| |
|---|
| Numéros du rôle : 7125, 7150, 7202, 7203 et 7211 |
| Arrêt n° 2/2021<br>du 14 janvier 2021 |

# A R R Ê T

*En cause* : les recours en annulation de l'article 27 de la loi du 25 novembre 2018 « portant des dispositions diverses concernant le Registre national et les registres de population », introduits par le Parti Libertarien et Baudoin Collard, par Matthias Dobbelaere-Welvaert et autres, par l'ASBL « Liga voor Mensenrechten », par l'ASBL « Ligue des droits humains » et par Siham Najmi et John Pitseys en leur qualité de représentants légaux de leur fils Samuel Pitseys Najmi.

La Cour constitutionnelle,

composée des présidents F. Daoût et L. Lavrysen, et des juges T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman, M. Pâques, Y. Kherbache et T. Detienne, assistée du greffier P.-Y. Dutilleux, présidée par le président F. Daoût,

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 11 février 2019 et parvenue au greffe le 12 février 2019, un recours en annulation de l'article 27 de la loi du 25 novembre 2018 « portant des dispositions diverses concernant le Registre national et les registres de population » (publiée au *Moniteur belge* du 13 décembre 2018) a été introduit par le Parti Libertarien et Baudoin Collard, 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 22 mars 2019 et parvenue au greffe le 25 mars 2019, un recours en annulation de la même disposition légale a été introduit par Matthias Dobbelaere-Welvaert, Bert Cattoor, Johan Gielen et Antoon Lowette, assistés et représentés par Me G. Lenssens, avocat au barreau de Bruxelles.

c. Par requête adressée à la Cour par lettre recommandée à la poste le 12 juin 2019 et parvenue au greffe le 13 juin 2019, l'ASBL « Liga voor Mensenrechten », assistée et représentée par Me D. Pattyn, avocat au barreau de Flandre occidentale, et Me R. Fonteyn, a introduit un recours en annulation de la même disposition légale.

d. Par requête adressée à la Cour par lettre recommandée à la poste le 12 juin 2019 et parvenue au greffe le 13 juin 2019, l'ASBL « Ligue des droits humains », assistée et représentée par Me D. Pattyn et Me R. Fonteyn, a introduit un recours en annulation de la même disposition légale.

e. Par requête adressée à la Cour par lettre recommandée à la poste le 12 juin 2019 et parvenue au greffe le 17 juin 2019, un recours en annulation de la même disposition légale a été introduit par Siham Najmi et John Pitseys en leur qualité de représentants légaux de leur fils Samuel Pitseys Najmi, assistés et représentés par Me R. Fonteyn.

Ces affaires, inscrites sous les numéros 7125, 7150, 7202, 7203 et 7211 du rôle de la Cour, ont été jointes.

Des mémoires ont été introduits par :

- le Parti Libertarien et Baudoin Collard, assistés et représentés par Me R. Fonteyn (parties intervenantes dans l'affaire n° 7150);

- l'ASBL « Ligue des droits humains », assistée et représentée par Me R. Fonteyn (partie intervenante dans l'affaire n° 7150);

- le Conseil des ministres, assisté et représenté par Me P. Goffaux, Me D. D'Hooghe et Me M. Van Den Langenbergh, avocats au barreau de Bruxelles (dans toutes les affaires).

Les parties requérantes ont introduit des mémoires en réponse.

Le Conseil des ministres a également introduit des mémoires en réplique.

Par ordonnance du 23 septembre 2020, la Cour, après avoir entendu les juges-rapporteurs M. Pâques et Y. Kherbache, a décidé que les affaires étaient en état, qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de cette ordonnance, à être entendue, et qu'en l'absence d'une telle demande, les débats seraient clos le 7 octobre 2020 et les affaires mises en délibéré.

À la suite des demandes des parties requérantes dans les affaires n$^{os}$ 7150 et 7202 à être entendues, la Cour, par ordonnance du 7 octobre 2020, a fixé l'audience au 12 novembre 2020.

À l'audience publique du 12 novembre 2020 :

- ont comparu :

. Me D. Pattyn *loco* Me R. Fonteyn, pour les parties requérantes dans les affaires n$^{os}$ 7125 et 7211, et pour les parties intervenantes dans l'affaire n° 7150;

. Me D. Pattyn, pour les parties requérantes dans les affaires n$^{os}$ 7202 et 7203;

. Me G. Lenssens, pour les parties requérantes dans l'affaire n° 7150;

. Me P. Goffaux et Me M. Van Den Langenbergh, pour le Conseil des ministres;

- les juges-rapporteurs M. Pâques et Y. Kherbache 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 la recevabilité*

*En ce qui concerne la recevabilité du mémoire du Conseil des ministres dans l'affaire n° 7150*

A.1.1. Les parties requérantes dans l'affaire n° 7150 invoquent la nullité du mémoire du Conseil des ministres au motif qu'il comporte un ou plusieurs passages en anglais, non traduits, ce qui constitue une violation de l'article 40 de la loi du 15 juin 1935 « sur l'emploi des langues en matière judiciaire » et entraîne une violation des droits de la défense.

A.1.2. Le Conseil des ministres répond que son mémoire contient une traduction de tous les passages en anglais. Seule la légende d'un graphique n'est pas traduite, mais ce graphique est explicité dans le paragraphe qui le suit, lequel contient une traduction des termes utilisés.

*En ce qui concerne l'incidence de l'entrée en vigueur du règlement (UE) 2019/1157 sur la recevabilité des recours*

A.2.1. Le Conseil des ministres fait valoir que la loi attaquée doit être considérée comme la transposition anticipée du règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 « relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation » (ci-après : le règlement (UE) 2019/1157), les deux normes ayant une portée identique. Depuis l'entrée en vigueur de ce règlement, les parties requérantes n'ont, en tout état de cause, plus intérêt au recours. À supposer que la disposition attaquée soit annulée, le règlement sera toujours d'application et l'État belge sera toujours obligé d'enregistrer les empreintes digitales sur les cartes d'identité, de sorte que l'annulation ne pourrait conduire au résultat escompté par les parties requérantes. En toute hypothèse, la Cour n'est pas compétente pour se prononcer sur la validité d'un règlement européen.

A.2.2. Les parties requérantes dans les affaires n$^{os}$ 7202, 7203 et 7211 répondent qu'elles justifient bien d'un intérêt à leur recours dès lors que le règlement (UE) 2019/1157 ne sera applicable qu'à partir du 2 août 2021. Elles font en outre valoir que celui-ci n'est pas compatible avec les normes du droit de l'Union qui lui sont supérieures. Elles suggèrent donc d'interroger la Cour de justice de l'Union européenne à titre préjudiciel à propos de la validité du règlement.

La partie requérante dans l'affaire n° 7202 fait par ailleurs valoir que la compétence de la Cour de justice ne porte pas préjudice à la compétence de la Cour d'apprécier, le cas échéant, la compatibilité de la disposition attaquée avec le droit de l'Union, en ce compris avec le règlement (UE) 2019/1157 ou, en cas d'invalidation par la Cour de justice du règlement précité, de vérifier si le législateur pouvait, au regard de l'article 4, paragraphe 2, du Traité sur l'Union européenne (ci-après : le TUE) et de l'article 72 du Traité sur le fonctionnement de l'Union européenne (ci-après : le TFUE), adopter la disposition attaquée et, le cas échéant, si cette disposition est compatible avec les obligations des États membres en matière de protection des données à caractère personnel et de libre circulation des citoyens de l'Union.

A.2.3. Le Conseil des ministres répond que le règlement (UE) 2019/1157 est entré en vigueur le 1er août 2019 et que l'État belge est tenu de prendre les mesures nécessaires pour assurer l'application du règlement à partir du 2 août 2021. La partie requérante dans l'affaire n° 7202 ne démontre pas l'intérêt qu'elle aurait à l'annulation de la disposition attaquée pour la courte période qui précède, cet intérêt disparaissant en toute hypothèse à cette date. Ensuite, il ne suffit pas aux parties requérantes de contester la validité du règlement (UE) 2019/1157 pour conserver leur intérêt au recours. Les parties requérantes ne démontrent pas qu'elles ont introduit un recours en annulation du règlement devant la Cour de justice, ni que les questions préjudicielles qu'elles suggèrent sont pertinentes. Enfin, en ce qui concerne la partie requérante dans l'affaire n° 7211, âgée d'un an lors de l'introduction du recours, elle ne justifie d'aucun intérêt pour ce qui concerne la période de deux ans précédant l'application du règlement (UE) 2019/1157, dès lors que ce n'est que lorsqu'elle aura douze ans qu'une carte d'identité intégrant ses empreintes digitales pourra lui être délivrée.

*En ce qui concerne l'intérêt des parties requérantes et intervenantes*

*Affaire n° 7125*

A.3.1. La première partie requérante dans l'affaire n° 7125, le Parti Libertarien, est une « association politique belge qui œuvre à la diffusion des idéaux libertariens et à la réalisation d'une société de pleine liberté fondée sur le respect des droits naturels inaliénables et sacrés des individus ». La seconde partie requérante dans cette affaire, Baudoin Collard, est citoyen belge, président du Parti Libertarien et ingénieur en sécurité informatique.

A.3.2. Le Conseil des ministres soutient que le Parti Libertarien ne justifie pas de l'intérêt requis, dès lors qu'il ne ressort pas de ses statuts qu'il est doté de la personnalité juridique ni qu'en l'espèce, il puisse se prévaloir de l'exception dans le cadre de laquelle les partis politiques sont admis à agir devant la Cour. La seconde partie requérante n'établit pas davantage son intérêt, dès lors qu'elle se limite à invoquer un risque d'atteinte à la vie privée non autrement défini, ni étayé. La simple qualité de président du Parti Libertarien ou celle d'ingénieur en sécurité informatique ne suffit pas à établir un tel intérêt.

A.3.3. Les parties requérantes répondent que la seconde d'entre elles est susceptible d'être victime d'une violation de son droit au respect de la vie privée avec un degré suffisant de probabilité, de sorte qu'elle justifie de l'intérêt requis. Dès lors que la seconde partie requérante justifie d'un intérêt à agir, la Cour ne doit pas examiner si c'est également le cas de la première.

*Affaire n° 7150*

A.4.1. Les parties requérantes dans l'affaire n° 7150 sont des citoyens belges. Elles considèrent que la disposition attaquée porte une atteinte à leur droit au respect de la vie privée.

A.4.2. Le Conseil des ministres fait valoir que les parties requérantes ne démontrent pas concrètement l'existence d'un lien suffisamment individualisé entre la disposition attaquée et leur situation.

A.4.3. Les parties requérantes répondent qu'elles sont directement et négativement affectées par la disposition attaquée, dès lors qu'elles seront tôt ou tard contraintes de faire enregistrer leurs empreintes digitales pour la fabrication d'une nouvelle carte d'identité.

A.4.4. Les parties requérantes dans l'affaire n° 7125 et dans l'affaire n° 7202, également parties intervenantes dans l'affaire n° 7150, estiment justifier de l'intérêt requis à leur intervention pour les mêmes raisons, mentionnées en A.3, que celles qui justifient leurs recours respectifs.

A.4.5. Le Conseil des ministres répond que le fait que les parties requérantes devront tôt ou tard faire prélever leurs empreintes digitales pour acquérir une nouvelle carte d'identité ne suffit pas à démontrer qu'elles seraient affectées défavorablement par la disposition attaquée. Il ajoute que les parties intervenantes ne justifient pas de l'intérêt requis, dès lors qu'elles ont pu faire valoir leurs moyens dans leur propre requête et, à titre subsidiaire, pour les mêmes motifs que ceux qui sont mentionnés en A.4.2, en ce qui concerne les deux premières parties intervenantes. En ce qui concerne l'intérêt de la troisième partie intervenante, l'ASBL « Ligue des droits humains », le Conseil des ministres s'en remet à la sagesse de la Cour.

*Affaires n$^{os}$ 7202 et 7203*

A.5. Les parties requérantes dans les affaires n$^{os}$ 7202 et 7203, l'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des droits humains », sont des ASBL actives dans le domaine des droits de l'homme. Elles estiment avoir intérêt à l'annulation de la disposition attaquée.

*Affaire n° 7211*

A.6.1. La partie requérante dans l'affaire n° 7211 est un enfant âgé d'un an au moment de l'introduction de la requête, et qui a la nationalité belge. Représentée par ses parents, elle fait valoir qu'elle se verra délivrer une carte d'identité dans un futur proche et certain.

A.6.2. Le Conseil des ministres répond que cet argument repose sur une interprétation erronée de la législation applicable aux documents d'identité des mineurs d'âge. En effet, les enfants de moins de douze ans ne sont pas obligés de solliciter une carte kids-ID, laquelle ne contient du reste pas d'empreintes digitales. Par ailleurs, les passeports délivrés aux enfants de moins de douze ans ne comprennent pas les empreintes digitales de ceux-ci.

A.6.3. La partie requérante répond qu'elle sera tôt ou tard, et au plus tard à l'âge de quinze ans, contrainte de se voir délivrer une carte d'identité, qui comprendra ses empreintes digitales.

A.6.4. Le Conseil des ministres réplique que l'intérêt de la partie requérante ne saurait être certain, dès lors que la disposition attaquée ne pourra la concerner qu'au plus tôt lorsqu'elle aura atteint l'âge de douze ans et que, d'ici là, la législation pourra encore changer.

*En ce qui concerne la recevabilité de certains moyens*

*Moyen unique dans l'affaire n° 7125 et quatrième moyen dans les affaires n$^{os}$ 7203 et 7211*

A.7.1. Le Conseil des ministres fait valoir que la première branche du moyen unique dans l'affaire n° 7125 et du quatrième moyen dans les affaires n$^{os}$ 7203 et 7211 doit être rejetée en ce qu'elle est prise de la violation des articles 10 et 11 de la Constitution, à défaut pour les parties requérantes d'identifier les catégories de personnes ou de situations qui seraient traitées de manière discriminatoire. Il fait également valoir que la seconde branche de ces moyens n'est pas recevable dès lors qu'elle porte sur le processus d'élaboration de la disposition attaquée, pour lequel la Cour n'est pas compétente.

A.7.2. Les parties requérantes répondent que la seconde branche des moyens précités ne vise pas à étendre la compétence de la Cour au contrôle du processus ou des modalités d'élaboration de la loi, mais à faire constater par la Cour qu'en privant une catégorie d'administrés des garanties prévues par le 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), la disposition attaquée viole les articles 10, 11 et 22 de la Constitution.

A.7.3. Le Conseil des ministres réplique que le fait que la formalité en question soit ou non source d'une garantie pour les administrés ou une catégorie d'entre eux n'est pas pertinent.

*Second moyen dans l'affaire n° 7150*

A.8.1. Le Conseil des ministres soutient que le second moyen dans l'affaire n° 7150 n'est pas recevable. Dès lors que le RGPD ne garantit aucun droit analogue au droit au respect de la vie privée consacré par l'article 22 de la Constitution, la Cour ne peut pas contrôler la loi attaquée au regard de ce règlement. Par ailleurs, la première branche du moyen n'est pas recevable, dès lors que la Cour n'est pas compétente en principe pour contrôler le processus d'élaboration d'une loi.

A.8.2. Les parties requérantes considèrent que le droit au respect de la vie privée comprend le droit à la protection des données à caractère personnel. La Cour est compétente pour connaître du moyen, dès lors que le RGPD et l'article 22 de la Constitution forment un ensemble indissociable.

*Premier à troisième moyens dans l'affaire n° 7202*

A.9.1. Le Conseil des ministres fait valoir que les trois moyens dans l'affaire n° 7202 doivent être rejetés en tant qu'ils allèguent une violation du RGPD, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil » (ci-après : la directive « police ») et de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » (ci-après : la loi du 30 juillet 2018).

Selon le Conseil des ministres, en ce qui concerne le RGPD et la directive « police », la partie requérante néglige d'indiquer les catégories de personnes qui doivent être comparées. Par ailleurs, le RGPD et la directive « police » ne garantissent pas, en soi, un droit analogue à celui qui est consacré par l'article 22 de la Constitution. Ensuite, la Cour n'est en principe pas compétente pour contrôler les lois au regard d'autres dispositions législatives, ni pour contrôler le processus d'élaboration de la loi.

A.9.2. La partie requérante répond que l'article 4, paragraphe 3, du TUE contraint la Cour à tenir compte du RGPD et de la directive « police » dans son contrôle de la loi attaquée. Elle précise que le RGPD, la directive « police » et la loi du 30 juillet 2018 sont invoqués en combinaison avec les articles 10, 11 et 22 de la Constitution. Ensuite, les obligations issues du RGPD et de la directive « police » forment un ensemble indissociable avec les garanties de l'article 22 de la Constitution, dès lors que le droit à la protection des données à caractère personnel est une composante du droit au respect de la vie privée. Enfin, la Cour peut associer la loi du 30 juillet 2018 à son contrôle en vue de garantir une protection cohérente des données à caractère personnel, notamment pour vérifier si le fait de priver les intéressés des garanties prévues par cette loi est compatible avec les articles 10 et 11 de la Constitution.

A.9.3. Le Conseil des ministres réplique que la partie requérante ne démontre pas concrètement comment les différentes dispositions doivent être combinées et notamment quelles catégories de citoyens doivent être comparées pour identifier une violation des articles 10 et 11 de la Constitution.

*Premier à troisième moyens dans les affaires n$^{os}$ 7203 et 7211*

A.10.1. Le Conseil des ministres fait valoir que les premier à troisième moyens dans les affaires n$^{os}$ 7203 et 7211 sont irrecevables, dès lors que les parties requérantes se contentent de renvoyer à la requête introduite dans l'affaire n° 7202, sans exposer ni développer ces moyens.

A.10.2. Les parties requérantes répondent que ce renvoi, justifié par une évidente économie de procédure, ne viole pas l'article 6 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, dès lors que la Cour et l'ensemble des parties disposaient des écrits de la procédure dans l'affaire n° 7202 lorsque les deux requêtes concomitantes et l'ordonnance ordonnant leur jonction ont été notifiées au Premier ministre.

*Quant au fond*

*En ce qui concerne les affaires n$^{os}$ 7125, 7203 et 7211*

*Moyen unique dans l'affaire n° 7125 et quatrième moyen dans les affaires n$^{os}$ 7203 et 7211*

A.11. Le moyen unique dans l'affaire n° 7125 et le quatrième moyen dans les affaires n$^{os}$ 7203 et 7211, identiques, sont pris de la violation, par l'article 27 de la loi du 25 novembre 2018 « portant des dispositions diverses concernant le Registre national et les registres de population » (ci-après : la loi du 25 novembre 2018), 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 (ci-après : la Charte) et avec les articles 9, 35 et 36 du RGPD.

A.12.1. Dans la première branche, les parties requérantes font valoir que la disposition attaquée porte une atteinte injustifiée et disproportionnée au droit au respect de la vie privée des titulaires d'une carte d'identité. En ce qu'elle oblige l'ensemble des détenteurs d'une carte d'identité et d'une carte d'étranger à faire enregistrer leurs empreintes digitales à l'occasion de la création ou du remplacement desdites cartes, la disposition attaquée instaure un traitement de données à caractère personnel visé par l'article 9 du RGPD. Par ailleurs, la disposition attaquée est dénuée de justification raisonnable quant au but poursuivi, tant les chiffres de fraude à l'identité qui sont exposés dans les travaux préparatoires soit sont sujets à caution, soit ne sont pas propres à la Belgique, soit se situent à un niveau qui ne justifie pas la collecte des empreintes digitales de l'ensemble de la population belge.

A.12.2. Le Conseil des ministres soutient que la disposition attaquée poursuit un but légitime, à savoir la lutte contre la fraude à la ressemblance (fraude « look alike »). Cette fraude consiste à exploiter une ressemblance physique pour usurper l'identité d'une personne à qui l'on ressemble soit lors d'un contrôle d'identité, soit en vue d'obtenir de nouveaux documents d'identité. Si les cas de fraude documentaire ont, pendant la période 2006-2010, fortement diminué, les cas de fraude « look alike » ont en revanche fortement augmenté. Or, ce type de fraude est en l'état actuel des choses plus difficile à détecter, sur la base d'une seule photographie. Le nombre de cas de fraudes à l'identité est donc en fait très probablement bien plus élevé que les chiffres ne le montrent. L'objectif poursuivi l'est également au niveau de l'Union européenne. Il se retrouve aussi dans le Pacte mondial pour des migrations sûres, ordonnées et régulières (objectif 21, point 37, c)).

Selon le Conseil des ministres, l'intégration de l'image numérisée de deux empreintes digitales sur la carte d'identité, permet de déjouer plus efficacement les fraudes à la ressemblance, ce qui renforce ainsi l'efficacité des contrôles aux frontières. La disposition attaquée poursuit des objectifs plus larges, à savoir la lutte contre toute une série d'infractions qui sont associées à la fraude à l'identité (trafic d'êtres humains, terrorisme, etc.) et la protection de la vie privée des personnes qui sont les victimes d'une telle fraude.

La mesure adoptée est en outre proportionnée au but légitime poursuivi. Ainsi, le législateur n'a pas créé un registre central des empreintes digitales de toute la population. L'image numérisée des empreintes ne sera conservée qu'aux fins de la fabrication de la carte d'identité et pour une durée maximale de trois mois. Une fois la carte d'identité délivrée à son titulaire, l'image numérisée ne figurera plus que sur cette carte, sous la forme d'une seconde puce sécurisée sans contact de type RFID. Il s'agit de la même technologie que celle qui est utilisée pour les passeports et qui, à la meilleure connaissance du Conseil des ministres, n'a à ce jour donné lieu à aucun problème. Le SPF Intérieur veille en outre à régulièrement tenir compte des évolutions technologiques et à adapter cette puce aux standards de sécurité et de cryptage les plus élevés. Cette puce ne pourra être lue que par les services dûment habilités à cette fin. Par ailleurs, il n'existe pas d'alternative raisonnable à la collecte des empreintes digitales. Les systèmes basés sur des hologrammes ou des photographies 3D sont beaucoup plus complexes et onéreux. Le Conseil des ministres renvoie à la récente décision du Conseil constitutionnel français n° 2019-797 QPC du 26 juillet 2019 concernant l'enregistrement des empreintes digitales de mineurs étrangers non accompagnés et il précise que la mise en œuvre de la disposition attaquée sera placée sous la surveillance de l'Autorité de protection des données.

A.13.1. Dans la seconde branche, les parties requérantes critiquent l'absence d'analyse d'impact relative à la protection des données, au sens de l'article 35 du RGPD, préalablement à l'adoption de la loi.

A.13.2. Le Conseil des ministres répond que l'article 35 du RGPD impose de réaliser une analyse d'impact relative à la protection des données avant le traitement, mais non lors de l'élaboration de la disposition attaquée. La mise en œuvre de celle-ci supposant diverses mesures d'exécution, l'analyse d'impact peut très bien être effectuée à ce stade et, en tout cas, avant le début de la collecte des empreintes digitales. À titre tout à fait surabondant, le Conseil des ministres fait valoir que les deux avis qui ont été rendus par l'Autorité de protection des données ont apporté une information suffisante, de sorte que les objectifs poursuivis par l'analyse d'impact prévue par l'article 35 du RGPD ont été largement atteints.

*Premier à troisième moyens dans les affaires n$^{os}$ 7203 et 7211*

A.14.1. Les parties requérantes dans les affaires n$^{os}$ 7203 et 7211 renvoient aux moyens exposés dans le recours déposé par l'ASBL « Liga voor Mensenrechten » (affaire n° 7202), celui-ci étant réputé intégralement reproduit dans les deux requêtes, les parties requérantes souscrivant intégralement à son contenu.

A.14.2. Le Conseil des ministres se réfère à l'argumentation qu'il a apportée en réponse à ces moyens.

*En ce qui concerne l'affaire n° 7150*

*Premier moyen dans l'affaire n° 7150*

A.15. Le premier moyen dans l'affaire n° 7150 est pris de la violation, par l'article 27 de la loi du 25 novembre 2018, de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec l'article 17 du Pacte international relatif aux droits civils et politiques et avec les articles 7, 8 et 52 de la Charte.

A.16.1. Dans la première branche, les parties requérantes font valoir que le but de la disposition attaquée n'est pas légitime. L'objectif de lutter contre la fraude est plus large et plus vague que la fraude à l'identité vu qu'il concerne un certain nombre d'infractions en matière pénale ou de contrôle des frontières. Ensuite, cet objectif

n'est pas explicitement formulé dans la loi. Enfin, les objectifs poursuivis sont ceux d'une ancienne législation, à savoir la loi du 9 novembre 2015 « portant dispositions diverses Intérieur », ce qui n'est pas admissible.

A.16.2. Le Conseil des ministres réitère ce qu'il a déjà dit en réponse au moyen unique dans l'affaire n° 7125. Il précise que la fraude à l'identité ne peut quasiment pas être détectée sans un élément biométrique supplémentaire comme l'empreinte digitale, la vérification d'une photographie par un agent n'étant pas infaillible et étant nécessairement basée sur une appréciation subjective. Par ailleurs, il n'est pas indispensable que l'intention du législateur ressorte du texte de la loi, même si, en l'occurrence, celle-ci se déduit de l'article 27, 2°, de la loi du 25 novembre 2018. Pour le reste, les objectifs de la loi du 9 novembre 2015 demeurent pertinents pour la disposition attaquée.

A.16.3. Les parties requérantes répondent que l'administration peut consulter la photographie qui figure sur la carte d'identité pendant quinze ans, ce qui rend impossible la fraude consistant à obtenir des documents authentiques sur la base de documents faux ou volés. L'administration étant immédiatement informée de la perte ou du vol d'une carte d'identité, compte tenu de l'obligation pour le citoyen de signaler cette perte ou ce vol, elle peut bloquer aussitôt les certificats de sécurité de la carte. Ensuite, la probabilité que deux personnes se ressemblent au point qu'une confusion soit possible est très faible. Par ailleurs, les chiffres avancés par le Conseil des ministres ne concernent pas uniquement la fraude « look alike », mais aussi l'obtention frauduleuse de documents officiels. Enfin, il existe en Europe des documents d'identité qui ne sont pas aussi sophistiqués que les documents belges, mais ce constat n'est pas pertinent en l'espèce. Le fait que les chiffres généraux relatifs à la fraude à l'identité diminuent depuis 2017 conduit à mettre en doute la légitimité du but poursuivi.

A.16.4. Le Conseil des ministres répond que la faculté pour les autorités de consulter les photographies des citoyens n'est pas pertinente pour les formes spécifiques de fraude à l'identité évoquées dans ce cadre, compte tenu notamment des ressemblances possibles. Ainsi, il n'est pas si rare que deux personnes (à tout le moins sur une photographie) ressemblent l'une à l'autre. Par ailleurs, les citoyens ne déclarent pas systématiquement la perte ou le vol de leur carte d'identité. Ensuite, le blocage des certificats de sécurité ne suffit pas pour éviter l'utilisation d'une carte d'identité volée. En effet, les citoyens ne doivent pas toujours indiquer le code de leur carte d'identité, comme lors d'un contrôle aux frontières. Enfin, le Conseil des ministres produit différents chiffres actualisés concernant la fraude à l'identité, qui émanent notamment des statistiques criminelles de la police fédérale et des chiffres relatifs aux contrôles aux frontières du Royaume. Les différents chiffres produits sont cohérents et justifient la disposition attaquée. Enfin, la question de la proportionnalité de la mesure au regard de l'objectif poursuivi n'est pas pertinente en ce qui concerne la présente branche.

A.17.1. Dans la deuxième branche, les parties requérantes font valoir que la disposition attaquée viole le principe de la légalité contenu dans l'article 22 de la Constitution, dès lors que la délégation conférée au pouvoir exécutif n'est pas décrite d'une manière suffisamment précise et qu'elle ne contient pas tous les éléments essentiels requis.

A.17.2.1. La première sous-branche concerne le processus de fabrication et de délivrance des cartes d'identité. Selon les parties requérantes, ce processus n'est pas suffisamment décrit, comme le montre une étude récente du « Computer Security and Industrial Cryptography Group » (ci-après : le COSIC) de la KU Leuven, intitulée « Vingerafdrukken op de Belgische eID – Technische analyse » (« Empreintes digitales sur les cartes d'identité électroniques belges – Analyse technique »). La période maximale de trois mois, trop brève, sera systématiquement dépassée en pratique, sans que cela donne lieu à une sanction. Telle qu'elle est libellée, la loi permet aux personnes habilitées à accéder aux données y compris pendant la phase de fabrication. Elle permet également que les empreintes digitales soient imprimées et donc visibles à l'œil nu. Elle n'indique pas la technologie qui sera utilisée et permet l'utilisation d'une puce pouvant être lue à distance. Par ailleurs, elle ne prévoit pas de mesures techniques en vue de protéger les empreintes digitales stockées sur la puce. Enfin, elle permet qu'à l'issue du processus de fabrication, l'autorité efface les données sans les supprimer complètement, ce qui pourrait aboutir à la constitution d'une base de données globale des empreintes digitales.

A.17.2.2. Le Conseil des ministres répond que le principe de la légalité ne s'oppose pas à une délégation au pouvoir exécutif. En l'occurrence, le législateur a réglé les éléments essentiels de la délégation : le but, la durée, le stockage, les catégories de données traitées, les entités qui sont habilitées à utiliser les empreintes digitales et à y accéder. L'exigence de prévisibilité est ainsi respectée. Les éléments évoqués par les parties requérantes (sanctions, type de puce, mesures techniques de sécurisation, modalités de suppression des données) concernent des aspects techniques, de pur détail, qui peuvent être réglés par arrêté royal. Par ailleurs, il ressort clairement de

la disposition attaquée que les empreintes digitales sont stockées uniquement sur une puce, que les données doivent être supprimées et effacées après trois mois maximum et, enfin, que les personnes habilitées peuvent uniquement lire les empreintes digitales sur les cartes d'identité, et non consulter celles-ci lors de la phase de fabrication.

A.17.2.3. Les parties requérantes répondent que la disposition attaquée ne fixe pas les éléments essentiels et qu'elle aurait dû à tout le moins mentionner le principe d'une sanction, ainsi que le but et les modalités du stockage temporaire. Les éléments essentiels doivent figurer dans la loi, non dans les travaux préparatoires. Les parties requérantes renvoient à l'arrêt de la Cour européenne des droits de l'homme *S. et Marper c. Royaume-Uni* du 4 décembre 2008, qui comprend une description de ce qu'il y a lieu d'entendre comme éléments essentiels. Elles signalent un accident survenu au Danemark concernant l'enregistrement irrégulier de plusieurs dizaines de milliers d'empreintes digitales sur des passeports et exposent que la disposition attaquée ne garantit pas la suppression définitive des données.

A.17.2.4. Le Conseil des ministres répond que la sanction ne constitue pas un élément essentiel qui doit être inscrit dans la loi attaquée. Ensuite, le respect du délai de trois mois sera assuré, compte tenu des dispositifs prévus par le RGPD et par la loi du 30 juillet 2018. L'objectif du stockage temporaire au cours de la phase de fabrication ressort clairement de la loi. Les modalités de ce stockage ne doivent pas être divulguées, pour des raisons de sécurité. Il en va de même pour la description technique de la puce et du certificat de protection. Compte tenu des garanties prévues, le risque de constitution d'une base de données globale des empreintes digitales est purement hypothétique.

A.17.3.1. La seconde sous-branche concerne la phase de lecture des cartes d'identité. Selon les parties requérantes, la loi ne précise pas en quoi consiste cette lecture et n'interdit pas l'enregistrement des données à cette occasion. Elle ne précise pas si les habilitations doivent être assorties de mesures techniques. Elle n'indique pas non plus le but de la lecture des empreintes digitales par les agents chargés du contrôle des frontières. En outre, l'habilitation vaut également pour le personnel à l'étranger qui peut, le cas échéant, être une firme privée.

A.17.3.2. Le Conseil des ministres répond qu'il ressort clairement de la loi ainsi que des travaux préparatoires que les personnes habilitées peuvent uniquement lire les empreintes digitales et non les conserver. Ensuite, la loi règle le but et les circonstances dans lesquels cette lecture peut avoir lieu. Ainsi, il est évident que les agents chargés du contrôle des frontières ne peuvent vérifier les empreintes digitales que pour autant que cela soit nécessaire dans l'exécution de leurs missions légales. Par ailleurs, les travaux préparatoires indiquent que les empreintes digitales seront protégées avec un certificat, que seules les personnes habilitées pourront lire. La sécurisation technique des données est évolutive, si bien qu'il ne serait pas pertinent de la prévoir dans la loi elle-même. Enfin, la disposition attaquée ne ressortit pas au droit pénal et n'incrimine aucun comportement, de sorte que le principe de la légalité plus strict en la matière n'est pas applicable.

A.17.3.3. Les parties requérantes répètent que la loi attaquée n'interdit pas la conservation des données lors de la lecture. Ensuite, la lecture sans contact des empreintes digitales implique que celles-ci peuvent être contrôlées à l'insu de la personne concernée. Enfin, le principe du certificat ne figure pas dans la loi.

A.17.3.4. Le Conseil des ministres réplique qu'il est clair que les personnes habilitées peuvent uniquement lire les empreintes digitales et non les conserver. L'appareil utilisé ne permettra pas d'un point de vue technique la conservation des empreintes digitales. Enfin, l'accident survenu au Danemark auquel les parties requérantes se réfèrent n'est pas pertinent, dès lors qu'aucun risque d'abus ne s'est posé à cette occasion.

A.18.1. Dans une troisième branche, les parties requérantes font valoir que la loi attaquée n'est pas nécessaire dans une société démocratique et qu'elle est disproportionnée.

A.18.2.1. La première sous-branche concerne le caractère non nécessaire de la loi. Tout d'abord, un règlement européen en projet ne saurait servir de justification à la disposition attaquée. Les cartes d'identité sont suffisamment sécurisées (photographie, signature, code secret, etc.) et peuvent difficilement être contrefaites. Ensuite, la majorité des fraudes à l'identité ne supposent pas l'emploi d'une carte d'identité. Même lorsque tel est le cas, le particulier ou l'entreprise en question ne peut pas contrôler les empreintes digitales, faute d'habilitation. Par ailleurs, les chiffres en matière de fraude qui sont avancés dans les travaux préparatoires sont négligeables. Ensuite, le fait que la loi permette la lecture des empreintes digitales à l'œil nu est inacceptable, dès lors que des personnes non habilitées pourraient facilement lire et copier ces empreintes digitales. L'argument selon lequel les empreintes digitales figurent déjà sur les passeports n'est pas davantage pertinent, comme l'a souligné le

Contrôleur européen de la protection des données (CEPD) dans son avis 7/2018 du 10 août 2018 sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents. Ensuite, aucun examen n'a été effectué à propos de l'effectivité d'alternatives (notamment sur la base des données dont l'autorité dispose déjà) ou de l'effectivité de la mesure attaquée. Par ailleurs, ainsi que le montre l'avis du COSIC, le recours aux empreintes digitales n'est pas infaillible. Or, il existe des alternatives qui attentent moins aux droits fondamentaux (*Sensor-on-card*, *Match-on-card*, etc.). Enfin, la conservation des empreintes digitales dans une base de données centrale n'est absolument pas nécessaire.

A.18.2.2. Le Conseil des ministres répond que l'exigence de nécessité dans une société démocratique ne signifie aucunement que l'ingérence soit réellement inévitable ni qu'il n'existe aucune autre manière, moins intrusive, de réaliser l'objectif poursuivi. En l'occurrence, la photographie sur la carte d'identité n'est pas suffisante pour lutter efficacement contre la fraude « look alike », même lorsqu'elle est combinée avec des algorithmes de comparaison des visages. Les autres mécanismes (hologramme, photographie 3D, scan de l'iris) sont soit non pertinents, soit trop onéreux. Enfin, il existe un large consensus européen sur l'introduction de la mesure.

A.18.2.3. Les parties requérantes répliquent que la jurisprudence de la Cour européenne des droits de l'homme qui est citée par le Conseil des ministres concerne la charge de la preuve. Or, il est démontré en l'espèce que la mesure litigieuse n'est pas effective et qu'il existe des alternatives. Ainsi, la technologie permet aujourd'hui d'effectuer un contrôle fiable sur la base d'une photographie, qui doit d'ailleurs satisfaire à des normes minimales de qualité.

Selon les parties requérantes, le règlement (UE) 2019/1157 n'est pas une simple reproduction de la loi attaquée. Ce règlement est plus détaillé et plus explicite, notamment en ce qui concerne les normes de sécurité applicables. Cependant, le règlement ne contient aucune obligation pour les États membres de délivrer une carte d'identité, ce qui engendre une Europe à deux vitesses avec une discrimination manifeste entre les citoyens de l'Union selon qu'ils ont l'obligation ou non de posséder une carte d'identité. Aussi, le règlement (UE) 2019/1157 viole les principes invoqués dans la requête. Les parties requérantes suggèrent donc d'interroger la Cour de justice à titre préjudiciel à propos de la validité de ce règlement.

A.18.2.4. Le Conseil des ministres répond que les parties requérantes ne tiennent pas compte de ce qu'outre le fait qu'elles nécessitent un matériel particulier, les techniques avancées en matière de reconnaissance faciale sont plus intrusives que la mesure litigieuse. Le Conseil des ministres renvoie à la décision précitée du Conseil constitutionnel français du 26 juillet 2019.

A.18.3.1. Dans la seconde sous-branche, les parties requérantes font valoir que la loi est disproportionnée. Les chiffres en matière de fraude à l'identité évoqués dans les travaux préparatoires, de même que la manière dont les calculs ont été faits et la période qui a été prise en compte, ne sont pas clairs. D'ailleurs, aucun chiffre ne concerne les condamnations effectives. La disproportion de la mesure litigieuse apparaît lorsque l'on met en relation le nombre de fraudes et le nombre de personnes qu'elle vise. Pourtant, comme le montrent les chiffres du CEPD, il s'agit d'un phénomène marginal, en voie de diminution. Ensuite, le prélèvement forcé des empreintes digitales présente inévitablement un lien avec le droit pénal. La mesure litigieuse revient à « précriminaliser » l'ensemble des personnes concernées. Or, cette matière est strictement réglée en droit pénal, en particulier la collecte des empreintes digitales par la police. Les parties requérantes dans l'affaire n° 7150 font valoir que les empreintes digitales peuvent facilement être sabotées, sans empêcher l'utilisation de la carte d'identité. Enfin, le risque d'abus est d'autant plus grand que de nombreuses données sont collectées et que l'empreinte digitale est aujourd'hui utilisée dans bon nombre d'applications.

A.18.3.2. Le Conseil des ministres considère que la disposition attaquée n'emporte pas une ingérence disproportionnée dans les droits des personnes concernées compte tenu des garanties prévues : une durée de conservation des empreintes digitales limitée à trois mois maximum; un stockage temporaire décentralisé auprès des administrations communales durant la phase de fabrication; la suppression et l'effacement des empreintes digitales après la fabrication de la carte d'identité et en tout cas après trois mois; la détermination des catégories de personnes habilitées à lire les empreintes digitales et ce, uniquement dans l'exercice de leurs missions, moyennant plusieurs garanties (lecture avec un certificat, avec des lecteurs de cartes pourvus d'une habilitation et impossibilité de sauvegarder ou de centraliser les empreintes digitales); l'applicabilité, pour le reste, du RGPD et

des droits qui y sont prévus. L'absence de problème concernant les empreintes digitales intégrées dans les passeports depuis 2012 confirme que le risque de sabotage dénoncé par les parties requérantes n'est pas établi.

Selon le Conseil des ministres, les chiffres concernant la fraude à l'identité ne doivent pas être minimisés. Le fait que ces chiffres ne rendent pas compte des condamnations effectives n'est pas pertinent, dès lors que la disposition attaquée ne vise pas l'incrimination ou la poursuite des fraudes à l'identité. Le fait que la fraude à l'identité soit marginale en comparaison d'autres types de criminalité n'est pas davantage pertinent, pas plus que la référence à des infractions spécifiques de fraude à l'identité sans utilisation de la carte d'identité. L'efficacité des empreintes digitales a été confirmée dans le cas des passeports, le nombre de cas d'abus ayant diminué. À ce jour, les cartes d'identité sont utilisées fréquemment comme documents de voyage au sein de l'Union européenne et même en dehors. En outre, l'identité est contrôlée dans de nombreux cas aux frontières de l'Union ainsi qu'à l'intérieur de la zone Schengen. Le règlement européen en projet montre que les cartes d'identité sont comparables aux passeports. Enfin, comme il a été dit précédemment, le législateur n'a nullement eu l'intention d'incriminer un comportement, mais simplement de faciliter la poursuite de certaines infractions.

A.18.3.3. Les parties requérantes ne contestent pas l'existence de la fraude mais estiment que la mesure litigieuse n'est pas proportionnée, compte tenu des alternatives possibles, du caractère marginal des chiffres avancés, de l'absence, d'une part, de sanction et, d'autre part, de garanties pendant la phase de lecture. Ensuite, l'efficacité du certificat n'est pas prouvée. Enfin, il n'y a pas de contrôle aux frontières pour certains vols à l'intérieur de l'Europe ainsi que dans le Thalys. Les cartes d'identité ne sont donc pas comparables aux passeports.

A.18.3.4. Le Conseil des ministres précise que le stockage temporaire des empreintes digitales durant la phase de fabrication est centralisé auprès du Registre national, et non au sein de chaque administration communale. En outre, la disposition attaquée doit être lue en combinaison avec le règlement (UE) 2019/1157, de sorte qu'il faut aussi tenir compte des garanties supplémentaires que ce règlement pourrait contenir. Ensuite, la critique des parties requérantes selon laquelle le règlement engendrerait une discrimination entre citoyens de l'Union est dirigée contre le règlement et non contre la loi. La Cour n'est donc pas compétente pour se prononcer sur ce point. Au reste, le règlement impose l'intégration d'empreintes digitales aux États membres qui délivrent des cartes d'identité. La loi attaquée et le règlement (UE) 2019/1157 ont donc les mêmes conséquences pour les citoyens belges.

*Second moyen dans l'affaire n° 7150*

A.19. Le second moyen dans l'affaire n° 7150 est pris de la violation, par l'article 27 de la loi du 25 novembre 2018, des articles 7, 8 et 52 de la Charte, de l'article 16 du TFUE, des articles 5, 6, 9, 35, paragraphe 1, et 36 du RGPD, de l'article 8 de la Convention européenne des droits de l'homme, lus en combinaison avec l'article 22 de la Constitution.

A.20.1. La première branche concerne l'absence d'analyse d'impact relative à la protection des données préalable, au sens de l'article 35 du RGPD, à l'adoption de la disposition attaquée.

A.20.2. Le Conseil des ministres réitère ce qu'il a dit en réponse à la seconde branche du moyen unique dans l'affaire n° 7125.

A.21.1. Dans la seconde branche, les parties requérantes font valoir que la disposition attaquée ne satisfait pas aux conditions relatives au traitement de données à caractère personnel sensibles pour un motif d'intérêt public important, prévues par l'article 9, paragraphe 2, point g), du RGPD. Elles en déduisent que le seul fondement pour un traitement légitime est celui qui est visé à l'article 9, paragraphe 2, point a), du RGPD, par lequel la personne concernée donne son consentement libre et univoque, et que les articles 5 et 6 du RGPD s'appliquent. Selon elles, la disposition attaquée ne satisfait toutefois pas aux principes et conditions prévus par ces dispositions.

Selon les parties requérantes, les empreintes digitales sont des données à caractère personnel sensibles au sens de l'article 9 du RGPD. Les exceptions à l'interdiction de principe de traitement doivent donc être interprétées limitativement. À cet égard, il y a lieu de souligner que les cartes d'identité ne sont pas assimilables aux passeports, comme la Cour de justice l'a jugé dans l'arrêt du 16 avril 2015, *Willems et a.* (C-446/12 à C-449/12), et que l'arrêt *Schwarz c. Stadt Bochum* du 17 octobre 2013 (C-291/12) n'est donc pas transposable en

l'espèce. Les cartes d'identité et les passeports sont intrinsèquement des documents différents et l'appréciation du test de nécessité et de proportionnalité doit être effectuée à l'aide de critères différents.

A.21.2. Le Conseil des ministres répond que la disposition attaquée satisfait aux conditions prévues par l'article 9, paragraphe 2, point g), du RGPD. Le traitement est justifié par un motif d'intérêt public important. Ensuite, l'ingérence est proportionnée au but légitime et ne porte pas atteinte à la substance du droit protégé. En outre, des mesures appropriées et spécifiques sont prévues en vue de la protection des droits des personnes concernées. Elles peuvent aussi être adoptées par arrêté royal. Enfin, le test de nécessité et de proportionnalité ne reçoit pas ici une interprétation plus stricte. Le Conseil des ministres renvoie à l'arrêt *Schwarz c. Stadt Bochum* précité en ce qui concerne l'admissibilité de l'ingérence. Cet arrêt est bien pertinent, dès lors que la carte d'identité aujourd'hui est un document de voyage très utilisé par les citoyens de l'Union.

Le Conseil des ministres fait valoir ensuite que la disposition attaquée est tout à fait conforme à l'article 5 du RGPD. Cette disposition n'exige aucunement que les principes de base qu'elle énumère soient mis en œuvre directement dans la loi. L'article 6 du RGPD n'est pas davantage méconnu.

*En ce qui concerne l'affaire n° 7202*

*Premier moyen dans l'affaire n° 7202*

A.22. Le premier moyen dans l'affaire n° 7202 est pris de la violation, par l'article 27 de la loi du 25 novembre 2018, de l'article 8 de la Convention européenne des droits de l'homme, des articles 7, 8 et 52 de la Charte, des articles 10, 11 et 22 de la Constitution, des articles 1er à 5, 9, 25, 32, 35 et 36 du RGPD, des articles 1er à 5, 8, 9, 10, 27 à 29 de la directive « police », ainsi que des articles 2, 4, 5, 26 à 28, 30 à 34, 58 à 60 de la loi du 30 juillet 2018.

A.23.1. Dans la première branche, la partie requérante fait valoir que le prélèvement de l'image numérisée des empreintes digitales et l'enregistrement de celle-ci sur les cartes d'identité et sur les cartes d'étranger entraînent une violation injustifiée et disproportionnée du droit à la protection de la sphère de vie personnelle, dès lors qu'il s'agit d'un traitement de données à caractère personnel sensibles qui n'est pas strictement nécessaire pour des motifs d'intérêt public important et dont la proportionnalité à l'objectif poursuivi n'est pas garantie.

Premièrement, l'adoption de la loi attaquée n'a pas été précédée d'une analyse d'impact relative à la protection des données, au sens de l'article 35 du RGPD, de sorte que la nécessité de la mesure n'est pas établie. Deuxièmement, la vérification de l'authenticité de la carte d'identité et de l'identité de son titulaire et la lutte contre la fraude ne sont pas des motifs d'intérêt public important. La partie requérante renvoie à l'avis de l'Autorité de protection des données, selon lequel le problème des fraudes à l'identité n'est pas établi, ainsi qu'à l'avis du CEPD, selon lequel le nombre de cas de fraudes diminue, de sorte que la lutte contre la fraude ne peut pas justifier le traitement massif des empreintes digitales. Enfin, le traitement des empreintes digitales par la police dans le cadre des entraves aux missions de police administrative n'est pas limité à des motifs d'intérêt public important. Troisièmement, la loi attaquée n'est pas pertinente pour réaliser l'objectif poursuivi. En effet, les empreintes digitales ne sont pas fiables et ne sont pas pertinentes à des fins de vérification et de constatation d'identité. Quatrièmement, le caractère insuffisant de la photographie comme moyen d'identification du titulaire de la carte n'est pas établi. Il existe des alternatives au traitement des empreintes digitales en vue d'améliorer la vérification de l'authenticité de la carte d'identité et de l'identité du titulaire (hologramme, algorithmes pour la comparaison des visages, etc.). Cinquièmement, la mesure litigieuse n'est pas accompagnée de garanties suffisantes en vue de garantir le respect des principes prévus par les dispositions citées dans le moyen. Sixièmement, l'avis du CEPD indique que seuls quinze États membres imposent la possession d'une carte d'identité et que, dans treize États membres, les cartes d'identité ne comportent pas de données biométriques, ce qui démontre que la loi attaquée n'est pas strictement nécessaire.

A.23.2. Le Conseil des ministres réitère ce qu'il a exposé en réponse au moyen unique dans l'affaire n° 7125 et au premier moyen dans l'affaire n° 7150. Sans contester la diminution du nombre de cartes d'identité falsifiées,

il souligne que les fraudes qui exploitent les failles des photographies augmentent. Par ailleurs, dans son avis, le CEPD ordonne uniquement d'apprécier à nouveau la nécessité et la proportionnalité du traitement des empreintes digitales, sans considérer que le traitement serait en tout cas disproportionné.

Le Conseil des ministres expose que la loi attaquée repose bien sur un motif d'intérêt public important, au sens du RGPD. Les arguments de la partie requérante sur la pertinence et sur la fiabilité de la mesure litigieuse ne sont pas convaincants, eu égard notamment à l'ancienneté des données sur lesquels elle se fonde. Le fait que les empreintes digitales puissent être facilement reproduites n'est pas pertinent, dès lors qu'elles ne sauraient être utilisées comme moyen d'identification avec la carte d'identité.

En ce qui concerne la nécessité de la mesure, il ne pourrait être déduit de l'absence d'analyse d'impact que le législateur n'aurait pas examiné les risques pour les droits et les libertés des personnes concernées ainsi que les mesures en vue de limiter ces risques.

A.23.3. La partie requérante fait valoir que le traitement des données relatives aux empreintes digitales prévu par le règlement (UE) 2019/1157 va plus loin que ce qui est adéquat et nécessaire au regard de l'objectif poursuivi, en violation notamment du règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE » (ci-après : le règlement (UE) 2018/1725). Une analyse d'impact insuffisante relative à la protection des données a été mise en œuvre préalablement à l'adoption du règlement (UE) 2019/1157, en violation du RGPD, de la directive « police » et du règlement (UE) 2018/1725 (voy. aussi le règlement (CE) n° 45/2001). La stricte nécessité du traitement litigieux tel qu'il est rendu obligatoire par le règlement (UE) 2019/1157 n'est donc pas prouvée. Ensuite, le renforcement de la sécurité des cartes d'identité et la facilitation de la libre circulation pour les citoyens de l'Union et les membres de leur famille ne constituent pas des motifs d'intérêt public important, compte tenu du nombre peu élevé de cas de fraudes avec une carte d'identité, tant au niveau national qu'européen. Par ailleurs, le règlement (UE) 2019/1157 n'est pas pertinent pour réaliser l'objectif poursuivi, pour les mêmes raisons que celles qui ont été exposées précédemment. La partie requérante invoque également l'absence de garanties suffisantes, ainsi que le fait qu'il n'existe pas d'obligation harmonisée au sein de l'Union européenne de posséder une carte d'identité. Elle précise que, lorsqu'elle examine la proportionnalité de l'ingérence, la Cour de justice vérifie s'il existe des mesures suffisamment efficaces mais qui entraînent une ingérence moins forte dans le droit concerné que la mesure litigieuse (CJUE, 17 octobre 2013, C-291/12, *Schwarz c. Stadt Bochum*). Enfin, l'article 4, paragraphe 3, du TUE et l'article 47 de la Charte peuvent être interprétés comme exigeant que le juge national vérifie si, lors de l'adoption d'une réglementation nationale comme celle qui est en cause, une analyse d'impact relative à la protection des données a été prise en compte tant formellement que matériellement. La partie requérante suggère d'interroger la Cour de justice à titre préjudiciel.

A.23.4. À titre liminaire, le Conseil des ministres fait valoir que l'argumentation de la partie requérante à propos de la validité du règlement (UE) 2019/1157 n'est pas pertinente à ce stade de la procédure. Il ne revient pas à l'État belge de démontrer la légalité de ce règlement.

Le Conseil des ministres considère que le renvoi qui est fait par la partie requérante au règlement (CE) n° 45/2001 et au règlement (UE) 2018/1725 n'est pas pertinent. Le premier règlement a été remplacé depuis le 10 septembre 2018 par le second. Ce dernier se limite au traitement des données à caractère personnel par toutes les institutions et organes de l'Union. Or, le règlement (UE) 2019/1157, dont la partie requérante conteste la validité, s'adresse aux États membres et non aux institutions ou organes de l'Union. Pour le reste, en ce qui concerne le contenu, le règlement (UE) 2018/1725 contient des dispositions analogues à celles du RGPD.

En ce qui concerne la validité du règlement (UE) 2019/1157, le Conseil des ministres fait valoir que les dispositions invoquées par la partie requérante n'exigent pas la mise en œuvre d'une analyse d'impact relative à la protection des données préalablement à l'adoption d'une loi ou d'un règlement. Le fait que, selon l'avis du CEPD, l'analyse d'impact effectuée au niveau européen soit insuffisante pour répondre aux exigences de l'article 35, paragraphe 10, du RGPD ne constitue pas un problème. Il découle de cette disposition que, s'il n'y a pas eu d'analyse d'impact au niveau européen ou si cette analyse d'impact est insuffisante, alors une analyse d'impact doit intervenir au niveau des États membres.

Le Conseil des ministres estime qu'il n'y a pas lieu d'avoir égard à la situation dans les autres États membres concernant notamment l'obligation ou non de posséder une carte d'identité. Il est ici question de la réglementation belge. La situation dans les autres États membres n'est pas pertinente.

En ce qui concerne l'adoption d'une réglementation nationale comme la loi attaquée sur la base des compétences réservées du législateur belge, le Conseil des ministres estime qu'il est prématuré et non pertinent de se demander sur la base de quelle compétence le législateur belge a adopté la disposition attaquée, dès lors qu'il est établi que cette mesure et ses caractéristiques les plus importantes résultent aussi du règlement (UE) 2019/1157. À titre subsidiaire, le Conseil des ministres fait valoir que la partie requérante n'établit pas que la loi attaquée empêcherait l'exercice de la libre circulation des citoyens de l'Union ou rendrait celle-ci moins attractive ni qu'elle violerait les normes supérieures du droit de l'Union.

Le Conseil des ministres répète que la lutte contre la fraude à l'identité est considérée comme un objectif légitime tant par la Cour de justice que par la Cour européenne des droits de l'homme. Il souligne que les cartes d'identité sont des documents de voyage fréquemment utilisés dans l'Union européenne et même aux frontières extérieures de l'Union. Comme c'est le cas avec les passeports, les cartes d'identité sont contrôlées aux frontières extérieures de la zone Schengen. Le Conseil des ministres mentionne également les contrôles aux frontières temporaires introduits par plusieurs pays au sein de la zone Schengen.

En ce qui concerne l'exigence d'une analyse d'impact préalable relative à la protection des données, le Conseil des ministres soutient que le principe d'effectivité contenu dans l'article 4, paragraphe 3, du TUE ne fait pas obstacle à la jurisprudence établie de la Cour concernant le contrôle de l'élaboration d'une loi. Ensuite, le RGPD et la loi du 30 juillet 2018 prévoient des recours effectifs contre une violation de l'obligation prévue par l'article 35 du RGPD, de sorte qu'il n'y a pas de violation de l'article 47 de la Charte.

A.24.1. Dans la seconde branche, la partie requérante fait valoir que le prélèvement des empreintes digitales et l'enregistrement de celles-ci sur les cartes d'identité et sur les cartes d'étranger, sous la forme d'une image numérisée lisible électroniquement, constituent un traitement de données biométriques en vue de l'identification unique d'une personne qui n'est pas assorti des mesures appropriées et spécifiques destinées à protéger les droits des intéressés.

La partie requérante conteste la constitutionnalité de la loi attaquée en ce qu'elle prévoit que les empreintes digitales sont collectées et conservées.

La partie requérante fait valoir qu'à défaut d'analyse d'impact, les mesures destinées à limiter les risques n'ont pas été suffisamment examinées. En outre, la loi attaquée ne détermine pas la technique ou la méthode par laquelle l'empreinte digitale est enregistrée et lue. Elle ne contient pas davantage les normes ou spécifications techniques auxquelles la puce électronique doit satisfaire et n'interdit pas la lecture à distance de cette puce, sans contact, par un appareil de lecture approprié au moyen de la technologie RFID. Enfin, il ressort de l'étude du COSIC que la puce n'est pas suffisamment sécurisée.

A.24.2. Le Conseil des ministres réitère ce qu'il a précédemment exposé dans les affaires n$^{os}$ 7125 et 7150, à propos de la proportionnalité de la disposition attaquée et de sa compatibilité avec le principe de légalité. Par ailleurs, la disposition attaquée ne viole pas les dispositions du RGPD citées dans le moyen.

Le Conseil des ministres ajoute que l'utilisation d'une puce sans contact ne met pas en péril la sécurité des données. La critique n'est du reste pas recevable dès lors qu'elle n'est pas dirigée contre la loi attaquée. Ensuite, le vol d'une image intégrale des empreintes digitales peut certes causer des dommages considérables mais il est plus facile de voler des empreintes digitales qui sont laissées sur toutes sortes d'objets que de saboter une puce hautement sécurisée. Enfin, il va de soi que tout abus sera sanctionné, le cas échéant pénalement (voy. les articles 461, 550*bis* et 550*ter* du Code pénal). Les garanties du RGPD et de la loi du 30 juillet 2018 s'appliquent également, sans préjudice de l'application des articles 6*quater* et 7 de la loi du 19 juillet 1991 « relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour ». Le risque d'abus dénoncé par la partie requérante n'est donc pas établi.

A.24.3. La partie requérante répond que le règlement (UE) 2019/1157, lu en combinaison avec la décision d'exécution C(2018) 7767 de la Commission du 30 novembre 2018 « établissant les spécifications techniques du

modèle uniforme de titre de séjour pour les ressortissants de pays tiers, et abrogeant la décision C(2002) 3069 », ne contient pas les mesures adéquates, techniques et organisationnelles en vue de garantir notamment l'intégrité et la confidentialité des données liées aux empreintes digitales.

A.24.4. Le Conseil des ministres répond que la disposition attaquée et le règlement (UE) 2019/1157 contiennent des garanties suffisantes pour protéger les droits fondamentaux et les intérêts fondamentaux des intéressés.

*Deuxième moyen dans l'affaire n° 7202*

A.25. Le deuxième moyen dans l'affaire n° 7202 est pris de la violation, par l'article 27 de la loi du 25 novembre 2018, de l'article 8 de la Convention européenne des droits de l'homme, des articles 7, 8 et 52 de la Charte, des articles 10, 11 et 22 de la Constitution, ainsi que des articles 1er à 5 et 9 du RGPD.

Selon la partie requérante, la conservation par les services du Registre national de l'image numérisée des empreintes digitales, en vue de la fabrication et de la délivrance de la carte d'identité, pendant une période maximale de trois mois, entraîne une violation injustifiée et disproportionnée du droit à la protection de la sphère de vie personnelle, dès lors qu'il s'agit d'un traitement de données à caractère personnel sensibles qui n'est pas strictement nécessaire pour des motifs d'intérêt public important et dont la proportionnalité à l'objectif poursuivi n'est pas garantie. L'étude du COSIC démontre que la conservation centrale des empreintes digitales pendant un délai de trois mois maximum est totalement superflue d'un point de vue technique, puisque les empreintes digitales peuvent être inscrites sur la puce au moment du retrait de la carte d'identité. En outre, aucune mesure technique ou adéquate n'a été prise en vue de garantir l'intégrité et la confidentialité des empreintes ainsi conservées.

A.26. Le Conseil des ministres répond que l'enregistrement temporaire des empreintes digitales vise à permettre aux autorités locales de fabriquer la carte d'identité, ce qui constitue un but légitime. Ensuite, le législateur a prévu des garanties suffisantes pour limiter cette durée, de sorte que la mesure est proportionnée. Ces garanties ont été énumérées plus haut. Enfin, l'enregistrement central temporaire des empreintes digitales auprès du Registre national vise à garantir la sécurité de celles-ci, ce que les autorités locales ne pourraient pas assurer.

A.27. La partie requérante considère que l'article 10, paragraphe 3, du règlement (UE) 2019/1157 n'est pas compatible avec le droit de l'Union, en ce que, premièrement, il permet la conservation des données jusqu'à 90 jours après la délivrance du document d'identité, en ce que, deuxièmement, il permet la conservation des données au-delà de 90 jours pour d'autres buts que ceux qui sont prévus par ce même règlement, et en ce que, troisièmement, il ne contient aucune mesure technique ou organisationnelle adéquate en vue d'assurer la sécurité des empreintes digitales conservées. Par ailleurs, l'aveu du Conseil des ministres selon lequel les communes ne peuvent pas satisfaire aux normes de sécurité montre bien que l'intégrité et la confidentialité des données relatives aux empreintes digitales ne sont pas garanties lors de la collecte de celles-ci.

A.28. Le Conseil des ministres répond que les critiques qui précèdent sont dirigées contre l'article 10, paragraphe 3, du règlement (UE) 2019/1157. La seconde de ces critiques n'est pas pertinente dans le cadre du présent recours dès lors que la disposition attaquée ne prévoit pas de délai de conservation de plus de 90 jours. Pour le reste, la justification de l'enregistrement central temporaire des empreintes digitales vaut également pour le délai maximal de conservation de 90 jours prévu par le règlement.

*Troisième moyen dans l'affaire n° 7202*

A.29. La partie requérante dans l'affaire n° 7202 prend un troisième moyen de la violation, par l'article 27 de la loi du 25 novembre 2018, de l'article 8 de la Convention européenne des droits de l'homme, des articles 7, 8 et 52 de la Charte, des articles 10, 11 et 22 de la Constitution, des articles 1er à 5 et 9 du RGPD, des articles 1er à 5, 8 à 10 et 27 à 29 de la directive « police », ainsi que des articles 2, 4, 5, 26 à 28, 30 à 34 et 58 à 60 de la loi du 30 juillet 2018.

A.30.1. Dans la première branche, la partie requérante fait valoir que l'habilitation que confère la disposition attaquée aux services de police de lire les empreintes digitales est un traitement de données à caractère personnel sensibles qui entraîne une violation injustifiée et disproportionnée du droit à la protection de la sphère de vie personnelle.

Selon la partie requérante, qui mentionne à cet égard l'absence d'analyse d'impact relative à la protection des données, la disposition attaquée confère une habilitation trop large aux autorités concernées en ce qui concerne l'accès aux données, y compris les données centralisées pendant le processus de fabrication, et leur utilisation ultérieure. Ainsi, la disposition attaquée n'interdit pas la lecture massive ou répétée des empreintes digitales ni le croisement de ces données avec d'autres informations en vue d'identifier un individu. Elle ne prévoit pas non plus que la lecture ne peut avoir lieu qu'à titre subsidiaire et qu'elle est limitée à des fins de vérification de l'authenticité de la carte d'identité et de l'identité de son titulaire.

A.30.2. Le Conseil des ministres répond que la première branche du moyen repose sur une prémisse erronée, dès lors qu'il ressort clairement du texte de la loi attaquée ainsi que des travaux préparatoires que les personnes habilitées peuvent uniquement lire les empreintes digitales sur la carte d'identité et non dans la banque de données centrale. Enfin, les personnes habilitées à lire les empreintes digitales peuvent le faire uniquement dans le cadre de contrôles d'identité qui sont nécessaires pour l'exercice de leur fonction. Ces contrôles d'identité interviennent logiquement par la vérification de la carte d'identité et non par la consultation des empreintes digitales conservées centralement. Ensuite, la loi attaquée détermine que les services de police sont habilités à lire les empreintes digitales dans leurs missions légales et uniquement pour autant que cela soit nécessaire. Eu égard à ce qui précède, le risque d'utilisation des données pour un autre but autre que celui pour lequel elles ont été collectées (notamment la lecture à grande échelle et secrète des empreintes digitales) est fortement limité. Pour le reste, la disposition attaquée encadre soigneusement la consultation des empreintes digitales sur les cartes d'identité, ainsi qu'il a été dit précédemment.

A.30.3. Selon la partie requérante, l'interprétation de la disposition attaquée par le Conseil des ministres n'a pas de fondement textuel. En ce qu'elle doit être interprétée comme permettant la consultation de la base de données centralisée par les autorités habilitées, la disposition attaquée viole le droit de l'Union et notamment le règlement (UE) 2019/1157. Ensuite, la possibilité pour les services de police de consulter les empreintes digitales telle qu'elle est prévue par la loi attaquée va au-delà de ce que permet le règlement (UE) 2019/1157, à savoir la vérification de l'authenticité des documents et de l'identité de leur titulaire.

La partie requérante se demande si le traitement prévu par la loi attaquée relève du RGPD ou de la directive « police » et de la loi du 30 juillet 2018. Enfin, à supposer que la Belgique ait adopté la loi attaquée sur la base de ses compétences réservées, se pose la question de la compatibilité de celle-ci avec les différentes normes de référence citées.

A.30.4. Le Conseil des ministres répond que la consultation des empreintes digitales par les services de police en exécution de leurs missions légales s'inscrit dans leur mission de vérification de l'authenticité du document ou de l'identité de son titulaire. La loi attaquée est en ce sens plus limitée que ce que prévoit l'article 11, paragraphe 6, du règlement (UE) 2019/1157, puisqu'elle exige que les services de police vérifient l'identité d'une personne et l'authenticité d'un document à l'aide des empreintes digitales, pour autant que cela s'inscrive dans leurs missions légales de police administrative et judiciaire dans le cadre de la lutte contre la fraude. Selon le Conseil des ministres, ces missions légales sont suffisamment délimitées. À titre subsidiaire, il fait valoir que le législateur pouvait imposer une telle mesure sur la base de ses compétences réservées.

Ensuite, le Conseil des ministres indique que l'obligation pour les services de police de contrôler les empreintes digitales uniquement en dernier ressort ne figure pas dans le règlement (UE) 2019/1157, mais dans un de ses considérants. En tout état de cause, les services de police ne peuvent lire les empreintes digitales que pour autant que cela soit nécessaire pour remplir leurs missions légales. Par ailleurs, la disposition attaquée doit être lue conjointement avec l'article 11, paragraphe 6, du règlement (UE) 2019/1157. Ainsi, les services de police ne liront les empreintes digitales que si, par exemple, ils éprouvent des difficultés lors de la constatation de l'identité d'une personne. Aussi, le RGPD et la directive « police », à supposer celle-ci applicable, prévoient des garanties analogues et suffisantes en faveur des intéressés.

Enfin, le Conseil des ministres indique que la question de savoir sur la base de quelle compétence le législateur belge a pu adopter la disposition attaquée n'est pas pertinente dès lors que cette mesure résulte clairement du règlement (UE) 2019/1157.

A.31.1. Dans la seconde branche, la partie requérante reproche à la disposition attaquée de ne pas interdire la lecture des empreintes digitales sur la carte d'identité à grande échelle, sans contact et secrètement par les services de police. Elle fait valoir que la possibilité précitée constitue un élément essentiel qui, selon le principe de légalité, aurait dû être réglé explicitement par le législateur, lequel aurait également dû en définir les modalités et prévoir des garanties suffisantes contre les abus.

A.31.2. Le Conseil des ministres répond que cette branche n'est pas claire et qu'elle constitue en substance une répétition des moyens précédents. Par ailleurs, la branche repose sur une prémisse erronée, qui est celle de la faculté pour les services de police de consulter les empreintes digitales sans limitation.

A.31.3. Selon la partie requérante, la question essentielle est de savoir si les données sur les cartes d'identité seront lues à grande échelle, sans contact et/ou secrètement ou si la loi attaquée interdit un tel traitement toujours et en toutes circonstances.

A.31.4. Le Conseil des ministres répond que la disposition attaquée est claire et qu'elle satisfait au principe de légalité. Tout d'abord, les empreintes digitales ne peuvent pas être lues à grande échelle, les personnes habilitées n'ayant pas d'accès à la banque de données centrale. Il appartiendra à chacune de ces instances de déterminer la manière dont les empreintes digitales sont lues. Ensuite, les empreintes digitales ne peuvent pas être lues secrètement, dès lors que la consultation des empreintes digitales suppose un contact direct avec le citoyen. Enfin, dès lors que les empreintes digitales ne peuvent pas être enregistrées après qu'elles sont lues, elles ne sauraient être croisées avec d'autres informations.

*Quant aux demandes de mesures d'instruction formulées par les parties requérantes*

A.32.1. Les parties requérantes dans l'affaire n° 7150 invitent la Cour à faire usage de ses pouvoirs d'instruction en vue d'obtenir un avis technique au sujet de la description insuffisante et de l'absence de détermination des éléments essentiels de la mesure litigieuse, de l'existence d'alternatives à celle-ci, ainsi que des risques qu'elle entraîne en matière de sécurité. Dans ce cadre, les parties requérantes dans l'affaire n° 7202 demandent à la Cour d'entendre les auteurs de l'analyse précitée du COSIC.

A.32.2. Le Conseil des ministres fait valoir que les parties requérantes ne démontrent pas la nécessité des mesures d'instruction demandées, eu égard aux questions que la Cour doit trancher et aux éléments qui ont été produits dans les travaux préparatoires et en cours de procédure. Il ajoute que les auteurs de l'étude du COSIC ne présentent pas les garanties suffisantes en termes d'indépendance et d'impartialité.

A.32.3. Les parties requérantes dans l'affaire n° 7202 répondent que les mesures d'instruction demandées sont nécessaires en raison du caractère particulièrement complexe et technique des spécifications techniques applicables en vertu du règlement (UE) 2019/1157. Elles demandent d'entendre les auteurs de l'étude précitée, non de les désigner comme experts.

*Quant aux demandes de poser des questions préjudicielles à la Cour de justice de l'Union européenne*

A.33.1. Les parties requérantes et intervenantes dans les affaires n$^{os}$ 7125 et 7150 suggèrent de poser plusieurs questions préjudicielles en interprétation à la Cour de justice de l'Union européenne concernant la compatibilité d'une norme législative telle que la disposition attaquée avec les dispositions du droit de l'Union qui garantissent le droit au respect de la vie privée et le droit à la protection des données à caractère personnel et, en particulier, concernant la question de savoir si la disposition attaquée aurait dû faire l'objet d'une analyse d'impact préalable.

Les parties requérantes dans l'affaire n° 7150 suggèrent également de poser deux questions préjudicielles concernant la validité du règlement (UE) 2019/1157 au regard, d'une part, du droit au respect de la vie privée et du droit à la protection des données à caractère personnel et, d'autre part, du principe d'égalité, en ce que le règlement créerait une discrimination entre les citoyens de l'Union selon qu'ils sont soumis à l'obligation de posséder une carte d'identité ou non.

A.33.2. Le Conseil des ministres répond qu'il n'y a pas lieu de poser les questions préjudicielles suggérées plus haut, dès lors qu'il ressort clairement de l'article 35 du RGPD que l'analyse d'impact relative à la protection des données ne doit pas avoir lieu avant l'adoption de la loi et que la Cour de justice s'est déjà prononcée sur une problématique analogue dans l'arrêt, précité, *Schwarz c. Stadt Bochum*. Lorsqu'une question porte, non pas sur l'interprétation du droit européen, mais sur la compatibilité du droit national avec le droit de l'Union, il n'y a pas lieu, en principe, de poser une question à la Cour de justice et il revient au juge national de trancher lui-même cette question. Enfin, l'éventuelle différence de traitement entre les citoyens des différents États membres qui résulterait du règlement (UE) 2019/1157 ne concerne pas la compatibilité de ce règlement avec le droit au respect de la vie privée.

A.34.1. Les parties requérantes dans l'affaire n° 7202 suggèrent de poser sept questions préjudicielles à la Cour de justice.

Les première, quatrième et sixième questions concernent la validité du règlement (UE) 2019/1157 au regard du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, tels qu'ils sont garantis par le droit de l'Union. Elles portent respectivement sur l'enregistrement des empreintes digitales sur les cartes d'identité, sur la technique utilisée à cet effet et sur la possibilité de conserver les empreintes digitales jusqu'à 90 jours après la délivrance de la carte, voire au-delà.

Les deuxième et cinquième questions portent sur l'interprétation du droit de l'Union en ce qui concerne l'admissibilité d'une norme législative telle que la disposition attaquée dans l'hypothèse où le législateur belge aurait adopté celle-ci pour des motifs autres que ceux du règlement (UE) 2019/1157 - à savoir en vue d'assurer la défense de l'intégrité territoriale, le maintien de l'ordre public et la protection de la sécurité nationale - au regard, d'une part, du droit au respect de la vie privée et du droit à la protection des données à caractère personnel et, d'autre part, de la libre circulation des citoyens de l'Union.

La troisième question porte sur l'interprétation du droit de l'Union concernant la question de savoir si une norme législative telle que la disposition attaquée aurait dû faire l'objet d'une analyse d'impact relative à la protection des données et si le juge national doit le vérifier.

La septième question porte sur l'interprétation du droit de l'Union (en ce compris le règlement (UE) 2019/1157) en ce qui concerne l'admissibilité d'une norme législative telle que la disposition attaquée au sujet de la lecture des empreintes digitales.

A.34.2. Le Conseil des ministres conteste la pertinence des questions préjudicielles suggérées.

Les première, quatrième et sixième questions ne sont pas pertinentes dès lors que, d'une part, malgré leur contenu analogue, la disposition attaquée et le règlement (UE) 2019/1157 constituent deux normes juridiques distinctes, le second n'étant pas le fondement juridique de la première, et que, d'autre part, la Cour de justice s'est déjà prononcée sur une problématique analogue dans l'arrêt *Schwarz c. Stadt Bochum*, comme il a été dit précédemment.

Le Conseil des ministres fait valoir que les deuxième, cinquième et septième questions préjudicielles sont à tout le moins prématurées et hypothétiques et qu'elles ne pourraient pas contribuer à la solution du litige. Indépendamment des compétences sur la base desquelles le règlement (UE) 2019/1157 et la loi du 25 novembre 2018 ont été adoptés, il est clair que ces deux textes ont la même portée. Pour ces raisons, la question de savoir sur la base de quelle compétence le législateur belge a pu adopter la mesure litigieuse n'est pas pertinente dans cette phase de la procédure. Ensuite, ces questions ne seraient pertinentes que si la Cour de justice invalidait préalablement le règlement (UE) 2019/1157. À titre subsidiaire, le Conseil des ministres soutient qu'il est évident que la disposition attaquée est compatible avec le droit au respect de la vie privée et avec le droit à la protection des données à caractère personnel, et qu'il n'est pas nécessaire de saisir la Cour de justice à ce propos.

Enfin, le Conseil des ministres considère qu'il n'y a pas lieu de poser la troisième question préjudicielle suggérée, dès lors que la portée de l'article 35 du RGPD est suffisamment claire, comme il a été dit précédemment.

A.35.1. Les parties requérantes dans les affaires n$^{os}$ 7203 et 7211 suggèrent de poser une question préjudicielle à la Cour de justice concernant la validité du règlement (UE) 2019/1157 au regard du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, tels qu'ils sont garantis en droit de l'Union, et notamment au regard des articles 9, 35 et 36 du RGPD.

A.35.2. Le Conseil des ministres répond que la question n'est pas pertinente, compte tenu de l'arrêt *Schwarz c. Stadt Bochum* précité.

*- B -*

*Quant à la disposition attaquée et à son contexte*

B.1.1. L'article 27 de la loi du 25 novembre 2018 « portant des dispositions diverses concernant le Registre national et les registres de population » (ci-après : la loi du 25 novembre 2018) dispose :

« À l'article 6 de la [loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques], modifié en dernier lieu par la loi du 9 novembre 2015, les modifications suivantes sont apportées :

1° le paragraphe 2, alinéa 3, est complété par le 8°, rédigé comme suit :

' 8° l'image numérisée des empreintes digitales de l'index de la main gauche et de la main droite du titulaire ou, en cas d'invalidité ou inaptitude, d'un autre doigt de chaque main, le Roi détermine par arrêté délibéré en Conseil des ministres après avis de l'Autorité de protection des données les conditions et modalités de capture de l'image numérisée des empreintes digitales. ';

2° le paragraphe 2 est complété par les alinéas suivants :

' L'information visée à l'alinéa 3, 8°, ne peut être conservée que durant le temps nécessaire à la fabrication et à la délivrance de la carte d'identité et, en tout cas, durant une période de maximum 3 mois, étant entendu que après ce délai de 3 mois, les données doivent impérativement être détruites et effacées.

Sont habilités à lire l'information visée à l'alinéa 3, 8° :

- le personnel des communes chargé de la délivrance des cartes d'identité;

- les services de police, pour autant que cela s'avère nécessaire pour l'accomplissement de leurs missions légales de police administrative et judiciaire dans le cadre de la lutte contre la fraude, notamment la lutte contre la traite et le trafic des êtres humains, l'escroquerie et l'abus de confiance, le blanchiment d'argent, le terrorisme, le faux et usage de faux, l'usurpation de nom et l'usage de faux nom, les violations de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et les entraves aux missions de police administrative;

- le personnel chargé du contrôle aux frontières, tant en Belgique qu'à l'étranger;

- les membres du personnel de l'Office des Etrangers, pour autant que cela s'avère nécessaire dans le cadre de la recherche et de la constatation des infractions à la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et à la loi 30 avril 1999 relative à l'emploi des travailleurs étrangers;

- les membres du personnel du Service public fédéral des Affaires étrangères et le personnel diplomatique et consulaire, individuellement habilité par l'ambassadeur ou le consul, dans la mesure où cela s'avère nécessaire dans le cadre de la lutte contre la fraude;

- l'entreprise chargée de la production des cartes d'identité et les personnes strictement habilitées par elle en son sein, et ce, aux seules fins de production et de délivrance des cartes d'identité. ';

3° dans le paragraphe 3, alinéa 2, le 1° est remplacé par ce qui suit :

' 1° de consulter les informations le concernant qui sont reprises au Registre national des personnes physiques, dans les registres de la population et le registre des étrangers ainsi que dans le Registre des cartes d'identité et le Registre des cartes d'étranger visés à l'article 6*bis*; ';

4° le paragraphe 4 est remplacé par ce qui suit :

' § 4. Les données figurant sur la carte d'identité électronique, aussi bien les données visibles à l'œil nu que celles lisibles au moyen d'un lecteur de carte, à l'exception de la photographie du titulaire, du numéro de Registre national et de l'image numérisée des empreintes digitales, peuvent être lues et/ou enregistrées conformément aux dispositions légales et règlementaires en matière de protection de la vie privée et de sécurité des données à caractère personnel.

Le numéro de Registre national et la photographie du titulaire ne peuvent être utilisés que si cette utilisation est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance. La carte d'identité électronique ne peut être lue ou utilisée qu'avec le consentement libre, spécifique et éclairé du titulaire de la carte d'identité électronique.

Lorsqu'un avantage ou un service est proposé à un citoyen au moyen de sa carte d'identité électronique dans le cadre d'une application informatique, une alternative ne nécessitant pas le recours à la carte d'identité électronique, doit également être proposée à la personne concernée.

Sans préjudice de l'article 1er de l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité, le titulaire de la carte d'identité électronique peut refuser que ses données soient lues et/ou enregistrées, sauf dans les cas déterminés par le Roi par arrêté délibéré en Conseil des ministres. ';

5° dans le paragraphe 7, l'alinéa 1er est remplacé par ce qui suit :

‘ Le Roi détermine, après avis de l’Autorité de protection des données, la forme et les modalités de fabrication, de délivrance et d’utilisation de la carte. ’;

6° le paragraphe 7 est complété par un alinéa, rédigé comme suit :

‘ Le certificat qualifié de signature n’est pas activé sur la carte d’identité des personnes mineures. ’; ».

B.1.2. À la suite de cette modification, l’article 6 de la loi du 19 juillet 1991 « relative aux registres de la population, aux cartes d’identité, aux cartes des étrangers et aux documents de séjour » (ci-après : la loi du 19 juillet 1991) dispose désormais :

« § 1er. La commune délivre aux Belges une carte d’identité, aux étrangers admis ou autorisés à séjourner plus de trois mois dans le Royaume ou autorisés à s’y établir, une carte d’étranger, et aux étrangers inscrits pour une autre raison conformément aux dispositions de la loi du 15 décembre 1980 sur l’accès au territoire, le séjour, l’établissement et l’éloignement des étrangers, un document de séjour. La carte d’identité, la carte d’étranger et le document de séjour valent certificat d’inscription dans les registres de la population.

[…]

§ 2. La carte d’identité et la carte d’étranger contiennent, outre la signature du titulaire, soit la signature du fonctionnaire communal qui délivre la carte, soit, lorsque la carte est délivrée par La Poste SA de droit public, celle de la personne de cette entreprise mandatée à cette fin conformément aux modalités fixées par l’arrêté royal visé au § 1er, alinéa 2. Elle contient en outre des informations à caractère personnel visibles à l’œil nu et lisibles de manière électronique.

Les informations à caractère personnel visibles à l’œil nu et lisibles de manière électronique concernent :

1° le nom;

2° les deux premiers prénoms;

3° la première lettre du troisième prénom;

4° la nationalité;

5° le lieu et la date de naissance;

6° le sexe;

7° le lieu de délivrance de la carte;

8° la date de début et de fin de validité de la carte;

9° la dénomination et le numéro de la carte;

10° la photographie du titulaire;

11° [...];

12° le numéro d'identification du Registre national.

Les informations à caractère personnel lisibles de manière électronique concernent :

1° les clés d'identité et de signature;

2° les certificats d'identité et de signature;

3° le prestataire de service de certification;

4° l'information nécessaire à l'authentification de la carte et à la protection des données visibles de manière électronique figurant sur la carte et à l'utilisation des certificats qualifiés y afférents;

5° les autres mentions, prévues ou autorisées par la loi ainsi que les mentions imposées par la législation européenne;

6° la résidence principale du titulaire;

7° la mention visée à l'article 374/1 du Code civil.

8° l'image numérisée des empreintes digitales de l'index de la main gauche et de la main droite du titulaire ou, en cas d'invalidité ou inaptitude, d'un autre doigt de chaque main, le Roi détermine par arrêté délibéré en Conseil des ministres après avis de l'Autorité de protection des données les conditions et modalités de capture de l'image numérisée des empreintes digitales.

Le titulaire de la carte peut, s'il le souhaite, renoncer à l'activation des données visées aux points 1° à 3° de l'alinéa précédent.

L'information visée à l'alinéa 3, 8°, ne peut être conservée que durant le temps nécessaire à la fabrication et à la délivrance de la carte d'identité et, en tout cas, durant une période de maximum 3 mois, étant entendu que après ce délai de 3 mois, les données doivent impérativement être détruites et effacées.

Sont habilités à lire l'information visée à l'alinéa 3, 8° :

- le personnel des communes chargé de la délivrance des cartes d'identité;

- les services de police, pour autant que cela s'avère nécessaire pour l'accomplissement de leurs missions légales de police administrative et judiciaire dans le cadre de la lutte contre la fraude, notamment la lutte contre la traite et le trafic des êtres humains, l'escroquerie et l'abus de confiance, le blanchiment d'argent, le terrorisme, le faux et usage de faux, l'usurpation de nom et l'usage de faux nom, les violations de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et les entraves aux missions de police administrative;

- le personnel chargé du contrôle aux frontières, tant en Belgique qu'à l'étranger;

- les membres du personnel de l'Office des Etrangers, pour autant que cela s'avère nécessaire dans le cadre de la recherche et de la constatation des infractions à la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et à la loi 30 avril 1999 relative à l'emploi des travailleurs étrangers;

- les membres du personnel du Service public fédéral des Affaires étrangères et le personnel diplomatique et consulaire, individuellement habilité par l'ambassadeur ou le consul, dans la mesure où cela s'avère nécessaire dans le cadre de la lutte contre la fraude;

- l'entreprise chargée de la production des cartes d'identité et les personnes strictement habilitées par elle en son sein, et ce, aux seules fins de production et de délivrance des cartes d'identité.

[…]

§ 3. Le titulaire de la carte peut à tout moment demander, au moyen de cette carte ou auprès de la commune dans laquelle il est inscrit aux registres de la population, de consulter les données électroniques qui sont enregistrées sur la carte ou sont accessibles au moyen de celle-ci, et a le droit de demander la rectification de ses données à caractère personnel qui ne seraient pas reprises de manière précise, complète et exacte sur la carte.

Le titulaire de la carte a le droit de demander, au moyen de cette carte ou auprès de la commune dans laquelle il est inscrit aux registres de la population :

1° de consulter les informations le concernant qui sont reprises au Registre national des personnes physiques, dans les registres de la population et le registre des étrangers ainsi que dans le Registre des cartes d'identité et le Registre des cartes d'étranger visés à l'article 6*bis*;

2° de procéder à la rectification de ces données si elles ne sont pas reprises de manière précise, complète et exacte;

3° de connaître toutes les autorités, organismes et personnes qui ont, au cours des six mois écoulés, consulté ou mis à jour ses données au registre de la population ou au Registre national des personnes physiques, à l'exception des autorités administratives et judiciaires chargées de la recherche et de la répression des délits ainsi que de la Sûreté de l'Etat et du Service général du renseignement et de la sécurité des Forces armées.

Le Roi détermine la date d'entrée en vigueur du droit de prendre connaissance mentionné à l'alinéa précédent, 3°, ainsi que le régime auquel sont soumis le droit de consultation et de rectification ainsi que la prise de connaissance visés aux alinéas précédents.

§ 4. Les données figurant sur la carte d'identité électronique, aussi bien les données visibles à l'œil nu que celles lisibles au moyen d'un lecteur de carte, à l'exception de la photographie du titulaire, du numéro de Registre national et de l'image numérisée des empreintes digitales, peuvent être lues et/ou enregistrées conformément aux dispositions légales et règlementaires en matière de protection de la vie privée et de sécurité des données à caractère personnel.

Le numéro de Registre national et la photographie du titulaire ne peuvent être utilisés que si cette utilisation est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance. La carte d'identité électronique ne peut être lue ou utilisée qu'avec le consentement libre, spécifique et éclairé du titulaire de la carte d'identité électronique.

Lorsqu'un avantage ou un service est proposé à un citoyen au moyen de sa carte d'identité électronique dans le cadre d'une application informatique, une alternative ne nécessitant pas le recours à la carte d'identité électronique, doit également être proposée à la personne concernée.

Sans préjudice de l'article 1er de l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité, le titulaire de la carte d'identité électronique peut refuser que ses données soient lues et/ou enregistrées, sauf dans les cas déterminés par le Roi par arrêté délibéré en Conseil des ministres.

[…]

§ 7. Le Roi détermine, après avis de l'Autorité de protection des données, la forme et les modalités de fabrication, de délivrance et d'utilisation de la carte.

[…]

Le certificat qualifié de signature n'est pas activé sur la carte d'identité des personnes mineures.

[…] ».

B.1.3. Aux termes de l'exposé des motifs, la disposition attaquée vise à « identifier le plus efficacement possible des individus », en vue de « renforcer la lutte contre la fraude à l'identité » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3256/001, p. 34).

À cet effet, la disposition attaquée prévoit que la carte d'identité contient désormais l'image numérisée des empreintes digitales de l'index de la main gauche et de la main droite du titulaire ou, en cas d'invalidité ou d'inaptitude, d'un autre doigt de chaque main (article 6,

§ 2, alinéa 3, 8°, de la loi du 19 juillet 1991). Ces informations personnelles sont lisibles uniquement de manière électronique, et non visibles à l'œil nu.

L'image numérisée des empreintes digitales ne peut être conservée que durant le temps nécessaire à la fabrication et à la délivrance de la carte d'identité et, en tout cas, durant une période de maximum trois mois. Passé ce délai de trois mois, les données doivent impérativement être détruites et effacées (article 6, § 2, alinéa 5).

À la suite d'une observation de l'Autorité de protection des données, qui considérait qu'« au lieu de déléguer au Roi la tâche de déterminer les autorités qui seront habilitées à lire les empreintes digitales, c'est au législateur au sens formel du terme qu'il appartient de le faire » (avis n° 106/2018 du 17 octobre 2018, *Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 121), la disposition attaquée énumère les instances habilitées à lire l'image numérisée des empreintes digitales (article 6, § 2, alinéa 6).

Il s'agit du personnel des communes chargé de la délivrance des cartes d'identité, des services de police, « pour autant que cela s'avère nécessaire pour l'accomplissement de leurs missions légales de police administrative et judiciaire dans le cadre de la lutte contre la fraude, notamment la lutte contre la traite et le trafic des êtres humains, l'escroquerie et l'abus de confiance, le blanchiment d'argent, le terrorisme, le faux et usage de faux, l'usurpation de nom et l'usage de faux nom, les violations de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et les entraves aux missions de police administrative », du personnel chargé du contrôle aux frontières, tant en Belgique qu'à l'étranger, des membres du personnel de l'Office des étrangers, « pour autant que cela s'avère nécessaire dans le cadre de la recherche et de la constatation des infractions à la loi du 15 décembre 1980 précitée et à la loi du 30 avril 1999 relative à l'emploi des travailleurs étrangers », des membres du personnel du Service public fédéral des Affaires étrangères et le personnel diplomatique et consulaire, individuellement habilité par l'ambassadeur ou le consul, « dans la mesure où cela s'avère nécessaire dans le cadre de la lutte contre la fraude » et, enfin, de l'entreprise chargée de la production des cartes d'identité et les personnes strictement habilitées par elle en son sein, et ce, « aux seules fins de production et de délivrance des cartes d'identité ».

Le législateur habilite le Roi à déterminer, d'une part, les conditions et modalités de capture de l'image numérisée des empreintes digitales, par arrêté délibéré en Conseil des ministres, et, d'autre part, la forme et les modalités de fabrication, de délivrance et d'utilisation de la carte, après avis de l'Autorité de protection des données dans les deux cas (article 6, § 2, alinéa 3, 8°, et § 7).

B.1.4. L'exposé des motifs indique que la disposition attaquée, alors en projet, est « en phase avec les recommandations de la Commission européenne » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3256/001, p. 35).

Celle-ci avait auparavant déposé, le 17 avril 2018, une proposition de règlement prévoyant le stockage obligatoire d'empreintes digitales sur les cartes d'identité pour les États membres qui délivrent des cartes d'identité, « afin d'endiguer l'utilisation de documents frauduleux dont les terroristes et les criminels peuvent se servir pour entrer dans l'UE à partir d'un pays tiers » (*ibid.*; voy. aussi *Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, pp. 5 et 17).

Il ressort des explications du ministre de la Sécurité et de l'Intérieur en commission de l'Intérieur, des Affaires générales et de la Fonction publique de la Chambre que la disposition attaquée poursuit le même objectif que celui qui est indiqué « dans la justification par la Commission européenne de la proposition de règlement COM (2018) 212 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des titres de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 30).

B.1.5. La disposition attaquée est entrée en vigueur le 23 décembre 2018.

B.2.1. Après l'adoption de la loi du 25 novembre 2018 a été publié au *Journal officiel de l'Union européenne* du 12 juillet 2019 le règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 « relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation » (ci-après : le règlement (UE) 2019/1157).

Ce règlement vise à « renforcer la sécurité pour faciliter l'exercice des droits à la libre circulation par les citoyens de l'Union et les membres de leur famille » (considérant 46). En prévoyant le stockage d'une image faciale et de deux empreintes digitales sur les cartes d'identité et de séjour, il tend à réduire le risque de fraude à l'identité et à « renforcer la sécurité des cartes d'identité et des cartes de séjour » (considérant 18).

B.2.2. Aux termes de son article 1er, le règlement (UE) 2019/1157 « renforce les normes de sécurité applicables aux cartes d'identité délivrées par les États membres à leurs ressortissants et aux documents de séjour délivrés par les États membres aux citoyens de l'Union et aux membres de leur famille lorsqu'ils exercent leur droit à la libre circulation ».

Le règlement s'applique entre autres « aux cartes d'identité délivrées par les États membres à leurs propres ressortissants, conformément à l'article 4, paragraphe 3, de la directive 2004/38/CE » (article 2, point a)).

L'article 3 du règlement (UE) 2019/1157 concerne les « normes de sécurité/format/spécifications » applicables aux cartes nationales d'identité :

« 1. Les cartes d'identité délivrées par les États membres sont de format ID-1 et comportent une zone de lecture automatique (ZLA). Ces cartes d'identité sont établies suivant les spécifications et les normes minimales de sécurité définies dans le document 9303 de l'OACI [Organisation de l'aviation civile internationale] et respectent les exigences énoncées aux points c), d), f) et g) de l'annexe du règlement (CE) n° 1030/2002 tel qu'amendé par le règlement (UE) 2017/1954.

2. Les éléments de données figurant sur les cartes d'identité respectent les spécifications énoncées à la partie 5 du document 9303 de l'OACI.

Par dérogation au premier alinéa, le numéro du document peut être inséré dans la zone I et la désignation du genre de la personne est facultative.

3. Le document porte le titre ' Carte d'identité ' ou un autre intitulé national reconnu dans la ou les langues officielles de l'État membre de délivrance, ainsi que les mots ' Carte d'identité ' dans au moins une autre langue officielle des institutions de l'Union.

4. La carte d'identité comporte, au recto, le code pays à deux lettres de l'État membre délivrant la carte, imprimé en négatif dans un rectangle bleu et entouré de douze étoiles jaunes.

5. Les cartes d'identité intègrent un support de stockage hautement sécurisé qui contient une image faciale du titulaire de la carte et deux empreintes digitales dans des formats numériques interopérables. Pour le recueil des éléments d'identification biométriques, les États membres appliquent les spécifications techniques établies par la décision d'exécution C(2018)7767 de la Commission.

6. Le support de stockage a une capacité suffisante pour garantir l'intégrité, l'authenticité et la confidentialité des données. Les données stockées sont accessibles sans contact et sécurisées comme le prévoit la décision d'exécution C(2018)7767. Les États membres échangent les informations nécessaires pour authentifier le support de stockage ainsi que pour consulter et vérifier les données biométriques visées au paragraphe 5.

7. Les enfants de moins de douze ans peuvent être exemptés de l'obligation de donner leurs empreintes digitales.

Les enfants de moins de six ans sont exemptés de l'obligation de donner leurs empreintes digitales.

Les personnes dont il est physiquement impossible de relever les empreintes digitales sont exemptées de l'obligation de les donner.

8. Lorsque cela est nécessaire et proportionné à l'objectif visé, les États membres peuvent ajouter des précisions et des observations à usage national requises conformément au droit national. L'efficacité des normes minimales de sécurité et la compatibilité transfrontalière des cartes d'identité ne doivent pas en être diminuées.

9. Lorsque les États membres intègrent un composant avec une double interface ou un support de stockage séparé dans la carte d'identité, le support de stockage supplémentaire respecte les normes ISO pertinentes et ne peut interférer avec le support de stockage visé au paragraphe 5.

10. Lorsque les États membres stockent des données pour des services électroniques tels que des services d'administration en ligne ou de commerce électronique dans les cartes d'identité, ces données nationales doivent être physiquement ou logiquement séparées des données biométriques visées au paragraphe 5.

11. Lorsque les États membres ajoutent des éléments de sécurité supplémentaires aux cartes d'identité, la compatibilité transfrontalière de ces cartes d'identité et l'efficacité des normes minimales de sécurité ne doivent pas être diminuées ».

L'article 10 du même règlement concerne le recueil d'éléments d'identification biométriques :

« 1. Les éléments d'identification biométriques sont recueillis exclusivement par du personnel qualifié et dûment habilité désigné par les autorités chargées de délivrer les cartes d'identité ou les cartes de séjour, dans le but d'être intégrés sur le support de stockage hautement sécurisé visé à l'article 3, paragraphe 5, pour les cartes d'identité et à l'article 7, paragraphe 1, pour les cartes de séjour. Par dérogation à la première phrase, les empreintes

digitales sont recueillies uniquement par le personnel qualifié et dûment autorisé de ces autorités, sauf dans le cas des demandes présentées aux autorités diplomatiques et consulaires de l'État membre.

Afin de garantir la cohérence des éléments d'identification biométriques avec l'identité du demandeur, ce dernier doit se présenter en personne au moins une fois au cours du processus de délivrance pour chaque demande.

2. Les États membres veillent à ce que des procédures appropriées et efficaces soient en place pour le recueil des éléments d'identification biométriques et que ces procédures respectent les droits et les principes énoncés dans la Charte, la convention de sauvegarde des droits de l'homme et des libertés fondamentales et la convention des Nations unies relative aux droits de l'enfant.

Lorsque des difficultés se présentent pour recueillir les éléments d'identification biométriques, les États membres veillent à ce que des procédures appropriées soient mises en place pour garantir le respect de la dignité de la personne concernée.

3. Sauf s'ils sont nécessaires aux finalités du traitement dans le respect du droit de l'Union et du droit national, les éléments d'identification biométriques stockés aux fins de la personnalisation des cartes d'identité ou des documents de séjour sont conservés de manière très sécurisée et uniquement jusqu'à la date de remise du document et, en tout état de cause, pas plus de 90 jours à compter de la date de délivrance du document. Après ce délai, ces éléments d'identification biométriques sont immédiatement effacés ou détruits ».

L'article 11 du même règlement concerne la protection des données à caractère personnel et la responsabilité :

« 1. Sans préjudice du règlement (UE) 2016/679, les États membres veillent à la sécurité, à l'intégrité, à l'authenticité et à la confidentialité des données recueillies et stockées aux fins du présent règlement.

2. Aux fins du présent règlement, les autorités chargées de la délivrance des cartes d'identité et des documents de séjour sont considérées comme le responsable du traitement visé à l'article 4, paragraphe 7, du règlement (UE) 2016/679 et sont responsables du traitement des données à caractère personnel.

3. Les États membres veillent à ce que les autorités de contrôle puissent exercer pleinement leurs missions visées dans le règlement (UE) 2016/679, y compris l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires ainsi que l'accès à tout local ou matériel de traitement des données des autorités compétentes.

4. La coopération avec les prestataires de services extérieurs n'exclut pas la responsabilité d'un État membre qui peut découler du droit de l'Union ou du droit national en cas de manquement aux obligations en matière de données à caractère personnel.

5. Les informations lisibles par machine ne peuvent figurer sur une carte d'identité ou un document de séjour que conformément au présent règlement et au droit national de l'État membre de délivrance.

6. Les données biométriques stockées sur le support de stockage des cartes d'identité et des documents de séjour ne sont utilisées, conformément au droit de l'Union et au droit national, que par le personnel dûment autorisé des autorités nationales compétentes et des agences de l'Union pour vérifier :

a) l'authenticité de la carte d'identité ou du document de séjour;

b) l'identité du titulaire grâce à des éléments comparables directement disponibles lorsque la loi exige la présentation de la carte d'identité ou du document de séjour.

7. Les États membres tiennent à jour et communiquent chaque année à la Commission la liste des autorités compétentes ayant accès aux données biométriques stockées sur le support de stockage visé à l'article 3, paragraphe 5, du présent règlement. La Commission publie en ligne une compilation de ces listes nationales ».

L'article 14 du même règlement concerne les spécifications techniques supplémentaires :

« 1. Afin de garantir, le cas échéant, que les cartes d'identité et les documents de séjour visés à l'article 2, points a) et c), respectent les futures normes de sécurité minimales, la Commission établit, au moyen d'actes d'exécution, des spécifications techniques complémentaires sur :

a) les éléments et les exigences de sécurité complémentaires, y compris les normes renforcées de lutte contre la contrefaçon et la falsification;

b) les spécifications techniques relatives au support de stockage des éléments biométriques visés à l'article 3, paragraphe 5, et à leur sécurisation, y compris la prévention de l'accès non autorisé et la facilitation de la validation;

c) les exigences en matière de qualité et les normes techniques communes en ce qui concerne l'image faciale et les empreintes digitales.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 15, paragraphe 2.

2. Conformément à la procédure mentionnée à l'article 15, paragraphe 2, il peut être décidé que les spécifications visées au présent article sont secrètes et ne sont pas publiées. Dans ce cas, elles ne sont communiquées qu'aux organismes chargés par les États membres de l'impression et aux personnes dûment autorisées par un État membre ou par la Commission.

3. Chaque État membre désigne un organisme chargé de l'impression des cartes d'identité ainsi qu'un organisme chargé de l'impression des cartes de séjour des membres de la famille des citoyens de l'Union, et communique le nom de ces organismes à la Commission et aux

autres États membres. Les États membres ont le droit de changer d'organisme désigné. Ils en informent la Commission et les autres États membres.

Les États membres peuvent également décider de désigner un organisme unique chargé de l'impression des cartes d'identité et des cartes de séjour des membres de la famille des citoyens de l'Union, et ils communiquent le nom de cet organisme à la Commission et aux autres États membres.

Deux ou plusieurs États membres peuvent également décider de désigner un organisme unique à ces fins. Ils en informent la Commission et les autres États membres ».

B.2.3. En vertu de son article 16, le règlement (UE) 2019/1157 est entré en vigueur le 1er août 2019. Il est applicable à partir du 2 août 2021, ce qui implique qu'à compter de cette date, les États membres ne doivent délivrer que des documents d'identité et de séjour qui respectent les exigences qu'il prévoit (considérant 44).

*Quant à la recevabilité*

*En ce qui concerne la recevabilité du mémoire du Conseil des ministres dans l'affaire n° 7150*

B.3.1. Les parties requérantes dans l'affaire n° 7150 invoquent la nullité du mémoire du Conseil des ministres, au motif qu'il comporte un ou plusieurs passages en anglais, non traduits, ce qui constituerait une violation de l'article 40 de la loi du 15 juin 1935 « sur l'emploi des langues en matière judiciaire » et entraînerait une violation des droits de la défense.

B.3.2. La loi du 15 juin 1935 « sur l'emploi des langues en matière judiciaire » n'est pas applicable aux procédures devant la Cour constitutionnelle. Le mémoire du Conseil des ministres a été rédigé en néerlandais, conformément à l'article 62, alinéa 2, 1°, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle. La reproduction par le Conseil des ministres d'un graphique dont la légende est en anglais, mais qui est explicité dans le mémoire, en néerlandais, à l'appui de son argumentation, ne constitue pas une violation de l'article 62, alinéa 2, 1°, précité.

B.3.3. L'exception est rejetée.

*En ce qui concerne l'incidence de l'entrée en vigueur du règlement (UE) 2019/1157 sur la recevabilité des recours*

B.4.1. Le Conseil des ministres soutient qu'à supposer que l'intérêt dont les parties requérantes doivent justifier existait au moment de l'introduction des requêtes, cet intérêt n'existe plus, en tout état de cause, en raison de l'entrée en vigueur du règlement (UE) 2019/1157, postérieurement à l'adoption de la disposition attaquée.

B.4.2. Comme il est dit en B.1.4, le législateur a adopté la disposition attaquée alors que le règlement (UE) 2019/1157 était encore à l'état de projet.

Il ne découle pas du fait que certaines dispositions de l'article 27, attaqué, de la loi du 25 novembre 2018 ont une portée analogue à certaines dispositions du règlement (UE) 2019/1157 que les parties requérantes ne justifient plus, le cas échéant, d'un intérêt actuel à leurs recours, ni que la Cour ne serait plus compétente pour juger de la constitutionnalité de la disposition attaquée. Toutefois, cette circonstance a pour conséquence que la Cour doit tenir compte du règlement précité.

B.4.3. Contrairement à ce que soutient le Conseil des ministres, les parties requérantes ne devaient pas introduire un recours en annulation du règlement (UE) 2019/1157 devant la Cour de justice de l'Union européenne pour conserver leur intérêt.

B.4.4. L'exception est rejetée.

*En ce qui concerne la recevabilité des recours*

B.5.1. Le Conseil des ministres conteste l'intérêt des parties requérantes dans les affaires n$^{os}$ 7125, 7150 et 7211. Selon lui, ces parties ne démontrent pas concrètement l'existence d'un lien suffisamment individualisé entre la disposition attaquée et leur situation, d'autant plus que la partie requérante dans l'affaire n° 7211, âgée d'un an au moment de l'introduction de la

requête, ne sera pas soumise avant l'âge de quinze ans à l'obligation de détenir une carte d'identité. Par ailleurs, le « Parti Libertarien », première partie requérante dans l'affaire n° 7125, n'établit pas qu'il dispose de la personnalité juridique ni qu'il peut se prévaloir de l'exception dans le cadre de laquelle les partis politiques sont admis à agir devant la Cour.

B.5.2. Aux termes de l'article 2, 2°, de la loi spéciale du 6 janvier 1989, la partie requérante devant la Cour doit être une personne physique ou morale justifiant d'un intérêt. Les partis politiques qui sont des associations de fait n'ont pas, en principe, la capacité requise pour introduire un recours devant la Cour.

Il n'en va autrement que lorsqu'ils agissent dans des matières pour lesquelles ils sont légalement reconnus comme formant des entités distinctes et que, alors que leur intervention est légalement reconnue, certains aspects de celle-ci sont en cause.

B.5.3. Tel n'est pas le cas en l'espèce. Le recours est irrecevable en ce qu'il est introduit par le « Parti Libertarien ».

B.5.4. 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 la norme attaquée.

B.5.5. La disposition attaquée impose à tous les Belges soumis à l'obligation de détenir une carte d'identité, à savoir tous les Belges à partir de l'âge de douze ans (articles 1er et 2 de l'arrêté royal du 25 mars 2003 « relatif aux cartes d'identité »), le prélèvement de deux empreintes digitales et le stockage de l'image numérisée de celles-ci sur la carte d'identité.

Elle affecte donc directement et défavorablement la situation de la seconde partie requérante dans l'affaire n° 7125, des quatre parties requérantes dans l'affaire n° 7150, ainsi que de la partie requérante dans l'affaire n° 7211. La circonstance qu'en ce qui concerne chacune de ces parties, la mise en œuvre de la disposition attaquée n'intervient pas

immédiatement, mais lors de la délivrance d'une nouvelle carte d'identité ou, le cas échéant, lorsque la personne concernée atteint l'âge de douze ans, ne change rien à ce constat.

La seconde partie requérante dans l'affaire n° 7125, les quatre parties requérantes dans l'affaire n° 7150 et la partie requérante dans l'affaire n° 7211 justifient d'un intérêt à leur recours.

B.5.6. Sauf en ce qui concerne la capacité à agir du « Parti Libertarien », les exceptions sont rejetées.

B.5.7. L'intérêt à agir des parties requérantes dans les affaires n$^{os}$ 7202 et 7203 n'est pas contesté par le Conseil des ministres.

*En ce qui concerne l'intérêt des parties intervenantes dans l'affaire n° 7150*

B.6.1. Le Conseil des ministres conteste l'intérêt du « Parti Libertarien » et de Baudoin Collard, parties requérantes dans l'affaire n° 7125, et de l'ASBL « Ligue des droits humains », partie requérante dans l'affaire n° 7203, à intervenir dans l'affaire n° 7150, dès lors que ces parties ont déjà pu faire valoir leurs moyens dans leur propre requête et, à titre subsidiaire, pour les mêmes motifs que ceux qui sont mentionnés en B.5.1.

B.6.2. Pour le même motif que celui qui est énoncé en B.5.2 et en B.5.3, l'intervention du « Parti Libertarien » est irrecevable.

B.6.3. Lorsque la Cour est saisie d'un recours en annulation, « toute personne justifiant d'un intérêt » peut adresser ses observations à la Cour dans un mémoire (article 87, § 2, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle).

Justifie d'un intérêt au sens de cette disposition la personne qui montre que sa situation peut être directement affectée par l'arrêt que la Cour est appelée à rendre à propos du recours en annulation.

B.6.4. Compte tenu de ce qui est dit en B.5.5, Baudoin Collard et l'ASBL « Ligue des droits humains » justifient de l'intérêt requis à leur intervention.

B.6.5. L'exception est rejetée.

*En ce qui concerne la recevabilité de certains moyens*

B.7.1. Le Conseil des ministres soutient que la seconde branche du moyen unique dans l'affaire n° 7125, la première branche du second moyen dans l'affaire n° 7150, le premier moyen dans l'affaire n° 7202 et la seconde branche du quatrième moyen dans les affaires n$^{os}$ 7203 et 7211 sont irrecevables, en ce qu'ils critiquent l'absence d'exécution d'une analyse d'impact sur la protection des données, au sens de l'article 35 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données) » (ci-après : le RGPD), préalablement à l'adoption de la disposition attaquée. Selon le Conseil des ministres, la Cour n'est pas compétente pour connaître d'un grief portant sur le processus ou les modalités d'élaboration d'une loi.

B.7.2. Si le traitement de données personnelles est susceptible d'engendrer un « risque élevé pour les droits et libertés des personnes physiques », le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel, conformément à l'article 35 du RGPD. En vertu de l'article 36 du même règlement, lorsque l'analyse d'impact indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque, le responsable du traitement doit consulter l'autorité de contrôle préalablement au traitement.

B.7.3. Sans qu'il soit nécessaire de se prononcer sur la compétence de la Cour pour connaître de griefs relatifs au processus ou aux modalités d'élaboration de la disposition

attaquée, il y a lieu de constater que l'article 35 du RGPD impose la réalisation d'une analyse d'impact relative à la protection des données avant le traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, mais non lors de l'élaboration d'une disposition législative relative à un tel traitement.

En vertu de l'article 35, paragraphe 10, du RGPD, lorsqu'un 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 et qu'il « a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit réglemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question », il n'y a pas lieu d'effectuer une nouvelle analyse d'impact avant les activités de traitement, à moins que les États membres ne l'estiment nécessaire.

Il s'ensuit que la réalisation d'une analyse d'impact générale dans le cadre de l'adoption d'une disposition législative relative à un traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques est facultative mais que si, néanmoins, une telle analyse d'impact est effectuée, il n'y a en principe pas lieu d'effectuer une nouvelle analyse d'impact avant le traitement.

L'article 35 du RGPD ne s'oppose donc pas à la réalisation d'une analyse d'impact lors de l'élaboration des arrêtés d'exécution de la disposition attaquée.

Ce constat ne porte pas préjudice à l'obligation pour les États membres de consulter « l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement », conformément à l'article 36, paragraphe 4, du RGPD, obligation à laquelle le législateur a déféré en l'espèce.

B.7.4. Le moyen unique dans l'affaire n° 7125, en sa seconde branche, le second moyen dans l'affaire n° 7150, en sa première branche, le premier moyen dans l'affaire n° 7202, en tant que ce moyen est pris de la violation de l'article 35 du RGPD, et le quatrième moyen dans les affaires n$^{os}$ 7203 et 7211, en sa seconde branche, ne sont donc pas fondés.

Dès lors que la portée de l'article 35 du RGPD ne laisse place à aucun doute raisonnable, au sens de l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 1982 en cause *CILFIT* (C-283/81), il n'y a pas lieu de poser de question préjudicielle en interprétation de cette disposition à la Cour de justice.

B.8.1. Le Conseil des ministres fait valoir que la première branche du moyen unique dans l'affaire n° 7125 n'est pas recevable en tant qu'elle est prise de la violation des articles 10 et 11 de la Constitution, à défaut pour les parties requérantes d'identifier deux catégories de personnes que la disposition attaquée traiterait d'une manière discriminatoire.

B.8.2. 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.8.3. 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.9.1. Le Conseil des ministres soutient que le second moyen dans l'affaire n° 7150, ainsi que les trois moyens dans l'affaire n° 7202 ne sont pas recevables, en tant qu'ils sont pris de la violation du RGPD, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil » (ci-après : la directive « police ») et de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » (ci-après : la loi du 30 juillet 2018).

Selon lui, la Cour n'est pas compétente pour connaître directement de la violation d'un règlement, d'une directive ou d'une loi. Ensuite, les parties requérantes dans l'affaire n° 7202 négligent d'indiquer, dans les trois moyens qu'elles invoquent, les catégories de citoyens qu'il conviendrait de comparer, dans le cadre d'un contrôle indirect, par le truchement des articles 10 et 11 de la Constitution. Enfin, le RGPD et la directive « police » ne garantiraient pas un droit analogue au droit au respect de la vie privée consacré par l'article 22 de la Constitution.

B.9.2. La Cour n'est pas compétente pour contrôler directement des normes législatives au regard de dispositions conventionnelles ou du droit de l'Union.

Toutefois, lorsqu'une disposition conventionnelle ou du droit de l'Union liant la Belgique a une portée analogue à celle d'une des dispositions constitutionnelles dont le contrôle relève de la compétence de la Cour et dont la violation est alléguée, les garanties consacrées par cette disposition conventionnelle ou du droit de l'Union constituent un ensemble indissociable avec les garanties inscrites dans les dispositions constitutionnelles concernées.

Il s'ensuit que, dans le contrôle qu'elle exerce au regard des dispositions constitutionnelles mentionnées en B.9.1, la Cour tient compte des dispositions de droit international ou de droit de l'Union qui garantissent des droits ou libertés analogues.

B.9.3. L'article 22 de la Constitution garantit le droit au respect de la vie privée et familiale. Ce droit comprend le droit à la protection des données à caractère personnel.

Aux termes de son article 1er, paragraphe 2, le RGPD « protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel ». Les dispositions du RGPD qui sont invoquées par les parties requérantes concrétisent ce droit.

B.9.4. Sans qu'il soit besoin, d'une part, de déterminer si et, le cas échéant, dans quelle mesure la directive « police » est applicable en l'espèce ni, d'autre part, de se prononcer sur la question de savoir si la Cour est compétente pour connaître d'une violation de la loi du 30 juillet 2018, lue en combinaison avec les articles 10 et 11 de la Constitution, il y a lieu de constater

que les parties requérantes dans l'affaire n° 7202 ne développent aucune critique particulière en lien avec cette directive ou avec cette loi ni n'indiquent en quoi celles-ci contiendraient des garanties distinctes de celles qui sont prévues par le RGPD et qui seraient pertinentes au regard de la problématique litigieuse.

B.9.5. En tant qu'ils sont pris de la violation de la directive « police » et de la loi du 30 juillet 2018, les premier et troisième moyens dans l'affaire n° 7202 sont irrecevables. Les exceptions sont rejetées pour le surplus.

B.10.1. Le Conseil des ministres fait valoir que les premier à troisième moyens dans les affaires n$^{os}$ 7203 et 7211 sont irrecevables, car les parties requérantes se contentent de renvoyer à la requête introduite dans l'affaire n° 7202, sans même exposer ni développer ces moyens.

B.10.2. 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.10.3. Le renvoi aux moyens exposés dans un recours distinct, même réputés intégralement reproduits, ne satisfait pas aux exigences précitées de l'article 6 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle. Les premier à troisième moyens dans les affaires n$^{os}$ 7203 et 7211 sont dès lors irrecevables.

*Quant aux demandes de mesures d'instruction formulées par les parties requérantes*

B.11.1. Les parties requérantes dans les affaires n^os^ 7150 et 7202 sollicitent de la Cour qu'elle ordonne des mesures d'instruction en vue notamment d'obtenir un avis technique au sujet de la description insuffisante et de l'absence de détermination des éléments essentiels de la mesure litigieuse, de l'existence d'alternatives à celle-ci, ainsi que des risques qu'elle entraîne en matière de sécurité.

B.11.2. Selon l'article 91, alinéa 1er, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, la Cour dispose des « pouvoirs d'instruction et d'investigation les plus étendus », dont certains sont énoncés à l'alinéa 2 de cette disposition. La Cour peut exclusivement faire usage de ces pouvoirs d'instruction et d'investigation lorsque ceux-ci sont nécessaires à la solution des questions juridiques qu'elle doit trancher. Une mesure d'instruction n'est utile qu'en ce qu'il est possible de constater des éléments matériels pertinents pour statuer sur un recours en annulation, une question préjudicielle ou un incident.

B.11.3. Compte tenu des éléments dont la Cour dispose et des explications qui ont été fournies à cet égard dans les requêtes et dans les mémoires, il n'y a pas lieu d'ordonner des mesures d'instruction complémentaires.

La demande de mesures d'instruction est rejetée.

*Quant au fond*

B.12. Les parties requérantes prennent plusieurs moyens de la violation, par la disposition attaquée, du droit au respect de la vie privée et du droit à la protection des données à caractère personnel (première branche du moyen unique dans l'affaire n° 7125 et du quatrième moyen dans les affaires n^os^ 7203 et 7211; premier moyen et seconde branche du second moyen dans l'affaire n° 7150; premier à troisième moyens dans l'affaire n° 7202).

*En ce qui concerne le droit au respect de la vie privée et le droit à la protection des données à caractère personnel*

B.13.1. 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.13.2. 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.13.3. 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.14.1. 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.

Ce droit 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 et les informations concernant des biens (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).

B.14.2. 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.

Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait établi un juste équilibre entre tous les droits et intérêts en cause.

B.15.1. Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (ci-après : la Charte) ont, en ce qui concerne le traitement des données à caractère personnel, une portée analogue à celle de l'article 8 de la Convention européenne des droits de l'homme (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke GbR et autres*) et de l'article 22 de la Constitution. Il en va de même pour l'article 16, paragraphe 1, du Traité sur le fonctionnement de l'Union européenne et pour l'article 17 du Pacte international relatif aux droits civils et politiques.

B.15.2. 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 identifiée ou identifiable (CJUE, grande chambre,

9 novembre 2010, précité, point 52; 16 janvier 2019, C-496/17, *Deutsche Post AG*, point 54). Ainsi, à l'instar de la Cour européenne des droits de l'homme, la Cour de justice juge que les empreintes digitales constituent des données à caractère personnel, « dès lors qu'elles contiennent objectivement des informations uniques sur des personnes physiques et permettent leur identification précise » (CJUE, 17 octobre 2013, C-291/12, *Schwarz c. Stadt Bochum*, point 27 ; 3 octobre 2019, C-70/18, *Staatssecretaris van Justitie en Veiligheid c. A, B et C*, point 55).

B.15.3. 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.15.4. Par l'arrêt *Schwarz c. Stadt Bochum* précité du 17 octobre 2013, la Cour de justice a jugé que le règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 « établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres » (ci-après : le règlement (CE) n° 2252/2004), qui impose le prélèvement des empreintes digitales et leur conservation dans les passeports, est compatible avec le droit au respect de la vie privée et avec le droit à la protection des données à caractère personnel.

B.16.1. L'article 5 du RGPD concerne les principes relatifs au traitement des données à caractère personnel :

« 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) ».

B.16.2. L'article 6 du RGPD concerne la licéité du traitement :

« 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 ».

B.16.3. L'article 9 du RGPD concerne le traitement de catégories particulières de données à caractère personnel :

« 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 :

[…]

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée;

[…]

3. […]

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 ».

B.16.4. L'article 25 du RGPD porte sur la protection des données dès la conception et sur la protection des données par défaut :

« 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des

moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article ».

B.16.5. L'article 32 du RGPD concerne la sécurité du traitement :

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

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre ».

*En ce qui concerne l'examen des griefs*

B.17. Il ressort de l'examen des moyens que les parties requérantes critiquent plusieurs aspects de la disposition attaquée, que la Cour examine dans l'ordre suivant :

1. Le prélèvement de deux empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité, en ce compris les aspects techniques;

2. La conservation centralisée de l'image numérisée des empreintes digitales pour les besoins de la fabrication et de la délivrance de la carte d'identité;

3. La lecture de l'image numérisée des empreintes digitales.

*1. Le prélèvement de deux empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité, en ce compris les aspects techniques*

B.18. Les parties requérantes font valoir qu'en ce qu'elle impose le prélèvement de deux empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité, 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 qui ne poursuit pas un but légitime. Les objectifs poursuivis ne constituent en tout état de cause pas un motif d'intérêt public important au sens de l'article 9, paragraphe 2, point g), du RGPD.

Les parties requérantes soutiennent que la disposition attaquée viole le principe de la légalité garanti par les dispositions visées dans les moyens, dès lors que la délégation conférée au Roi en ce qui concerne l'exécution de la disposition attaquée n'est pas décrite d'une manière suffisamment précise et qu'elle n'en fixe pas tous les éléments essentiels requis.

Elles font valoir, en particulier, que le processus de fabrication et de délivrance des cartes d'identité n'est pas suffisamment décrit par la disposition attaquée. Ainsi, celle-ci ne détermine ni la technologie utilisée, ni les mesures techniques en vue de protéger les empreintes digitales sur la puce, ce qui permet ainsi la lecture des empreintes digitales sans contact et à distance, à l'insu du détenteur de la carte, ainsi que la lecture de celles-ci à l'œil nu. Elle ne détermine pas non plus la technique ou la méthode par laquelle l'empreinte digitale est enregistrée et lue. La disposition attaquée ne prévoit pas non plus le principe d'une sanction en cas de non-respect des règles relatives à la fabrication, notamment en ce qui concerne l'effacement obligatoire des données à l'issue de ce processus. Enfin, la disposition attaquée permet la conservation des données après la fabrication de la carte d'identité.

Les parties requérantes font également valoir que l'ingérence n'est pas nécessaire ni proportionnée aux objectifs poursuivis. Elles soutiennent que les cartes d'identité sont aujourd'hui suffisamment sécurisées et qu'elles peuvent difficilement être contrefaites. Par ailleurs, les chiffres en matière de fraude qui sont avancés dans les travaux préparatoires sont négligeables et ne sauraient justifier le prélèvement des empreintes digitales et le stockage de celles-ci sur la carte d'identité de l'ensemble des Belges âgés de douze ans et plus, ce qui aboutit à « précriminaliser » l'ensemble des personnes concernées et entraîne un risque d'abus considérable. Enfin, les parties requérantes font valoir que, outre le fait que les empreintes digitales ne sont pas infaillibles, il existe des mesures alternatives moins attentatoires au droit au respect de la vie privée.

B.19.1. Comme il est dit en B.14.1, le droit au respect de la vie privée englobe la protection des données à caractère personnel et des informations personnelles dont relèvent, notamment, les empreintes digitales.

En ce qu'elle prévoit le prélèvement de deux empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité, la disposition attaquée entraîne donc une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel, tels qu'ils sont garantis par les dispositions citées en B.13 à B.16.

B.19.2. Comme il est en dit en B.14.2, 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. Il ressort par ailleurs de l'article 52, paragraphe 1, de la Charte que l'ingérence doit respecter le contenu essentiel des droits concernés et que, 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.

Dès lors que les empreintes digitales constituent des données biométriques, au sens de l'article 4, point 14), 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. En vertu de l'article 11, paragraphe 1, du règlement (UE) 2019/1157, les données à caractère personnel qui doivent être traitées en application du règlement sont soumises au RGPD.

L'article 9, paragraphe 2, point g), du RGPD permet le traitement des données à caractère personnel sensibles, telles les données biométriques, lorsqu'il est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

B.20.1. Selon l'exposé des motifs, la disposition attaquée vise à permettre l'identification le plus efficacement possible des individus, en vue de renforcer la lutte contre la fraude à l'identité :

« À l'heure actuelle, il s'impose de prendre les mesures nécessaires en vue d'identifier le plus efficacement possible les individus.

Sur le même principe que le passeport et pour renforcer la lutte contre la fraude à l'identité, le présent article prévoit que la puce des cartes d'identité intégrera les empreintes digitales, plus précisément l'image numérisée des empreintes digitales de l'index de la main gauche et celui de la main droite.

Cet enregistrement sur la carte d'identité permettra par exemple aux services de police de vérifier l'exactitude du lien entre une carte d'identité et le porteur de celle-ci » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3256/001, p. 34).

Le rapport de la commission de l'Intérieur, des Affaires générales et de la Fonction publique de la Chambre expose :

« Il sera ainsi possible de contrôler les cartes d'identité, comme les passeports, lors du franchissement des frontières intérieures de l'Europe » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 16).

La disposition attaquée vise à lutter plus spécifiquement contre la fraude basée sur la ressemblance (également dite « fraude *look alike* ») et l'obtention frauduleuse de documents authentiques. Ces deux types de fraude seraient en voie d'augmentation, alors que la fraude classique, consistant dans la contrefaçon des documents d'identité (la fraude dite « documentaire »), diminue (*ibid.*, p. 31).

La disposition attaquée contribue ainsi à prévenir les infractions liées à la fraude à l'identité, celle-ci étant « la plupart du temps associée à un autre délit (trafic d'êtres humains, fraude, criminels souhaitant rester sous le radar, personnes parties combattre en Syrie qui essaient d'entrer clandestinement en Europe, terroristes potentiels, etc.) » (*ibid.*, p. 33).

Comme il est dit en B.1.4, la disposition attaquée poursuit le même objectif que la proposition de règlement devenue le règlement (UE) 2019/1157, comme l'a confirmé le ministre de la Sécurité et de l'Intérieur en commission de la Chambre :

« De manière générale, [l'Autorité de protection des données] se demande quel est l'objectif de cette mesure. Ce dernier est pourtant indiqué dans l'exposé des motifs ainsi que dans la justification par la Commission européenne de la proposition de

règlement COM (2018) 212 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des titres de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation.

Le ministre renvoie également à la communication de la Commission au Parlement européen et au Conseil de 2016 (COM 2016/790) relative au Plan d'action visant à renforcer la réponse de l'UE aux fraudes liées aux documents de voyage. Le dépôt de l'actuelle proposition de règlement de la Commission européenne découle directement de ce document. On peut y lire ce qui suit :

‘ Les documents de voyage de l'UE sont très prisés des fraudeurs. Au moins trois quarts des documents frauduleux détectés aux frontières extérieures, mais également dans l'espace sans contrôle aux frontières intérieures, imitent certains documents délivrés par des États membres de l'UE et des pays associés à l'espace Schengen. Selon des rapports récents du corps européen de garde-frontières et de garde-côtes, les cartes nationales d'identité d'un moindre degré de sécurité délivrées par des États membres sont les faux documents les plus fréquemment détectés en ce qui concerne les déplacements à l'intérieur de l'espace Schengen. La fraude basée sur la ressemblance (où la personne en possession du document n'est qu'un sosie du véritable titulaire) continue d'augmenter et demeurait, au deuxième trimestre 2016, le type de fraude le plus fréquemment signalé. L'obtention de documents authentiques à partir de faux documents ‘‘ sources ’’ (certificats de naissance, de mariage ou de décès) reste l'une des plus grandes menaces car elle est extrêmement difficile à détecter. ’

Selon le rapport 2016 du corps européen de garde-frontières et de garde-côtes, les faits d'imposture et d'obtention frauduleuse de documents authentiques ont respectivement augmenté de 4 % et 76 % entre le premier trimestre 2015 et le premier trimestre 2016, tandis que la fraude consistant en la falsification de documents a diminué (-8 %).

Nous apprenons ainsi que trois quarts des documents frauduleux détectés aux frontières extérieures sont d'origine européenne. Il s'avère de même que la fraude basée sur la ressemblance et l'obtention frauduleuse de documents authentiques (par le biais des communes) ne cessent de s'accroître, l'augmentation atteignant respectivement 4 % et 76 % en 2015 et 2016.

Comment cela se traduit-il en Belgique, l'un des 15 États membres à rendre la carte d'identité obligatoire ? Depuis l'introduction des nouvelles cartes d'identité électroniques en 2005 et l'utilisation d'éléments de sécurité de pointe, le nombre de cartes falsifiées a considérablement baissé. La falsification d'une carte d'identité électronique a été rendue si difficile qu'un glissement s'est opéré vers la fraude basée sur la ressemblance et l'obtention frauduleuse de documents authentiques par le biais de la commune, sur la base d'un faux nom ou d'une fausse photo. Au cours de la période 2006-2010, les falsifications ont reculé de 62 % à 29 %, la fraude intellectuelle (basée sur la ressemblance et l'obtention frauduleuse de documents authentiques) passant de 38 % à 71 %.

Les chiffres du SPOC fraude à l'identité nationale (mis en place au sein de la task force fraude à l'identité) concernant le nombre de dossiers de fraude potentielle à l'identité ouverts en 2016, 2017 et jusqu'en septembre 2018 sont éloquents. Il est passé de 402 dossiers en 2016 à 796 en 2017 et à 955 dossiers déjà en 2018.

À cet égard, il est frappant de constater la différence entre les cartes d'identité électroniques et les passeports et les cartes pour étrangers sur lesquels les empreintes digitales figurent déjà. En 2016, on a dénombré 230 dossiers de fraude à l'identité à l'aide d'une carte d'identité électronique, en 2017, 467 et en 2018, déjà 566. Pour ce qui est des passeports et des cartes pour étrangers, le nombre de dossiers s'élevait respectivement à 76 et 13 en 2016, 60 et 19 en 2017 et 97 et 7 en 2018. Il ressort donc des chiffres que la fraude aux titres pourvus d'empreintes digitales recule par rapport à la carte d'identité électronique qui devient un maillon faible et est davantage utilisée pour la fraude à l'identité.

Les dossiers du SPOC national ' fraude à l'identité ' se basent sur les cas signalés par les communes. Les services de police observent toutefois également une augmentation du nombre de tentatives de fraude fondées sur la ressemblance et de tentatives d'obtention frauduleuse d'un document authentique établi au nom d'une autre personne. En 2013, le service de police ' faux documents ' a été amené à enquêter sur 96 cas. Ce chiffre est passé à 340 en 2017 et on enregistrait déjà 159 cas au premier semestre 2018. Il convient de souligner à nouveau que ces statistiques reprennent uniquement les cas qui ont été découverts. Entre 2013 et le premier semestre 2018, 2 027 cas ont été enregistrés lors de contrôles de police effectués à la frontière.

Si l'on y ajoute les 1 374 dossiers instruits par le service ' faux documents ', on obtient au total 3 401 cas pour cette période. On constate également qu'au cours de la même période, la fraude fondée sur la ressemblance et l'acquisition frauduleuse de documents authentiques sont passées de 20 à 30 % du nombre total de cas de fraude à l'identité perpétrés par le biais de documents.

Or, la fraude fondée sur la ressemblance et l'acquisition frauduleuse de documents authentiques sont précisément des formes de fraude qui exploitent les points faibles de la photographie. Dans le premier cas, le fraudeur utilise la carte d'une personne qui lui ressemble ou à laquelle il fait en sorte de ressembler (il peut s'agir d'une carte volée ou trouvée ou encore d'une carte qui a été donnée). Dans le second, le fraudeur fournit sa propre photo pour faire établir un document au nom d'une autre personne. Il affirme par exemple avoir égaré sa carte d'identité électronique et introduit une demande pour en obtenir une nouvelle. En l'absence d'éléments biométriques supplémentaires comme l'empreinte digitale, ce type de fraude est impossible à déceler. La photo ne suffit pas à elle seule à garantir rapidement et de façon efficace qu'il s'agit bien de la véritable identité de l'intéressé » (*ibid.*, pp. 30-32).

La disposition attaquée met ainsi en œuvre, certes de manière anticipée, le règlement (UE) 2019/1157 qui, comme il est dit en B.2.1, vise à « renforcer la sécurité pour faciliter l'exercice des droits à la libre circulation par les citoyens de l'Union et les membres de leur famille » (considérant 46) à et réduire le risque de fraude à l'identité (considérant 18).

B.20.2. Ces objectifs sont légitimes, dès lors qu'ils visent à protéger les droits et libertés d'autrui. Ils constituent par ailleurs des objectifs d'intérêt général reconnus par l'Union.

La Cour de justice de l'Union européenne a en effet jugé que le règlement (CE) n° 2252/2004, qui prévoit l'intégration de deux empreintes digitales sur les passeports et dont les objectifs sont, d'une part, de prévenir la falsification des passeports et, d'autre part, d'empêcher leur utilisation frauduleuse, et ce en vue d'empêcher, notamment, l'entrée illégale de personnes sur le territoire de l'Union, poursuit un objectif d'intérêt général reconnu par l'Union (CJUE, 17 octobre 2013, C-291/12, *Schwarz c. Stadt Bochum*, points 36-38; voy. aussi CJUE, 7 novembre 2013, C-225/12, *Demir*, point 41; 3 octobre 2019, C-70/18, *Staatssecretaris van Justitie en Veiligheid c. A, B et C*, points 46-49).

Les objectifs précités constituent également des motifs d'intérêt public important, au sens de l'article 9, paragraphe 2, point g), du RGPD, ce qui se déduit par ailleurs de l'adoption, par le législateur européen, du règlement (UE) 2019/1157.

B.21.1. La disposition attaquée est pertinente en vue de la réalisation des objectifs poursuivis, dès lors que la conservation de l'image numérisée des empreintes digitales sur la carte d'identité est susceptible, d'une part, de réduire le risque de falsification des cartes d'identité et de faciliter la tâche des autorités chargées d'examiner, notamment aux frontières, l'authenticité de celles-ci et, d'autre part, de prévenir l'utilisation frauduleuse des cartes d'identité, comme la Cour de justice l'a jugé en matière de passeports à propos du règlement (CE) n° 2252/2004 (CJUE, 17 octobre 2013, C-291/12, *Schwarz c. Stadt Bochum*, points 41-45).

L'absence de fiabilité totale du procédé et l'impossibilité corrélative d'exclure complètement la non-détection de certains cas de fraude à la ressemblance ne conduisent pas à une conclusion différente. Ainsi que la Cour de justice l'a jugé par son arrêt *Schwarz c. Stadt Bochum* précité, « il n'est pas déterminant que [la] méthode ne soit pas totalement fiable. En effet, d'une part, bien qu'elle n'exclue pas complètement les acceptations de personnes non autorisées, il suffit qu'elle réduise considérablement le risque de telles acceptations qui existerait si cette même méthode n'était pas utilisée » (point 43).

B.21.2. Le fait que certaines formes de fraude à l'identité ne supposent pas l'utilisation d'une carte d'identité ne change rien à la réalité du phénomène de la fraude à la ressemblance au moyen d'une carte d'identité, que la disposition attaquée tend à combattre en permettant aux instances qui y sont habilitées de lire l'image numérisée de deux empreintes digitales.

B.21.3. Contrairement à ce que soutiennent les parties requérantes, le fait que la puce contenant l'image numérisée des empreintes digitales puisse être endommagée, sans empêcher l'utilisation de la carte d'identité par son titulaire, à le supposer techniquement avéré, n'est pas de nature à mettre en doute l'efficacité de la disposition attaquée. La neutralisation de la puce aurait pour effet d'éveiller la suspicion des instances habilitées à lire l'image numérisée des empreintes digitales et les conduirait à exercer un contrôle plus approfondi de l'identité de la personne concernée, ce qui n'est vraisemblablement pas le but poursuivi par les personnes qui usurpent l'identité d'un tiers.

B.22.1. 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.

B.22.2. 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).

Toute personne doit dès lors 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.22.3. Il convient donc d'examiner si, d'une part, les délégations au Roi sont conformes au principe de la légalité et si, d'autre part, eu égard aux différents éléments contenus dans la disposition attaquée, toute personne soumise à l'obligation de détention d'une carte d'identité peut savoir de manière suffisamment précise dans quelles conditions le prélèvement de ses empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité ont lieu, le cas échéant, selon des modalités déterminées par le Roi. Ces deux questions étant intrinsèquement liées, la Cour les examine conjointement.

B.23.1. Comme il est dit en B.1.3, la disposition attaquée détermine les données qui font l'objet de la mesure litigieuse, à savoir l'image numérisée de deux empreintes digitales, la durée maximale de conservation de cette information pour les besoins de la fabrication et de la délivrance de la carte d'identité, le fait que les données sont uniquement stockées sur la carte d'identité et qu'elles sont lisibles exclusivement de manière électronique, ainsi que les instances habilitées à les lire.

Contrairement à ce que soutiennent les parties requérantes, il ressort clairement du libellé de la disposition attaquée que l'image numérisée des empreintes digitales sur la carte d'identité n'est lisible que sous forme électronique, et non à l'œil nu, et que cette information doit être détruite définitivement au terme de la période nécessaire à la fabrication et à la délivrance de la carte d'identité, qui peut atteindre trois mois maximum, sans possibilité de récupération ultérieure des données.

Le législateur a également limité la délégation conférée au Roi à la détermination, d'une part, des conditions et des modalités entourant la capture de l'image numérisée des empreintes digitales et, d'autre part, de la forme et des modalités de fabrication, de délivrance et d'utilisation de la carte d'identité. La mise en œuvre de ces délégations doit avoir lieu après avis de l'Autorité de protection des données et, dans le premier cas, par arrêté délibéré en Conseil des ministres.

B.23.2. Il découle de ce qui précède que le législateur a déterminé les éléments essentiels des mesures dont il délègue l'exécution au Roi et que, partant, ces délégations ne sont pas contraires au principe de la légalité contenu dans l'article 22 de la Constitution.

Comme le soutient le Conseil des ministres, les éléments qui, selon les parties requérantes, auraient dû être réglés par le législateur lui-même, à savoir le type de puce utilisée, les mesures techniques de sécurisation et de lecture et les modalités concrètes de suppression des données, au moment de la délivrance de la carte d'identité, concernent des aspects d'exécution ou des aspects purement techniques qui, à ce titre, peuvent être réglés par le Roi, dans le respect des normes supérieures et, notamment, du règlement (UE) 2019/1157 et des décisions prises en exécution de celui-ci, ainsi que du RGPD.

Le cas échéant, il appartient au juge compétent d'examiner si l'utilisation, faite par le Roi, des délégations précitées est conforme aux dispositions constitutionnelles, conventionnelles et du droit de l'Union citées dans les moyens, telles qu'elles ont été précisées en B.13 à B.16.

Enfin, il n'apparaît pas que, pour respecter le principe de légalité, le législateur aurait dû instituer une sanction spécifique en cas de violation des règles fixées par la disposition attaquée, eu égard aux sanctions qui sont déjà prévues, notamment par l'article 7 de la loi du 19 juillet 1991, combiné avec l'article 6*quater* de la même loi.

B.24. Les personnes soumises à l'obligation de détention d'une carte d'identité peuvent par ailleurs connaître de manière suffisamment précise les conditions dans lesquelles le

prélèvement des empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité ont lieu, le cas échéant, selon les modalités déterminées par le Roi.

B.25.1. La Cour examine maintenant la nécessité et la proportionnalité de l'ingérence.

B.25.2. 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).

B.25.3. 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.26.1. Les parties requérantes font valoir que les cartes d'identité ne sont pas comparables aux passeports, de sorte que l'arrêt *Schwarz c. Stadt Bochum* du 17 octobre 2013, précité, de la Cour de justice de l'Union européenne ne pourrait pas s'appliquer par analogie. Selon elles, les cartes d'identité et les passeports sont des documents intrinsèquement différents. L'appréciation de la nécessité et de la proportionnalité de l'ingérence devrait dès lors être effectuée à l'aune de critères différents.

B.26.2. Dans son avis à propos de la proposition de règlement devenue le règlement (UE) 2019/1157, le Contrôleur européen de la protection des données (CEPD) a émis les observations suivantes :

« 22. À cet égard, le CEPD soutient l'objectif de la Commission visant à faciliter la libre circulation. Néanmoins, le CEPD fait observer que les deux types de documents – cartes d'identité et passeports – sont en fait très différents, tant du point de vue juridique qu'au niveau de leur utilisation pratique. Même lorsqu'elles sont utilisées en tant que documents de voyage dans le cadre de la libre circulation, les cartes d'identité nationales, contrairement aux passeports, ne peuvent l'être que pour se rendre dans des États membres de l'Union et les pays tiers concernés, ce qui permet aux citoyens de l'Union de voyager grâce à leurs cartes d'identité nationales. Dans ce contexte, le CEPD met en doute la valeur ajoutée de l'intégration des données biométriques dans les cartes d'identité, étant donné qu'elles ne sont pas systématiquement contrôlées lors des voyages entre États membres de l'Union.

23. Plus important encore, les cartes d'identité font l'objet de diverses utilisations qui vont bien au-delà de l'exercice du droit à la libre circulation lié à la citoyenneté de l'Union, depuis les démarches auprès des administrations du pays d'origine du citoyen jusqu'aux relations avec différents acteurs du secteur privé (banques, compagnies aériennes, etc.). En outre, selon l'analyse d'impact accompagnant la proposition, environ 15 millions de citoyens de l'Union résident dans un autre État membre, et 11 millions travaillent dans un autre État membre. Le CEPD en conclut que, pour la grande majorité des citoyens de l'Union, les fonctions principales d'une carte d'identité ne sont pas directement associées à la libre circulation. On ne peut présumer que tous les citoyens de l'Union potentiellement concernés par l'obligation d'inclure leurs empreintes digitales dans leur carte d'identité nationale, introduite par la proposition, exercent effectivement leurs droits en matière de libre circulation, loin de là. Les citoyens mobiles de l'Union constituent au contraire une petite minorité de ceux qui sont potentiellement concernés par la proposition. En outre, même ceux qui exercent concrètement leur droit à la libre circulation peuvent le faire, et le font souvent, sur la base d'un passeport, et non d'une carte d'identité. La justification de la proposition avancée par la Commission n'est donc pas totalement convaincante » (avis 7/2018 du CEPD sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents, 10 août 2018, p. 11).

L'Autorité de protection des données a émis des observations analogues :

« 25. L'assimilation des cartes d'identité avec les passeports qui est avancée par le gouvernement pour justifier cette mesure n'est pas acceptable : même si les cartes d'identité peuvent aussi être utilisées comme titre de voyage dans l'Union européenne, elles ne font actuellement pas l'objet de contrôle systématique pour ces voyages vu le principe de liberté de circulation au sein de l'Union européenne. De plus, contrairement aux passeports, les cartes d'identité nationale offrent beaucoup d'autres utilisations (applications du secteur privé, …). Ce point a également été relevé par le CEPD dans son avis. Compte tenu des différences entre les cartes d'identité et les passeports, l'introduction dans les cartes d'identité d'éléments de sécurité pouvant être considérés comme appropriés dans le cas des passeports ne peut être automatique, mais exige une réflexion et une analyse approfondie qui ne semble pas avoir été réalisée » (avis n° 106/2018 du 17 octobre 2018, *Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 120).

B.26.3. Les travaux préparatoires de la disposition attaquée mentionnent que les cartes d'identité sont aujourd'hui utilisées comme documents de voyage :

« En effet, en ce qui concerne les passeports, ainsi que le rappelle la Commission, une réglementation européenne spécifique impose aux États membres de collecter les empreintes digitales.

Or, les cartes d'identité électroniques constituent elles aussi un document de voyage » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3256/001, p. 34).

C'est d'ailleurs parce que « la liberté de circulation implique le droit de sortir d'un État membre ou d'y entrer avec une carte d'identité ou un passeport en cours de validité » que le législateur européen a adopté le règlement (UE) 2019/1157, qui instaure des normes minimales en matière de sécurité et de format pour les cartes d'identité, en vue de « renforcer la sécurité pour faciliter l'exercice des droits à la libre circulation par les citoyens de l'Union et les membres de leur famille » (voy. les considérants 2 et 46 de ce règlement).

En réponse aux observations de l'Autorité de protection des données, le ministre de la Sécurité et de l'Intérieur a fourni les explications suivantes en commission de la Chambre :

« Dans le point 25 de son avis, l'APD conteste l'assimilation opérée entre le passeport et la carte d'identité électronique en tant que document de voyage. Le ministre observe à ce sujet que les premières e-gates équipées de lecteur d'empreintes digitales sont déjà en cours d'utilisation en Europe. Vu la législation européenne, elles seront de plus en plus utilisées. Si l'on souhaite encore utiliser la carte eID comme document de voyage, il faudra également s'y adapter. Pour rappel, la carte eID est reconnue dans une cinquantaine de pays, même hors

Europe. Le fait que la carte eID comporte encore d'autres fonctions est pertinent. Comme titre de voyage, la carte eID doit satisfaire aux mêmes normes. En effet, ce n'est pas parce que la libre circulation est en vigueur au sein de l'Union européenne que les autorités des autres États membres ou des citoyens ne peuvent pas demander la carte eID. Dans d'autres États membres, il peut également être demandé à une personne de prouver son identité au moyen de sa carte eID.

Lors d'un contrôle d'identité, il est essentiel de pouvoir en apporter la preuve rapidement et efficacement. Comme [le ministre] l'a expliqué plus haut, la photo seule ne suffit pas alors que la vérification des empreintes digitales enregistrées sur la carte offre bien ces garanties » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 34).

B.26.4. Bien que les cartes d'identité et les passeports soient des documents de nature différente, qui sont généralement destinés à des usages distincts, il y a lieu de constater que les cartes d'identité sont aujourd'hui fréquemment utilisées comme documents de voyage au sein de l'Union européenne, ainsi que dans le cadre de voyages vers un nombre limité d'États tiers, et qu'elles sont, à ce titre, susceptibles de faire l'objet de contrôles. Les cartes d'identité peuvent également servir de documents « sources » pour l'obtention d'un passeport.

B.26.5. Une analogie entre les passeports et les cartes d'identité est donc permise. Toutefois, il peut être admis, avec le CEPD et avec l'Autorité de protection des données, que le test de nécessité et de proportionnalité doit être plus strict pour les cartes d'identité que pour les passeports, compte tenu notamment de l'importance des premières dans les actes de la vie quotidienne et du caractère obligatoire de leur détention, comme il est dit en B.5.5. Il incombe donc à la Cour de vérifier si, en l'espèce, le législateur a pris une mesure qui est nécessaire et proportionnée à l'objectif poursuivi. Dans le cadre de cet examen, la Cour tient compte de l'arrêt *Schwarz c. Stadt Bochum*, précité, de la Cour de justice.

B.27.1. L'avis n° 19/2018 du 28 février 2018 de l'Autorité de protection des données (anciennement Commission de la protection de la vie privée) mentionne :

« 69. En l'absence de justification étayée et chiffrée sur des cas avérés de fraudes liés à l'insuffisance des moyens de non falsification dont est dotée notre actuelle carte d'identité susceptible d'attester du caractère éventuellement insuffisant de la photo comme moyen d'authentification du porteur de la carte et en l'absence de justification conforme aux exigences de l'article 9.2.g, la mesure apparait disproportionnée aux yeux de la Commission et non conforme au RGPD » (avis n° 19/2018 du 28 février 2018, *Doc. parl.*, Chambre, 2017-2018, DOC 54-3256/001, p. 220).

Son avis n° 106/2018 du 17 octobre 2018 mentionne également :

« 23. Il n'y a toujours pas de réelle justification de la mesure envisagée dans l'exposé des motifs alors que cela a été demandé par l'Autorité de protection des données. Notre carte d'identité est déjà dotée de dispositifs de lutte contre la falsification (hologramme, …) ainsi que d'un élément biométrique (l'image faciale). En quoi concrètement est-ce insuffisant ? Quelles sont les statistiques dont disposent le gouvernement qui étayent la mesure envisagée ?

24. Dans son avis précité, le contrôleur européen à la protection des données (CEPD) a relevé que les statistiques ne plaident pas en faveur de la proposition de la Commission européenne qui va dans le même sens de celle du gouvernement. Des statistiques de l'agence européenne des gardes-frontières (frontex) ne révèlent qu'un constat de 38.870 cas d'utilisation frauduleuse de cartes d'identité nationale pour la période 2013-2017. De plus, on constate une baisse d'utilisation de titre de séjour frauduleux de personnes en provenance des pays tiers depuis 2015 de l'ordre d'au moins 11 %.

25. L'assimilation des cartes d'identité avec les passeports qui est avancée par le gouvernement pour justifier cette mesure n'est pas acceptable : même si les cartes d'identité peuvent aussi être utilisées comme titre de voyage dans l'Union européenne, elles ne font actuellement pas l'objet de contrôle systématique pour ces voyages vu le principe de liberté de circulation au sein de l'Union européenne. De plus, contrairement aux passeports, les cartes d'identité nationale offrent beaucoup d'autres utilisations (applications du secteur privé, …). Ce point a également été relevé par le CEPD dans son avis. Compte tenu des différences entre les cartes d'identité et les passeports, l'introduction dans les cartes d'identité d'éléments de sécurité pouvant être considérés comme appropriés dans le cas des passeports ne peut être automatique, mais exige une réflexion et une analyse approfondie qui ne semble pas avoir été réalisée.

[…]

27. L'interdiction de traitement des données biométriques ne peut être levée que sur base de l'article 9.2.g du RGPD qui exige non seulement le motif d'intérêt public important mais également notamment le caractère proportionné de la mesure face à l'objectif poursuivi et l'adoption de mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts des personnes concernées. Elles sont actuellement insuffisantes :

a. Le choix du gouvernement de collecter et stocker dans la puce de la carte l'image numérisée des empreintes digitales ne constitue selon le CEPD pas un choix des plus opportun au vu du risque d'usurpation d'identité en cas de hacking des données figurant sur la puce électronique de la carte. Il convient de revoir ce choix et de limiter les données dactyloscopiques stockées dans la puce des cartes d'identité à un sous-ensemble de caractéristiques extrait de l'image de l'empreinte digitale ou encore à des techniques biométriques sans trace (contour de la main, réseau veineux d'un doigt…).

b. Au lieu de déléguer au Roi la tâche de déterminer les autorités qui seront habilitées à lire les empreintes digitales, c'est au législateur au sens formel du terme qu'il appartient de le faire.

c. Il convient également que la loi précise que la lecture de ces données ne pourra se faire que pour vérifier l'authenticité de la carte d'identité. Il convient de prévoir déjà dans la loi des mesures de limitation pour les lecteurs de cartes qui permettront de lire les empreintes digitales.

d. Quelles seront les mesures de protection spécifiques qui seront prises pour limiter au maximum le risque de hacking du certificat de la carte d'identité qui contiendra l'image des empreintes digitales que ce soit tant en terme de sécurisation de la puce dans laquelle ces données seront insérées que de sécurisation des lecteurs de ces données ?

e. Quelles sont les mesures de protection pour la base de données temporaire qui reprendra de manière centralisée les empreintes digitales pendant 3 mois et quel en sera le responsable de traitement ?

f. Enfin, comme relevé par le CEPD, des enfants de moins de 14 ans ne devraient pas être soumis à cette mesure » (avis n° 106/2018 du 17 octobre 2018, *Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, pp. 119-121).

B.27.2. En réponse à ces avis défavorables, le ministre de la Sécurité et de l'Intérieur a apporté les explications suivantes, en commission de la Chambre :

« Dans le point 24 de l'avis, l'APD [Autorité de protection des données] déclare ceci : ' on constate une baisse d'utilisation de titre de séjour frauduleux de personnes en provenance des pays tiers depuis 2015 de l'ordre d'au moins 11 % '. Le ministre rappelle à ce sujet que les empreintes digitales sur les cartes d'étranger n'ont commencé à être enregistrées qu'à partir de 2013, la généralisation s'est essentiellement déroulée début 2014. Dès lors, l'APD ne fait que confirmer que la mesure relative à l'intégration des empreintes digitales sur les cartes est efficace. Lors d'un contrôle des empreintes digitales sur la carte, les fraudeurs qui ont pour mode opératoire le ' lookalike ' tombent inéluctablement dans les mailles du filet.

Selon l'APD, ' des statistiques de l'agence européenne des gardes-frontières (frontex) ne révèlent qu'un constat de 38 870 cas d'utilisation frauduleuse de cartes d'identité nationale pour la période 2013-2017 '. Le ministre estime que ce nombre ne doit pas être sous-estimé. Ce sont en effet 38 870 personnes qui ont essayé d'entrer en Europe sous une fausse identité.

Or, la fraude à l'identité est la plupart du temps associée à un autre délit (trafic d'êtres humains, fraude, criminels souhaitant rester sous le radar, personnes parties combattre en Syrie qui essaient d'entrer clandestinement en Europe, terroristes potentiels, etc.). Il ne s'agit par ailleurs que des cas qui ont été découverts. Si, tout comme pour les passeports et les cartes d'étranger, il est possible de faire une vérification au moyen des empreintes digitales, ces chiffres augmenteront sans nul doute.

[…]

Le ministre réagit ensuite aux observations formulées par l'APD dans le point 27 de son avis.

a) La procédure pour les empreintes digitales est exactement la même que pour les passeports et les titres de séjour pour les ressortissants de pays tiers. Dès lors, la remarque de l'APD ne manque pas d'étonner puisqu'elle impliquerait qu'un problème existe depuis fin 2012, moment où les premiers passeports biométriques ont commencé à être délivrés dans les communes. Pourtant, le ministre n'a eu connaissance d'aucun piratage de la puce. La puce répond aux normes de sécurité les plus élevées et n'est accessible que de manière limitée (inspection des frontières, police). Il se demande dès lors sur quelles informations concrètes se fonde cette remarque.

b) L'APD estime qu'il appartient au législateur de désigner les autorités habilitées à lire les empreintes digitales. Cette proposition peut être suivie.

Actuellement, [le] projet de loi prévoit qu'il appartiendra au Roi, par un arrêté délibéré en Conseil des ministres et après avis de l'APD, de procéder à cette désignation.

[…]

c) Seuls les lecteurs de cartes habilités pourront lire les empreintes digitales. Dans la pratique, il s'agira des communes, des consulats et de la police. Cela sera confirmé lorsque le projet de loi sera adapté comme annoncé au point b).

d) L'APD se demande à quelles normes de sécurité devra répondre la puce se trouvant sur la carte eID afin d'éviter le piratage de la puce et le vol des empreintes digitales. On utilise la même norme internationale que pour les passeports et les titres de séjour pour les ressortissants de pays tiers. Les mêmes normes sont également d'application en ce qui concerne la base de données dans laquelle les empreintes digitales sont provisoirement enregistrées. Cette base de données a un accès limité avec habilitations personnelles pour les personnes autorisées. Cet accès se fait via des connexions sécurisées et il y a une journalisation de l'utilisation de celle-ci ainsi que des personnes qui l'utilisent.

e) Enfin, l'APD propose que les empreintes digitales ne soient collectées qu'à partir de l'âge de 14 ans. Cela serait toutefois discriminatoire par rapport aux ressortissants de pays tiers pour lesquels on doit enregistrer les empreintes digitales sur les cartes d'étranger dès l'âge de 12 ans » (*Doc. parl*., Chambre, 2018-2019, DOC 54-3256/003, pp. 33-36).

Il a également été précisé :

« Les empreintes digitales seront protégées par un certificat permettant une lecture uniquement par des lecteurs autorisés » (*Doc. parl*., Chambre, 2017-2018, DOC 54-3256/001, p. 35).

B.28. Tout d'abord, il ne peut être déduit des chiffres reproduits dans les travaux préparatoires de la disposition attaquée, cités en B.20.1, que le phénomène de la fraude à la ressemblance et de l'obtention frauduleuse de documents authentiques, que la disposition attaquée vise à combattre, serait purement marginal, que ce soit au niveau belge ou au niveau de l'Union européenne. Ainsi qu'il ressort des travaux préparatoires, si les chiffres relatifs à la fraude documentaire ont diminué au cours de la période récente, il en va différemment des chiffres relatifs à la fraude à la ressemblance, ces chiffres visant par ailleurs uniquement les fraudes détectées (voy. notamment en ce sens, *Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 33).

B.29. En ce qui concerne le caractère proportionné de la disposition attaquée, il n'apparaît pas - et les parties requérantes ne le prétendent pas - que la disposition attaquée affecterait le contenu essentiel du droit au respect de la vie privée et du droit à la protection des données à caractère personnel.

B.30. Comme l'a constaté la Cour de justice en matière de passeports dans l'arrêt *Schwarz c. Stadt Bochum,* précité, à propos du règlement (CE) n° 2252/2004, « le prélèvement ne consiste qu'à prendre l'empreinte de deux doigts. Ceux-ci sont d'ailleurs normalement exposés à la vue des autres, de sorte qu'il ne s'agit pas d'une opération revêtant un caractère intime. Celle-ci n'entraîne pas non plus un désagrément physique ou psychique particulier pour l'intéressé, à l'instar de la prise de sa photo faciale » (point 48; voy. aussi CJUE, 3 octobre 2019, C-70/18, *Staatssecretaris van Justitie en Veiligheid c. A, B et C,* point 58).

B.31.1. La disposition attaquée n'établit pas un registre central des empreintes digitales de l'ensemble des détenteurs d'une carte d'identité. Sous réserve de la conservation de l'image numérisée des empreintes digitales pour les besoins de la fabrication et de la délivrance de la carte d'identité, pendant une durée maximale de trois mois, la disposition attaquée se limite à intégrer l'image numérisée de deux empreintes digitales sur la carte d'identité et sur ce seul support, comme le confirment les travaux préparatoires (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 16).

Contrairement à ce que soutiennent les parties requérantes, la disposition attaquée, en visant à lutter contre la fraude à la ressemblance, n'a donc pas pour objet ni pour effet de « précriminaliser » l'ensemble des détenteurs d'une carte d'identité.

B.31.2. L'appréciation du législateur concernant la nécessité de la disposition attaquée n'est donc pas déraisonnable.

B.32.1. Comme il est dit en B.23.2, il appartient au Roi, dans l'exécution des délégations qui lui ont été conférées, de prendre les mesures techniques et organisationnelles adéquates en vue de la sécurisation des données, dans le respect, notamment, des dispositions pertinentes du RGPD et du règlement (UE) 2019/1157.

Il appartient au juge compétent, le cas échéant, de vérifier si ces mesures constituent des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée, au sens de l'article 9, paragraphe 2, point g), du RGPD.

B.32.2. Sous réserve de la mise en œuvre par le Roi de ces habilitations, le risque d'abus dénoncé par les parties requérantes n'est pas suffisamment caractérisé.

S'il est exact que le vol des données relatives aux empreintes digitales est susceptible d'entraîner de graves inconvénients pour la personne concernée, dont l'identité pourrait être usurpée, il reste que ce risque peut être significativement circonscrit par la durée de conservation limitée des données, pour les besoins de la fabrication et de la délivrance de la carte d'identité, ainsi que par les mesures techniques de sécurisation qu'il appartient au Roi de prendre. Par ailleurs, comme l'observait le ministre de la Sécurité et de l'Intérieur en commission de la Chambre, « pour celui qui souhaite ' voler ' les empreintes d'un individu, il est plus facile de prendre un objet sur lequel cet individu a déposé ses empreintes que d'essayer de s'emparer de celles qui figureront sur la carte d'identité » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 61).

B.33. Enfin, conformément à l'article 6*quater* de la loi du 19 juillet 1991, « toutes les personnes qui, dans l'exercice de leurs fonctions, interviennent dans la collecte, le traitement ou la transmission des informations sont tenues au secret professionnel » (alinéa 1er). Ces mêmes personnes « doivent prendre toute précaution utile afin d'assurer la sécurité des informations enregistrées et, en particulier, d'empêcher qu'elles soient déformées, endommagées ou communiquées à des personnes qui n'ont pas obtenu l'autorisation d'en prendre connaissance » (alinéa 2). Le non-respect de ces obligations est pénalement

sanctionné, conformément à l'article 7 de la loi du 19 juillet 1991. Par ailleurs, les articles 461, 550*bis* et 550*ter* du Code pénal incriminent respectivement le vol, l'accès non autorisé à un système informatique et la modification non autorisée apportée à un tel système.

B.34. La disposition attaquée n'entraîne donc pas d'effets disproportionnés pour les personnes concernées, eu égard aux objectifs poursuivis.

B.35. En ce qu'elle prévoit le prélèvement de deux empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité, la disposition attaquée ne viole pas le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, tels qu'ils sont garantis par les dispositions citées dans les moyens.

Pour le surplus, les parties requérantes ne démontrent pas concrètement en quoi la disposition attaquée violerait les articles 1er à 4, 25 et 32 du RGPD.

B.36. En ce qu'ils portent sur le prélèvement de deux empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité, les griefs ne sont pas fondés.

*2. La conservation centralisée de l'image numérisée des empreintes digitales pour les besoins de la fabrication et de la délivrance de la carte d'identité*

B.37. Les parties requérantes critiquent la conservation centralisée de l'image numérisée des empreintes digitales pour les besoins de la fabrication et de la délivrance de la carte d'identité, pendant une durée maximale de trois mois. Elles soutiennent qu'une telle mesure n'est pas nécessaire dès lors qu'il serait techniquement possible d'intégrer directement l'information dans la puce au moment du retrait de la carte d'identité par son titulaire. Elles critiquent par ailleurs l'absence de mesures techniques adéquates afin de garantir l'intégrité et la confidentialité des données ainsi conservées.

B.38.1. Il ressort des travaux préparatoires que, pour les besoins de la fabrication et de la délivrance de la carte d'identité, l'image numérisée des empreintes digitales est conservée temporairement dans une banque de données centralisée :

« Les empreintes digitales ne seront en aucune façon stockées ni centralisées, si ce n'est durant la période nécessaire à la fabrication et à la délivrance de la carte d'identité, à l'instar de toutes autres données figurant sur la carte, et en tout état de cause durant maximum 3 mois. Aussi longtemps que la carte n'est pas délivrée au citoyen, il se peut qu'elle soit détruite, défectueuse,…, et dans ce cas, une nouvelle carte serait fabriquée, sans que le citoyen ne doive se présenter à nouveau auprès de son administration communale. Après ce délai, la loi en projet spécifie que ces données doivent impérativement être détruites et effacées de la banque de données » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3256/001, p. 34).

En commission de la Chambre, le ministre de la Sécurité et de l'Intérieur a expliqué que le délai maximal de conservation des données de trois mois se justifie par des obligations techniques et que les empreintes digitales sont effacées aussitôt que la carte d'identité est délivrée :

« En ce qui concerne les empreintes digitales, [le membre] estime que le délai maximal de trois mois pour la fabrication de la carte d'identité est trop long.

Il s'agit en l'occurrence d'obligations techniques. Le délai est d'ailleurs identique à celui des passeports et des cartes d'étranger. Il n'y a donc rien de nouveau sous le soleil. En outre, il est explicitement indiqué que les empreintes digitales ne peuvent être conservées qu'aussi longtemps que nécessaire pour la fabrication, avec un maximum de trois mois. Cela signifie que dès que la carte a été délivrée au citoyen, généralement dans un délai de 1 à 2 semaines, les empreintes digitales sont effacées immédiatement » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 48).

B.38.2. Avec le Conseil des ministres, il peut être admis que la centralisation des empreintes digitales, pour les besoins de la fabrication et de la délivrance de la carte d'identité, est justifiée pour des motifs de sécurité et d'intégrité des données. La centralisation des données, au lieu de leur intégration sur la puce de la carte d'identité lors de la délivrance de celle-ci, offre davantage de garanties en ce qui concerne leur sécurité et leur intégrité. Le risque d'abus serait en effet plus élevé s'il était possible d'intégrer les empreintes digitales sur une carte d'identité au sein de chaque administration communale du pays.

À cet égard, la conservation de l'image numérisée des empreintes digitales « durant le temps nécessaire à la fabrication et à la délivrance de la carte d'identité et, en tout cas, durant une période de maximum 3 mois » n'est pas manifestement excessive par rapport à l'objectif poursuivi, à savoir la fabrication et la délivrance de la carte d'identité. La disposition attaquée

prévoit explicitement l'obligation de détruire et d'effacer les données à l'issue de cette période, ce qui suppose une suppression définitive de celles-ci, comme il est dit en B.23.1.

Pour le surplus, il appartient au Roi de prendre les mesures techniques et organisationnelles adéquates en vue de garantir l'intégrité et la confidentialité des données ainsi conservées, en exécution des délégations qui lui ont été conférées, comme il est dit en B.23.2.

B.38.3. Les critiques que, dans son mémoire en réponse, la partie requérante dans l'affaire n° 7202 dirige contre l'article 10, paragraphe 3, du règlement (UE) 2019/1157, en ce qu'il permet la conservation des données, d'une part, jusqu'à 90 jours après délivrance du document d'identité et, d'autre part, au-delà de 90 jours pour d'autres buts que ceux qui sont prévus par le règlement, ne sont pas pertinentes en l'espèce, dès lors que la disposition attaquée ne prévoit la conservation des données « que durant le temps nécessaire à la fabrication et à la délivrance de la carte d'identité » et, en tout cas, pour une durée maximale de trois mois, à compter du prélèvement de l'image numérisée des empreintes digitales et non de la délivrance de la carte d'identité.

L'affirmation de cette même partie requérante selon laquelle le règlement (UE) 2019/1157, lu en combinaison avec la décision d'exécution C(2018) 7767 de la Commission européenne du 30 novembre 2018 « établissant les spécifications techniques du modèle uniforme de titre de séjour destiné aux ressortissants de pays tiers, et abrogeant la décision C(2002) 3069 », ne contiendrait pas les mesures techniques et organisationnelles adéquates en vue d'assurer la sécurité des empreintes digitales conservées, n'est pas étayée. Compte tenu de ce qui est dit en B.38.2, cette critique n'est en tout état de cause pas pertinente en l'espèce.

B.39. Les griefs cités en B.37 ne sont donc pas fondés. Compte tenu de ce qui est dit en B.38.3, il n'y a pas lieu de poser à la Cour de justice la question préjudicielle suggérée par la partie requérante dans l'affaire n° 7202 sur la validité de l'article 10, paragraphe 3, du règlement (UE) 2019/1157.

*3. La lecture de l'image numérisée des empreintes digitales par les instances habilitées à cet effet*

B.40. Les parties requérantes formulent plusieurs griefs contre la disposition attaquée en ce qui concerne la lecture de l'image numérisée des empreintes digitales par les instances habilitées à cet effet.

B.41.1. Les parties requérantes font grief à la disposition attaquée de ne pas déterminer la technique ou la méthode par laquelle l'empreinte digitale est enregistrée et lue et de ne pas interdire l'enregistrement des données à cette occasion. Elles lui reprochent également de ne pas préciser si les habilitations doivent être assorties de mesures techniques.

B.41.2. La détermination des modalités concrètes de lecture de l'image numérisée des empreintes digitales relève de l'exécution de la loi. Pour les mêmes motifs que ceux qui sont mentionnés en B.23.2, c'est au Roi qu'il appartient de prendre les mesures techniques adéquates à cet effet, dans le respect des dispositions pertinentes du RGPD et du règlement (UE) 2019/1157, sous le contrôle du juge compétent.

À ce sujet, il a été précisé dans les travaux préparatoires :

« Les empreintes digitales seront protégées par un certificat permettant une lecture uniquement par des lecteurs autorisés » (*Doc. parl*., Chambre, 2017-2018, DOC 54-3256/001, p. 35 ; voy. aussi *Doc. parl*., Chambre, 2018-2019, DOC 54-3256/003, p. 36).

L'article 6*quater*, alinéa 2, de la loi du 19 juillet 1991 prévoit par ailleurs explicitement l'obligation pour « toutes les personnes qui, dans l'exercice de leurs fonctions, interviennent dans la collecte, le traitement ou la transmission des informations » de « prendre toute précaution utile afin d'assurer la sécurité des informations enregistrées et, en particulier, d'empêcher qu'elles soient déformées, endommagées ou communiquées à des personnes qui n'ont pas obtenu l'autorisation d'en prendre connaissance ».

B.41.3. La disposition attaquée habilite plusieurs instances à lire l'image numérisée des empreintes digitales. Cette habilitation ne vaut que pour la lecture. Aussi, la disposition attaquée doit être interprétée comme ne permettant pas l'enregistrement des données lors de la lecture de celles-ci. Les travaux préparatoires indiquent ainsi que « les empreintes digitales ne seront en aucune façon stockées ni centralisées, si ce n'est durant la période nécessaire à la fabrication et à la délivrance de la carte d'identité » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3256/001, p. 34 et *Doc. parl.*, Chambre, 2018-2019, DOC 54-3256/003, p. 16).

B.41.4. Sous réserve de l'interprétation mentionnée en B.41.3, le grief cité en B.41.1 n'est pas fondé.

B.42.1. Les parties requérantes reprochent à la disposition attaquée de ne pas préciser en quoi consiste la lecture de l'image numérisée des empreintes digitales. Elles soutiennent que la disposition attaquée confère une habilitation trop large aux autorités concernées en ce qui concerne l'accès aux données et leur utilisation ultérieure. Ainsi, la disposition attaquée n'indique pas le but de la lecture des empreintes digitales par les agents chargés du contrôle des frontières - l'habilitation valant également pour le personnel étranger qui peut, le cas échéant, être une firme privée - et le traitement des empreintes digitales par la police dans le cadre d'entraves aux missions de police administrative n'est pas limité à des motifs d'intérêt public important.

B.42.2.1 La finalité de la lecture de l'image numérisée des empreintes digitales par les instances qui y sont habilitées découle logiquement de l'objet de la mesure ainsi que des missions que ces instances assument, telles que ces missions sont visées par la disposition attaquée.

B.42.2.2. En ce qui concerne le personnel chargé du contrôle aux frontières, tant en Belgique qu'à l'étranger, la disposition attaquée doit être raisonnablement interprétée comme n'autorisant la lecture que dans le cadre du contrôle aux frontières et à cette seule fin.

Le fait que le personnel à l'étranger soit habilité à lire l'image numérisée des empreintes digitales résulte de la nécessité de vérifier l'identité des personnes non seulement aux frontières belges, mais aussi aux frontières intérieures, entre États membres, et extérieures de l'Union

européenne. En vertu de l'article 11, paragraphe 6, du règlement (UE) 2019/1157, les empreintes digitales ne peuvent être lues « que par le personnel dûment autorisé des autorités nationales compétentes et des agences de l'Union […] ».

B.42.2.3. En ce qui concerne les services de police, ceux-ci ne peuvent lire l'image numérisée des empreintes digitales que « pour autant que cela s'avère nécessaire pour l'accomplissement de leurs missions légales de police administrative et judiciaire dans le cadre de la lutte contre la fraude, notamment la lutte contre la traite et le trafic des êtres humains, l'escroquerie et l'abus de confiance, le blanchiment d'argent, le terrorisme, le faux et usage de faux, l'usurpation de nom et l'usage de faux nom, les violations de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et les entraves aux missions de police administrative ».

Cette habilitation des services de police est suffisamment délimitée et repose sur des motifs d'intérêt public important, au sens de l'article 9, paragraphe 2, point g), du RGPD.

B.42.2.4. Les intéressés peuvent donc connaître de manière suffisamment précise les finalités de la lecture de l'image numérisée de leurs empreintes digitales sur la carte d'identité.

B.42.2.5. Enfin, comme il est dit en B.41.3, l'habilitation ne vaut que pour la lecture de l'image numérisée des empreintes digitales et ne permet donc pas l'enregistrement des données, ce qui exclut toute utilisation ultérieure de celles-ci.

B.42.3. Sous réserve de l'interprétation mentionnée en B.42.2.2, le grief cité en B.42.1 n'est pas fondé.

B.43.1. Les parties requérantes critiquent le fait que la disposition attaquée permet aux instances énumérées à l'article 6, § 2, alinéa 6, de la loi du 19 juillet 1991 de lire l'image numérisée des empreintes digitales non seulement sur la carte d'identité, une fois celle-ci délivrée à son titulaire, mais aussi lors de la phase de fabrication, en pouvant accéder à la banque de données centralisée qui conserve temporairement les informations.

B.43.2. Certes, en ce qui concerne l'habilitation à lire l'image numérisée des empreintes digitales, la disposition attaquée ne fait pas de distinction entre, d'une part, la phase de fabrication et de délivrance de la carte d'identité et, d'autre part, la phase qui suit la délivrance de la carte d'identité à son titulaire.

Cependant, comme le soutient le Conseil des ministres, les différentes instances habilitées à lire l'image numérisée des empreintes digitales le sont dans le cadre de l'exercice de leurs fonctions, telles que celles-ci sont légalement décrites.

Il s'en déduit que, pendant la phase de fabrication et de délivrance de la carte d'identité, la disposition attaquée doit être raisonnablement interprétée comme ne permettant la consultation de l'image numérisée des empreintes digitales qu'aux seules fins de la fabrication et de la délivrance de la carte d'identité.

Il ressort à cet égard des travaux préparatoires que l'accès à la base de données dans laquelle les empreintes digitales sont provisoirement enregistrées est limité :

« Cette base de données a un accès limité avec habilitations personnelles pour les personnes autorisées. Cet accès se fait via des connexions sécurisées et il y a une journalisation de l'utilisation de celle-ci ainsi que des personnes qui l'utilisent » (*Doc. parl*., Chambre, 2018-2019, DOC 54-3256/003, p. 36).

Dans cette interprétation, la disposition attaquée ne permet donc pas aux services de police et au personnel chargé du contrôle aux frontières de consulter les empreintes digitales lors de la phase de fabrication et de délivrance de la carte d'identité.

B.43.3. Sous réserve de l'interprétation mentionnée en B.43.2, le grief cité en B.43.1 n'est pas fondé.

B.44.1. Les parties requérantes font grief à la disposition attaquée de permettre la lecture des empreintes digitales sur la carte d'identité à grande échelle, sans contact et secrètement, notamment par les services de police, et de permettre le croisement de ces données avec

d'autres informations en vue d'identifier un individu. La disposition attaquée ne prévoit pas non plus que la lecture ne peut avoir lieu qu'à titre subsidiaire et qu'elle est limitée à des fins de vérification de l'authenticité de la carte d'identité et de l'identité du titulaire.

B.44.2. Les instances habilitées à lire les empreintes digitales le sont uniquement dans le cadre de l'exercice de leurs fonctions, telles que celles-ci sont légalement décrites.

Il leur appartient de mettre en œuvre cette habilitation dans le respect des principes applicables en matière de protection des données à caractère personnel. Conformément à l'article 9, paragraphe 2, point g), du RGPD, il ne peut être procédé au traitement de données à caractère personnel sensibles que si ce traitement est nécessaire et proportionné aux motifs d'intérêt public important poursuivis, ce qui implique que la vérification des empreintes digitales ne doit intervenir qu'après vérification en priorité de l'image faciale et que si elle est « nécessaire pour confirmer sans aucun doute l'authenticité du document et l'identité du titulaire », ainsi que le préconise le considérant 19 du règlement (UE) 2019/1157.

La mise en œuvre de ces obligations relève de l'application de la loi, pour laquelle la Cour n'est pas compétente.

Pour le surplus, les parties requérantes n'expliquent pas en quoi, dans le cadre de l'exercice de leurs fonctions, les services de police pourraient lire l'image numérisée des empreintes digitales à d'autres fins que la vérification de l'authenticité de la carte d'identité ou de l'identité du titulaire.

B.44.3. Le croisement des données afin d'identifier un individu n'est pas possible, dès lors que les empreintes digitales ne peuvent pas être enregistrées à l'occasion de la lecture, comme il est dit en B.41.3.

Par ailleurs, comme le soutient le Conseil des ministres, les empreintes digitales ne peuvent pas être lues à l'insu de l'intéressé dès lors que, dans le cadre d'un contrôle effectué par les services de police, la consultation des empreintes digitales suppose un contact direct avec le

citoyen, à propos duquel il s'agit de vérifier que les empreintes digitales correspondent à celles dont l'image numérisée est stockée sur la carte d'identité.

B.44.4. Le grief cité en B.44.1 n'est pas fondé.

*Quant aux demandes de poser des questions préjudicielles à la Cour de justice de l'Union européenne*

B.45.1. Les parties requérantes dans les affaires n$^{os}$ 7150, 7202, 7203 et 7211 suggèrent de poser à la Cour de justice de l'Union européenne plusieurs questions préjudicielles sur la validité du règlement (UE) 2019/1157.

Les parties requérantes suggèrent également de poser à la Cour de justice plusieurs questions préjudicielles sur l'interprétation du droit de l'Union.

B.45.2. L'examen des griefs invoqués n'a pas soulevé de doute concernant la validité d'une ou de plusieurs mesures de la disposition attaquée qui trouvent leur équivalent dans le règlement (UE) 2019/1157 ou 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 aux demandes précitées.

Par ces motifs,

la Cour,

sous réserve des interprétations mentionnées en B.41.3, B.42.2.2 et B.43.2, rejette les recours.

Ainsi rendu en langue française, en langue néerlandaise et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 14 janvier 2021.

Le greffier, Le président,

P.-Y. Dutilleux F. Daoût