lue en combinaison avec le RGPD, à l'exception de lacunes consistant en l'absence, contraire au RGPD, de l'établissement d'un délai maximal de conservation des données à caractère personnel enregistrées dans une base de données et de la désignation de certaines entités comme responsables conjoints du traitement de données, la Cour assure la protection du plein effet du droit de l'Union en imposant au législateur un bref délai dans lequel celui-ci doit mettre fin à l'inconstitutionnalité constatée.

B.65.3. Afin de préserver la sécurité juridique du traitement des données à caractère personnel effectué sur la base de l'accord de coopération du 25 août 2020, il y a lieu de maintenir les effets des actes attaqués, en tant qu'ils portent assentiment :

- aux articles 2, § 3, et 15, § 1er et § 3, deuxième phrase, de l'accord de coopération du 25 août 2020, jusqu'à ce que les législateurs concernés approuvent un accord de coopération complémentaire prévoyant un délai maximal de conservation des données à caractère personnel enregistrées dans la base de données IV, et au plus tard jusqu'au 31 mars 2023;

- à l’article 2, § 4, du même accord de coopération, jusqu’à ce que les législateurs concernés approuvent un accord de coopération complémentaire qui dispose que les entités fédérées compétentes ou leurs agences sous l’autorité desquelles travaillent les centres de contact, les équipes mobiles et les services d’inspection d’hygiène sont responsables conjoints du traitement de la base de données I, et au plus tard jusqu’au 31 mars 2023.

B.65.4. 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,

1) annule le décret de la Région wallonne du 30 septembre 2020, l'article 1er du décret de la Communauté germanophone du 12 octobre 2020, l'article 2 de la loi du 9 octobre 2020, l'ordonnance de la Commission communautaire commune du 1er octobre 2020 et le décret de la Communauté flamande du 2 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 », en tant qu'ils portent assentiment :

- aux articles 2, § 3, et 15, § 1er et § 3, deuxième phrase, de l'accord de coopération du 25 août 2020, en ce que ces dispositions ne prévoient pas un délai maximal de conservation des données à caractère personnel enregistrées dans la base de données IV;

- à l'article 2, § 4, du même accord de coopération, en ce que cette disposition ne prévoit pas que les entités fédérées compétentes ou leurs agences sous l'autorité desquelles travaillent les centres de contact, les équipes mobiles et les services d'inspection d'hygiène sont responsables conjoints du traitement de la base de données I;

- au même accord de coopération, en ce que son article 11, § 1er, contient les mots « tant » et « que la communication ultérieure de ces données à caractère personnel par Sciensano à des tiers tels que prévus dans l'article 10 »;

- à l'article 10, § 3, seconde phrase, du même accord de coopération;

2) sous réserve des interprétations mentionnées en B.30.4 et en B.61 et compte tenu de ce qui est dit en B.55.2, rejette les recours pour le surplus;

3) maintient les effets des actes annulés, en tant qu'ils portent assentiment :

- aux articles 2, § 3, et 15, § 1er et § 3, deuxième phrase, de l'accord de coopération du 25 août 2020, jusqu'à ce que les législateurs concernés approuvent un accord de coopération complémentaire prévoyant un délai maximal de conservation des données à caractère personnel enregistrées dans la base de données IV, et au plus tard jusqu'au 31 mars 2023 inclus;

- à l'article 2, § 4, du même accord de coopération, jusqu'à ce que les législateurs concernés approuvent un accord de coopération complémentaire qui dispose que les entités fédérées compétentes ou leurs agences sous l'autorité desquelles travaillent les centres de contact, les équipes mobiles et les services d'inspection d'hygiène sont responsables conjoints du traitement de la base de données I, et au plus tard jusqu'au 31 mars 2023 inclus.

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, le 22 septembre 2022.

Le greffier — le président,

P.-Y. Dutilleux — P. Nihoul