Cour constitutionnelle

Arrêt n° 33/2022
du 10 mars 2022
Numéro du rôle : 7330

En cause : le recours en annulation partielle de la loi du 22 mai 2019 « modifiant diverses dispositions en ce qui concerne la gestion de l'information policière », introduit par l'ASBL « Ligue des droits humains ».

La Cour constitutionnelle,

composée des présidents P. Nihoul et L. Lavrysen, et des juges J.-P. Moerman, T. Giet, R. Leysen, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne, D. Pieters, S. de Bethune et E. Bribosia, assistée du greffier P.-Y. Dutilleux, présidée par le président P. Nihoul,

après en avoir délibéré, rend l'arrêt suivant :

I. *Objet du recours et procédure*

Par requête adressée à la Cour par lettre recommandée à la poste le 17 décembre 2019 et parvenue au greffe le 18 décembre 2019, l'ASBL « Ligue des droits humains », assistée et représentée par Me C. Forget, avocat au barreau de Bruxelles, a introduit un recours en annulation des articles 4, 7, 8, 13, 14, 21 et 22 de la loi du 22 mai 2019 « modifiant diverses dispositions en ce qui concerne la gestion de l'information policière » (publiée au *Moniteur belge* du 19 juin 2019).

Le Conseil des ministres, assisté et représenté par Me B. Lombaert, Me S. Adriaenssen et Me J. Simba, avocats au barreau de Bruxelles, a introduit un mémoire, la partie requérante a introduit un mémoire en réponse et le Conseil des ministres a également introduit un mémoire en réplique.

Par ordonnance du 20 octobre 2021, la Cour, après avoir entendu les juges-rapporteurs T. Detienne et D. Pieters, a décidé que l'affaire était en état, qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de cette ordonnance, à être entendue, et qu'en l'absence d'une telle demande, les débats seraient clos le 10 novembre 2021 et l'affaire mise en délibéré.

Aucune demande d'audience n'ayant été introduite, l'affaire a été mise en délibéré le 10 novembre 2021.

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 au moyen unique

A.1. Le moyen unique est pris de la violation des articles 14, 15, 16, 17 et 28 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 des articles 10, 11 et 22 de la Constitution, lus en combinaison ou non avec les articles 6 et 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 47 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et avec les principes généraux du droit de la proportionnalité, de la transparence, de la prévisibilité, de la légalité et de l'égalité. Il est divisé en sept branches.

A.2. Le Conseil des ministres soulève l'irrecevabilité du moyen unique en raison, d'une part, du contrôle direct au regard des dispositions de la directive « police » auquel il invite la Cour et, d'autre part, de l'absence d'exposé des griefs.

Il relève que la loi attaquée s'inscrit dans un cadre légal général qui vise à assurer le respect des droits et libertés de manière structurelle. Il se réfère aux garanties prévues par les articles 28, 29 et 65, 2°, 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), par les titres 5 et 7 de la même loi, par l'article 144 de la loi du 7 décembre 1998 « organisant un service de police intégré, structuré à deux niveaux » et par les articles 44/1 à 44/11/13 de la loi du 5 août 1992 « sur la fonction de police » (ci-après : la loi sur la fonction de police).

A.3. La partie requérante expose qu'il ressort des développements du moyen unique que celui-ci est pris de la violation des articles 10, 11 et 22 de la Constitution, lus en combinaison ou non avec les autres normes de référence qu'elle invoque.

En ce qui concerne les catégories particulières de données (article 44/1, § 2, de la loi sur la fonction de police)

A.4. Dans la première branche du moyen unique, la partie requérante reproche à l'article 44/1 de la loi sur la fonction de police, tel qu'il a été modifié par l'article 4 de la loi attaquée, de ne pas limiter au strict nécessaire le traitement, par les services de police, des catégories particulières de données que sont les données biométriques, les données relatives à la santé et les données génétiques.

En ce qui concerne les données biométriques, la partie requérante fait valoir que la durée de conservation de ces données n'est pas proportionnée et que l'absence d'interdiction de transmettre celles-ci est contraire au considérant 37 de la directive « police ».

En ce qui concerne les données de santé, la partie requérante soutient que la finalité du traitement est énoncée en des termes qui ne satisfont pas au critère de la légalité. Elle souligne que, dans son avis n° 9/2018 du 12 décembre 2018, l'Organe de contrôle de l'information policière (ci-après : l'Organe de contrôle) a invité le législateur à clarifier les termes « comprendre le contexte lié à la personne concernée ». Par ailleurs, selon la partie

requérante, la durée de conservation des données de santé n'est pas proportionnée. Elle soutient en outre que la disposition attaquée ne prévoit pas des conditions d'accès plus strictes pour le traitement des données de santé, ni une interdiction de transmettre ces données, ce qui est contraire à la directive « police ». Elle estime enfin que la disposition attaquée devrait prévoir des critères d'évaluation de la qualité des données de santé, une procédure de validation ainsi qu'un mécanisme d'information préalable de l'Organe de contrôle.

En ce qui concerne les données génétiques, la partie requérante fait valoir que la finalité du traitement est trop large et qu'elle ne permet pas d'apprécier si la durée de conservation de ces données est justifiée. Elle fait également valoir que la disposition attaquée ne prévoit pas de limiter la collecte des données génétiques à « celles en rapport avec la personne concernée », ni des conditions d'accès plus strictes pour le traitement des données génétiques, ni une interdiction de transmettre ces données. Elle soutient que le traitement des données génétiques ou biométriques nécessite des exigences de sécurisation plus strictes.

La partie requérante expose par ailleurs que le législateur a omis de transposer les règles relatives aux droits de la personne concernée d'avoir accès aux données auprès du responsable du traitement et de l'autorité de contrôle prévues aux articles 14, 15 et 17 de la directive « police », qui sont toutefois un préalable indispensable à l'exercice du droit à un recours effectif. La partie requérante invite la Cour à poser à la Cour de justice de l'Union européenne les questions préjudicielles suivantes :

« Est-ce que les articles 42, § 2 et 38, § 2, de la loi du 30 juillet 2018 en ce qu'ils transposent l'article 17, 1 et 17, 3 de la directive ' police ', peuvent être interprétés comme permettant de limiter entièrement le droit d'accès en autorisant l'autorité de contrôle à uniquement informer les personnes concernées qu'elle ' a procédé à toutes les vérifications nécessaires ' ou au contraire est-ce que l'article 17, 1 de la directive ' police ' impose ' également ' de prévoir que le droit d'accès de la personne concernée puisse être exercé auprès du responsable du traitement, outre l'accès par l'intermédiaire de l'autorité de contrôle ? »

« Est-ce que l'article 17, 3 de la directive ' police ' doit être interprété dans le sens où lorsque les droits s'exercent par l'intermédiaire de l'autorité de contrôle comme le prévoit l'article 42, § 1 de la loi du 30 juillet 2018, celle-ci peut se limiter à indiquer qu'elle a procédé à toutes les vérifications nécessaires au sens de l'article 42, § 2 de la loi du 30 juillet 2018 ou au contraire, est-ce que en l'absence de limitation totale ou partielle par la loi nationale (en l'occurrence la loi sur la fonction de police) du droit d'accès doit être interprété en ce que l'autorité de contrôle est tenue d'identifier le responsable du traitement à la demande de la personne concernée et de lui communiquer l'ensemble d'information la concernant au sens de l'article 38, § 1, de la loi du 30 juillet 2018 ? ».

A.5.1. Le Conseil des ministres observe que les griefs concernent uniquement l'article 4, 2°, de la loi attaquée, en ce qu'il insère dans la loi sur la fonction de police un second paragraphe dans l'article 44/1. Il soulève l'irrecevabilité de la première branche du moyen unique en raison de la tardiveté des griefs relatifs aux garanties insuffisantes prévues en matière de droit d'accès aux données et de droit à un recours effectif qui auraient dû être dirigés, selon lui, contre la loi du 30 juillet 2018.

A.5.2. En ordre subsidiaire, le Conseil des ministres expose d'abord que le respect du critère de la légalité fait l'objet d'une appréciation particulière quant aux ingérences visant à protéger la sécurité nationale. En ce qui concerne les données de santé, le Conseil des ministres indique que la finalité d'« assurer la sécurité et [de] protéger la santé de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention policière » vise à permettre que les interventions, planifiées ou non, se déroulent en toute sécurité et à éviter que les personnes présentes lors de l'intervention courent le risque d'être contaminées par une maladie infectieuse. Selon lui, dès lors que le traitement des données vise à assurer l'ordre public et le droit à la vie, il est impossible pour le législateur d'identifier de façon exhaustive l'ensemble des interventions concrètes qui pourraient donner lieu à un traitement des données de santé. Le Conseil des ministres soutient, d'une part, que l'Organe de contrôle a invité le législateur à étendre le champ d'application du traitement des données de santé et, d'autre part, que le législateur a tenu compte des remarques formulées par cet Organe à propos des termes « comprendre le contexte lié à la personne concernée ». En ce qui concerne les données génétiques, le Conseil des ministres estime que le grief manque de pertinence dès lors que l'article 3 de la loi du 22 mars 1999 « relative à la procédure d'identification par analyse ADN en matière pénale » définit les conditions dans lesquelles les données

génétiques peuvent faire l'objet d'un traitement, tandis que la disposition attaquée se limite à exécuter cette disposition. Il relève par ailleurs que la partie requérante n'invoque pas la violation de l'exigence de légalité en ce qui concerne les données biométriques.

A.5.3. Le Conseil des ministres considère ensuite que les catégories particulières de données sont soumises aux délais de conservation prévus par les articles 44/1, § 1er, 44/9 et 44/11/2 de la loi sur la fonction de police, introduits par la loi du 18 mars 2014 « relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle » (ci-après : la loi du 18 mars 2014). Il estime que, par son arrêt n° 108/2016 du 14 juillet 2016, la Cour a déjà jugé que ces délais de conservation sont proportionnés (B.109 à B.116). Selon lui, la Cour ne doit pas procéder à un nouveau contrôle de proportionnalité, dès lors que la directive « police » ne prescrit pas de règle spécifique en ce qui concerne les délais de conservation des catégories particulières de données. Le Conseil des ministres fait en outre valoir que le législateur a pu raisonnablement aligner les délais de conservation des catégories particulières de données sur ceux qui sont applicables aux autres catégories de données qu'ils complètent ou soutiennent. Il conclut que les catégories particulières de données ne sont pas conservées, en vertu de la disposition attaquée, pour une durée qui excéderait la durée nécessaire au regard de la finalité pour laquelle elles sont traitées.

A.5.4. Le Conseil des ministres soutient en outre que l'interdiction de transmettre les données est citée au considérant 37 de la directive « police » comme l'une des garanties appropriées possibles pour les droits et libertés des personnes concernées, sans que cette directive impose l'adoption de cette interdiction. Après avoir relevé que la circulation des données constitue l'un des objectifs de la réglementation européenne en matière de protection des données, il estime que les garanties prévues par l'article 4 de la loi attaquée sont appropriées.

En ce qui concerne les données de santé, le Conseil des ministres fait valoir, premièrement, qu'une distinction entre les données de santé fondées sur des faits ou sur des appréciations personnelles est prévue par l'article 32 de la loi du 30 juillet 2018 et par l'article 4 de la loi attaquée. Deuxièmement, ni le considérant 30, ni l'article 7 de la directive « police » ne prévoient que les États membres doivent établir des catégories en fonction du degré d'exactitude ou de fiabilité des informations traitées. Troisièmement, l'article 32, § 2, de la loi du 30 juillet 2018 impose aux autorités compétentes de vérifier l'exactitude des données avant leur transmission et de fournir au destinataire les informations nécessaires pour juger de cette exactitude. Quatrièmement, l'absence de critères d'évaluation de la qualité des données de santé, d'une procédure de validation ainsi que d'un mécanisme d'information préalable de l'Organe de contrôle n'est pas démontrée. Cinquièmement, les États membres ne sont pas tenus de respecter la recommandation du Groupe 29 à laquelle la partie requérante se réfère de façon imprécise. Sixièmement, l'article 58 de la loi du 30 juillet 2018 prévoit des garanties en cas de recours aux nouvelles technologies.

En ce qui concerne les données génétiques, le Conseil des ministres soutient que l'arrêt de la Cour européenne des droits de l'homme du 4 décembre 2008, en cause *S. et Marper c. Royaume-Uni*, n'est pas transposable.

A.5.5. Le Conseil des ministres estime enfin que le droit d'accès aux données à caractère personnel et le droit de recours effectif des personnes concernées sont garantis par la loi du 30 juillet 2018 et qu'il n'y a pas lieu de poser des questions préjudicielles à la Cour de justice.

A.6. La partie requérante soutient que la première branche du moyen unique est recevable dès lors que l'article 44/1 de la loi sur la fonction de police, inséré par la loi du 18 mars 2014, ne prévoyait pas le traitement des données biométriques, des données de santé et des données génétiques.

Elle soutient par ailleurs que cette disposition générale n'encadre pas la durée de conservation des données. Se référant aux délais de conservation prévus aux articles 44/9 et 44/11/2 de la loi sur la fonction de police, elle fait valoir que le législateur a omis de limiter la durée de conservation des données biométriques et des données de santé au strict nécessaire. Elle observe que les données relatives aux personnes enregistrées pour un fait infractionnel commis dans le cadre du maintien de l'ordre public ne peuvent par exemple pas être archivées tant qu'une mesure doit être prise par une autorité administrative ou judiciaire compétente, même s'il s'agit de données biométriques dont le traitement a pour finalité d'identifier la personne concernée.

Elle précise ne pas critiquer la loi du 30 juillet 2018 mais bien l'absence, dans la loi attaquée, de dispositions spécifiques visant à encadrer les droits des personnes concernées. Selon la partie requérante, la loi du 30 juillet

2018, qui a un caractère générique, ne constitue pas une base légale suffisante. La nécessité d'encadrer les garanties des justiciables par une législation sectorielle ressort, selon elle, de l'article 38, § 2, de la loi du 30 juillet 2018, des travaux préparatoires de cette loi ainsi que des avis de la Commission de la vie privée et de l'Organe de contrôle. Elle observe en outre que la loi attaquée ne se réfère pas à la loi du 30 juillet 2018. Elle estime que la personne concernée ne dispose en aucun cas d'un recours effectif puisque lorsqu'elle exerce son droit d'accès aux données par l'intermédiaire de l'Organe de contrôle, ce dernier se limite à indiquer qu'il a procédé aux vérifications nécessaires sans permettre à la personne concernée de savoir si des données qui la concernent sont traitées ou non. Se référant à la jurisprudence de la Cour de justice de l'Union européenne, la partie requérante soutient que le défaut d'information, d'accès et de recours juridictionnel quant au traitement des catégories particulières de données est d'autant plus critiquable que l'article 14 de la directive « police » généralise le droit d'accès direct à celles-ci et que l'article 17 de cette directive exige qu'une base légale spécifique justifie une limitation à ce droit d'accès.

A.7.1. Selon le Conseil des ministres, ni la directive « police » ni la loi du 30 juillet 2018 n'obligent le législateur à consacrer les droits des personnes concernées au sein d'une loi sectorielle. Selon lui, ces droits tels qu'ils sont prévus par la directive « police » ont été transposés de manière exhaustive par les articles 38, 42 et 209 et suivants de la loi du 30 juillet 2018.

Il fait valoir qu'en optant pour un droit d'accès indirect, par l'intermédiaire de l'Organe de contrôle, aux données concernées, le législateur a mis en œuvre le choix laissé aux États membres sur ce point par la directive « police ». Il fait également valoir que l'exercice des droits des personnes concernées via l'autorité de contrôle compétente était consacré auparavant par l'article 13 de la loi du 8 décembre 1992 « relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ».

Il estime que la partie requérante se réfère à tort à des extraits des travaux préparatoires de la loi du 30 juillet 2018 qui concernent le règlement (UE) n° 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). Or, la directive « police » établit un régime de protection des données à caractère personnel en matière de police et de justice, qui déroge au régime prévu par le RGPD. La directive « police » ne contient notamment pas de dispositions comparables aux articles 9 et 23, paragraphe 2, du RGPD, qui exigent que le traitement des catégories particulières de données fasse l'objet de dispositions législatives spécifiques.

En ce qui concerne l'avis de l'Organe de contrôle, le Conseil des ministres soutient que cet organe n'est pas habilité à juger de la constitutionnalité des lois, qu'il se réfère dans son avis à l'intention du législateur européen et qu'il reconnaît sur son site internet exercer les droits de la personne concernée sur la base de l'article 42, § 2, de la loi du 30 juillet 2018.

Le Conseil des ministres expose enfin que l'article de l'avant-projet de loi à l'origine de l'article 42 de la loi du 30 juillet 2018 a été adopté à la suite de l'avis de la Commission de la vie privée.

A.7.2. En ordre subsidiaire, le Conseil des ministres soutient que les délais de conservation maximaux s'appliquant aux catégories particulières de données à caractère personnel, prévus aux articles 44/9 et 44/11/2 de la loi du 30 juillet 2018, sont proportionnés. Premièrement, la partie requérante demande que le délai de conservation soit déterminé uniquement sur la base de la nature de la donnée traitée, ce qui n'est pas compatible avec le principe selon lequel le délai de conservation doit toujours répondre à des critères objectifs permettant d'établir un rapport entre la donnée conservée et l'objectif poursuivi par le traitement. Deuxièmement, des délais de conservation spécifiques pour les catégories particulières de données, qui seraient différents des délais de conservation prévus pour les données principales qu'elles complètent, compromettraient l'efficacité du traitement. Troisièmement, le traitement des catégories particulières de données à caractère personnel est entouré de nombreuses garanties, dont le contrôle exercé par l'Organe de contrôle. Le Conseil des ministres se réfère à l'arrêt de la Cour européenne des droits de l'homme du 17 décembre 2009, en cause *B.B. c. France*.

Selon le Conseil des ministres, il ressort de la jurisprudence de la Cour européenne des droits de l'homme, de celle de la Cour constitutionnelle et des articles 15 à 17 de la directive « police » que les droits de la personne concernée, en ce compris le droit d'information et le droit d'accès aux données, peuvent être partiellement ou entièrement limités pour autant que la limitation des droits de la personne concernée soit justifiée par un but légitime, qu'il existe des garanties contre les abus, en ce compris l'exercice des droits de la personne concernée

par l'intermédiaire de l'autorité de contrôle compétente, et qu'un contrôle efficace exercé par le pouvoir judiciaire soit établi. Il estime que la loi du 30 juillet 2018 et la loi attaquée assurent le respect de ces conditions.

Selon le Conseil des ministres, premièrement, la limitation des droits de la personne concernée est justifiée par la protection de la sécurité publique et nationale. Deuxièmement, les mesures prévues en matière de délai de conservation et d'accès aux données, les mesures supplémentaires concernant les catégories particulières de données à caractère personnel ainsi que le régime d'accès indirect aux données par l'intermédiaire de l'Organe de contrôle, sont de nature à prévenir les abus. Le Conseil des ministres fait valoir que l'Organe de contrôle est un organe indépendant composé de personnes bénéficiant d'une expérience pertinente en matière de protection des données à caractère personnel. Selon lui, le fait que l'Organe de contrôle se limite à indiquer qu'il a procédé aux examens et vérifications nécessaires découle de l'article 17, paragraphe 3, de la directive « police ». Il estime en outre que, par son arrêt du 18 mai 2010 en cause *Kennedy c. Royaume-Uni*, la Cour européenne des droits de l'homme a jugé conforme à l'article 8 de la Convention européenne des droits de l'homme un mécanisme similaire au mécanisme attaqué. Troisièmement, la personne concernée dispose d'un droit à un recours effectif. Les articles 209 et suivants de la loi du 30 juillet 2018 prévoient une action en cessation devant le président du tribunal de première instance, statuant en référé, tandis que l'article 220 de la même loi organise d'autres recours juridictionnels ou administratifs. Selon le Conseil des ministres, la Cour européenne des droits de l'homme a jugé, par son arrêt en cause *Kennedy c. Royaume-Uni* précité, qu'un mécanisme similaire au mécanisme attaqué ne viole pas le droit à un recours effectif prévu par l'article 6, paragraphe 1, de la Convention européenne des droits de l'homme.

Le Conseil des ministres considère enfin que, par son arrêt n° 108/2016 précité, la Cour a jugé que le régime prévu par la loi du 8 décembre 1992 et par la loi du 18 mars 2014 était proportionné au regard de l'article 22 de la Constitution et de l'article 8 de la Convention européenne des droits de l'homme, et qu'il garantissait un recours effectif. Ce régime étant identique à celui qui est prévu par la loi du 30 juillet 2018, il y a lieu de confirmer les enseignements de cet arrêt.

En ce qui concerne l'interconnexion des banques de données policières (article 44/4 de la loi sur la fonction de police)

A.8. Dans la deuxième branche du moyen unique, la partie requérante fait valoir qu'en confiant directement des missions d'exécution aux ministres de l'Intérieur et de la Justice, l'article 44/4 de la loi sur la fonction de police, tel qu'il a été remplacé par l'article 7 de la loi attaquée, ne satisfait pas au critère de la légalité. Selon elle, la disposition attaquée manque en outre de clarté et de prévisibilité en ce qu'elle ne précise pas les catégories de banques de données, les modalités d'interconnexion et les règles d'accès que doivent établir ces ministres au moyen de directives.

La partie requérante soutient ensuite que la disposition attaquée est incompatible avec l'article 28 de la directive « police » en ce qu'elle ne prévoit pas que les responsables du traitement sont tenus de consulter l'Organe de contrôle avant le traitement des données à caractère personnel qui feront partie d'un nouveau fichier à créer. Elle invite la Cour à poser à la Cour de justice de l'Union européenne la question préjudicielle suivante :

« Est-ce qu'une interconnexion entre différentes bases de données entraîne *ipso facto* la création d'un nouveau fichier au sens de la directive ' police ' et dès lors, doit être soumis à consultation préalable de l'autorité de contrôle (a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 27, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; ou (b) lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées, conformément à l'article 28 de la directive ' police ' ? ».

La partie requérante soutient par ailleurs que la disposition attaquée est incompatible avec l'article 16 de la directive « police » en ce qu'elle ne prévoit pas que les responsables du traitement sont tenus d'indiquer aux destinataires des données que celles-ci font l'objet d'une rectification ou d'un effacement. Elle estime enfin que la disposition attaquée est disproportionnée en ce que l'interconnexion des banques de données rend accessibles aux enquêteurs des données sans intérêt pour eux et en ce que les personnes concernées par ces données sont privées d'un recours effectif. Elle se réfère au projet d'application « i-Police », au rapport intermédiaire du 15 juin 2017 de la commission d'enquête parlementaire « Attentats terroristes » et aux travaux préparatoires de la loi attaquée.

A.9. Le Conseil des ministres soulève l'irrecevabilité de la deuxième branche du moyen unique en raison du caractère purement légistique des modifications introduites, par l'article 7 de la loi attaquée, dans l'article 44/4, § 4, de la loi sur la fonction de police.

En ordre subsidiaire, le Conseil des ministres soutient que la délégation conférée par l'article 7 de la loi attaquée aux ministres de l'Intérieur et de la Justice concernant les modalités de l'interconnexion satisfait à l'exigence de légalité dès lors qu'elle est définie de manière suffisamment précise, qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur et qu'elle se matérialise par l'adoption de textes contraignants. Il relève en outre que la directive « police » n'impose pas de règle particulière en matière d'interconnexion et que les ministres de l'Intérieur et de la Justice sont désignés comme les responsables du traitement par l'article 44/4, § 1er, de la loi sur la fonction de police.

Le Conseil des ministres estime que l'exigence de prévisibilité est également respectée, dès lors qu'il est impossible de déterminer à l'avance l'ensemble des circonstances dans lesquelles une interconnexion se justifie aux fins de la sécurité nationale, que des précisions ont été apportées lors des travaux préparatoires et que le soin de définir les modalités de l'interconnexion et les règles d'accès a été délégué aux ministres en des termes précis.

Le Conseil des ministres expose que, conformément à l'article 59, § 1er, de la loi du 30 juillet 2018 qui transpose l'article 8, paragraphe 1, de la directive « police », l'Organe de contrôle doit être consulté avant un traitement entraînant une interconnexion entre différentes banques de données existantes en vertu de l'article 7 de la loi attaquée. De même, conformément à l'article 39, § 6, de la même loi qui transpose l'article 16, paragraphes 5 et 6, de la directive « police », les responsables du traitement sont tenus d'adresser, en cas de rectification ou d'effacement de données communiquées, une notification aux destinataires de celles-ci.

Il observe que la disposition attaquée établit un fondement légal pour la création de la future plateforme « i-Police », sans porter déjà création de cette plateforme. Il soutient en outre que, conformément à l'article 44/4, § 4, alinéa 2, de la loi sur la fonction de police, les enquêteurs n'auront accès qu'aux informations pertinentes pour leur enquête et qu'un agent aura uniquement accès aux données à caractère personnel selon les droits d'utilisation qui lui sont octroyés vis-à-vis de la banque de données « source ». Il relève que la banque-carrefour de sécurité voulue par la commission d'enquête parlementaire « Attentats terroristes » est un projet distinct de celui de la plateforme « i-Police ». Il souligne que, par la loi attaquée, le législateur a toutefois déjà tenu compte des recommandations de la Commission d'enquête parlementaire en intégrant le principe selon lequel l'accès des enquêteurs aux données disponibles dans une banque-carrefour doit être limité à l'objet de la mission qu'ils mènent.

A.10. La partie requérante soutient que la deuxième branche du moyen unique est recevable dès lors que l'interconnexion entre banques de données prévue par la loi du 21 mars 2018 « modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière » diffère de celle qui est organisée par la loi attaquée.

En ce qui concerne le traitement des données relatives aux personnes faisant l'objet d'une mesure administrative (article 44/5, § 1er, alinéa 1er, 7°, de la loi sur la fonction de police)

A.11. Dans la troisième branche du moyen unique, la partie requérante fait valoir que l'article 44/5 de la loi sur la fonction de police, tel qu'il a été modifié par l'article 8 de la loi attaquée, ne satisfait pas au critère de la légalité en ce que ni cette disposition ni ses travaux préparatoires ne définissent la notion de « mesure administrative ». Elle se réfère à l'avis de l'Organe de contrôle n° 9/2018 du 12 décembre 2018.

A.12. Le Conseil des ministres fait valoir que le législateur a clarifié la notion de « mesure administrative » à la suite de l'avis de l'Organe de contrôle. Il ressort des travaux préparatoires que les mesures administratives sont les mesures adoptées par toute administration susceptible de prendre des mesures ou sanctions dont la surveillance des missions de la police.

En ce qui concerne la conservation et l'archivage des données (article 44/11/2 de la loi sur la fonction de police)

A.13. Dans la quatrième branche du moyen unique, la partie requérante soutient que le système de conservation et d'archivage des données prévu par l'article 44/11/2 de la loi sur la fonction de police, tel qu'il a été modifié par l'article 13 de la loi attaquée, est disproportionné. Elle se réfère à l'avis de l'Organe de contrôle n° 9/2018 du 12 décembre 2018, à l'arrêt de la Cour constitutionnelle n° 108/2016 et à l'arrêt de la Cour européenne des droits de l'homme du 18 septembre 2014 en cause *Brunet c. France*.

A.14. Le Conseil des ministres soulève l'irrecevabilité de la quatrième branche du moyen unique, dès lors que le grief de la partie requérante consiste à critiquer le régime de conservation et d'archivage des données qui a été introduit par la loi du 18 mars 2014 ainsi que la compatibilité de la disposition attaquée avec une autre norme législative (l'article 30 de la loi du 30 juillet 2018). Ce grief a, en outre, déjà été rejeté par l'arrêt n° 108/2016.

En ordre subsidiaire, le Conseil des ministres soutient que le régime de conservation et d'archivage des données introduit en 2014 est constitutionnel. Il se réfère aux développements consacrés à la réfutation de la première branche du moyen unique et à l'arrêt n° 108/2016. Selon le Conseil des ministres, l'arrêt de la Cour européenne des droits de l'homme en cause *Brunet c. France* n'est pas pertinent dès lors qu'il porte sur une situation qui n'est pas visée par la disposition attaquée (la conservation, dans une banque de données policière, de la mention du classement sans suite après médiation pénale) et que le système prévu par la loi sur la fonction de police est très différent du système censuré par cet arrêt.

En ce qui concerne l'avertissement de l'Organe de contrôle en cas de création ou de modifications relatives à une banque de données particulière (article 44/11/3 de la loi sur la fonction de police)

A.15. Dans la cinquième branche du moyen unique, la partie requérante fait valoir que l'article 44/11/3 de la loi sur la fonction de police, tel qu'il a été modifié par l'article 14 de la loi attaquée, viole les normes de référence en ce qu'il supprime l'obligation de déclarer, préalablement à sa création, une banque de données particulière auprès de l'Organe de contrôle.

A.16. Le Conseil des ministres soulève l'irrecevabilité de la cinquième branche du moyen unique en raison de l'absence d'identification des normes de référence dont la violation est alléguée.

En ordre subsidiaire, le Conseil des ministres observe qu'aucune disposition de droit constitutionnel ou de droit européen n'impose l'avis de l'Organe de contrôle avant la création d'une banque de données particulière. Selon lui, le législateur a estimé que l'ancien système de déclaration obligatoire et de demande d'avis auprès de l'Organe de contrôle qui tenait à jour un registre, n'était plus adapté à la loi du 30 juillet 2018. Le Conseil des ministres considère que le nouveau système d'avertissement par le biais du registre unique des activités de traitement est encadré par de nombreuses garanties. La consultation préalable de l'Organe de contrôle est maintenue par l'article 59 de la loi du 30 juillet 2018 mais cette consultation est limitée à certaines hypothèses, que l'Organe de contrôle peut compléter.

En ce qui concerne l'accès direct des services de renseignement et de sécurité à la banque de données nationale générale (ci-après : la B.N.G.) (article 44/11/8bis de la loi sur la fonction de police)

A.17. Dans la sixième branche du moyen unique, la partie requérante soutient que l'article 44/11/8*bis* de la loi sur la fonction de police, inséré par l'article 21 de la loi attaquée, ne satisfait pas au critère de la légalité en ce qu'il ne détermine pas les règles selon lesquelles les services de renseignement et de sécurité bénéficient d'un accès direct à la B.N.G. Selon la partie requérante, la disposition attaquée ne respecte pas non plus le principe de finalité, le droit à la présomption d'innocence et les critères de la nécessité et de la proportionnalité.

A.18. Le Conseil des ministres soulève l'irrecevabilité de la sixième branche du moyen unique au motif que l'accès contesté à la B.N.G. est prévu par l'article 24 de la loi du 22 mai 2019, lequel n'est pas attaqué.

En ordre subsidiaire, le Conseil des ministres soutient que, par les articles 44/11/12, § 1er, et 44/11/8*bis* de la loi sur la fonction de police, le législateur a expressément désigné les autorités qui peuvent prétendre à un accès direct à la B.N.G. Par ailleurs, l'article 44/11/12 de la loi sur la fonction de police prévoit, dans son paragraphe 1er,

que les modalités de cet accès direct sont fixées par le Roi, après avis de l'Organe de contrôle. La même disposition définit, dans son paragraphe 2, les éléments essentiels de ces modalités d'accès. Selon le Conseil des ministres, la Cour a déjà jugé que cette délégation est constitutionnelle par son arrêt n° 108/2016 (B.66.4). Il relève en outre que les services de renseignement et de sécurité pouvaient déjà obtenir auprès des services de police toutes les informations utiles à l'exécution de leurs missions en vertu de l'article 14 de la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité » (ci-après : la loi du 30 novembre 1998).

Le Conseil des ministres considère par ailleurs que l'accès direct des services de renseignement et de sécurité à la B.N.G. sert la sauvegarde de la sécurité nationale et publique, la prévention des troubles et de la criminalité et la protection des droits et libertés d'autrui, qui sont des objectifs légitimes. Il fait valoir que l'article 29, § 2, de la loi du 30 juillet 2018 autorise le traitement ultérieur à d'autres fins que celles pour lesquelles elles ont été collectées par les services de police si cette finalité est permise conformément à la loi et que ce traitement ultérieur est autorisé par l'article 44/11/8*bis* de la loi sur la fonction de police et par les articles 14 et 19 de la loi du 30 novembre 1998. Il relève également que les finalités des services de renseignement et de sécurité sont déterminées aux articles 7, 8 et 11 de la loi du 30 novembre 1998 et que l'accès direct octroyé à ces services répond aux exigences de la recommandation du Groupe 29. Selon le Conseil des ministres, la présomption d'innocence ne peut pas être violée dès lors que, conformément à l'article 19/1 de la loi du 30 novembre 1998, le traitement de données par les services de renseignement et de sécurité ne peut pas contribuer à lui seul à la condamnation d'une personne. Il estime, au contraire, que l'accès direct à la B.N.G. par les services de renseignement et de sécurité, et la discrétion des recherches qu'ils effectuent contribuent à préserver la présomption d'innocence de la personne concernée à l'égard des services de police, qui pourraient interpréter erronément l'existence d'une recherche effectuée par les services de renseignement et de sécurité dans la B.N.G.

Selon le Conseil des ministres, il ressort des travaux préparatoires que l'accès direct à la B.N.G. au profit des services de renseignement et de sécurité est proportionné. Selon lui, les affirmations de la partie requérante en sens contraire s'apparentent à des pétitions de principe. Il soutient que l'affirmation selon laquelle les services de renseignements et de sécurité estiment que la mesure attaquée est disproportionnée est inexacte. Il se réfère à un courrier du Comité R du 5 février 2019.

En ce qui concerne l'avis de l'Organe de contrôle en cas de communication de données à des autorités publiques (article 44/11/9 de la loi sur la fonction de police)

A.19. Dans la septième branche du moyen unique, la partie requérante fait valoir que l'article 44/11/9 de la loi sur la fonction de police, tel qu'il a été modifié par l'article 22 de la loi attaquée, viole les normes de référence en ce qu'il n'impose pas un avis contraignant de l'Organe de contrôle en cas de communication de données à caractère personnel à des autorités publiques.

A.20. Le Conseil des ministres soulève l'irrecevabilité de la septième branche du moyen unique en raison de l'absence d'identification des normes de référence dont la violation est alléguée.

En ordre subsidiaire, le Conseil des ministres fait valoir qu'un contrôle préalable par l'Organe de contrôle est maintenu par l'article 44/11/9, § 2, de la loi sur la fonction de police qui prévoit que la liste des autorités, organes ou organismes publics auxquels pourront être également communiquées les données à caractère personnel est élaborée après avis de l'Organe de contrôle. Il fait également valoir que la Cour a déjà jugé, par son arrêt n° 108/2016 que l'avis préalable de l'Organe de contrôle était constitutionnel (B.99). Il observe qu'après avoir renforcé le rôle du responsable du traitement et les missions de l'Organe de contrôle dans les articles 59, 239, § 3, et 247 de la loi du 30 juillet 2018, le législateur n'a pas jugé nécessaire de rendre contraignant l'avis préalable de l'Organe de contrôle en cas de communication de données à des autorités publiques.

Le Conseil des ministres relève que le considérant 22 de la directive « police » s'applique uniquement dans le cas précis de l'inapplicabilité du RGPD au destinataire. Selon lui, la disposition attaquée ne saurait être interprétée comme permettant aux autorités publiques de se voir communiquer indistinctement l'ensemble d'une banque de données policière, dès lors que la communication de données aux autorités publiques doit être licite, proportionnée et conforme au principe de minimisation visé à l'article 28 de la loi du 30 juillet 2018.

- B -

Quant au contexte des dispositions attaquées

B.1.1. La partie requérante demande l'annulation partielle de la loi du 22 mai 2019 « modifiant diverses dispositions en ce qui concerne la gestion de l'information policière » (ci-après : la loi attaquée).

Cette loi vise à adapter la législation relative à la gestion des données à caractère personnel et des informations par les services de police après l'adoption, le 27 avril 2016, du règlement (UE) 2016/679 du Parlement européen et du Conseil « 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) et de la directive (UE) 2016/680 du Parlement européen et du Conseil « 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 ») (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, p. 5).

En vue de l'exécution du RGPD et de la transposition de la directive « police », le législateur belge a adopté une législation-cadre, constituée notamment de la loi du 3 décembre 2017 « portant création de l'Autorité de protection des données » (ci-après : la loi du 3 décembre 2017) 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).

Le titre 2 de la loi du 30 juillet 2018 fixe le cadre général applicable au traitement des données à caractère personnel par les services de police. La loi attaquée vise à traduire ce cadre général « de façon concrète dans la législation opérationnelle et statutaire actuelle de la police intégrée » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, p. 6).

B.1.2. La loi attaquée modifie deux autres lois. Elle modifie en premier lieu la loi du 5 août 1992 « sur la fonction de police » (ci-après : la loi sur la fonction de police).

Les modifications apportées à la loi sur la fonction de police figurent dans le chapitre 1er du titre II de la loi attaquée (articles 2 à 26).

B.1.3. La loi attaquée modifie également la loi du 7 décembre 1998 « organisant un service de police intégré, structuré à deux niveaux ».

Les modifications apportées à la loi du 7 décembre 1998, précitée, figurent dans le chapitre 2 du titre II de la loi attaquée (articles 27 à 33).

B.1.4. La loi attaquée est entrée en vigueur le 29 juin 2019.

Quant à la recevabilité

B.2.1. Les griefs soulevés par la partie requérante étant exclusivement dirigés contre les articles 4, 7, 8, 13, 14, 21 et 22 de la loi attaquée, le recours est seulement recevable en ce qu'il est dirigé contre ces articles.

B.2.2. Le Conseil des ministres conteste la recevabilité de la plupart des griefs formulés dans le moyen unique au motif qu'ils ne seraient pas suffisamment développés ou qu'ils seraient dirigés contre des dispositions législatives autres que celles qui sont attaquées. En outre, il souligne que le moyen unique serait irrecevable parce que la Cour n'est pas compétente pour exercer un contrôle direct au regard d'actes législatifs de l'Union européenne (la directive « police » précitée).

B.2.3. La Cour est compétente pour contrôler des normes de nature législative au regard des règles répartitrices de compétences entre l'autorité fédérale, les communautés et les régions, ainsi qu'au regard des articles du titre II (« Des Belges et de leurs droits ») et des articles 143, § 1er, 170, 172 et 191 de la Constitution.

Tous les griefs sont pris de la violation d'une ou de plusieurs règles dont la Cour garantit le respect. Pour autant que la partie requérante invoque en outre la violation d'un acte législatif de l'Union européenne, la Cour n'examine les griefs qu'en tant que la partie requérante dénonce la violation des dispositions constitutionnelles précitées, lues en combinaison avec l'acte visé. Dans cette mesure, les griefs sont recevables.

B.2.4.1. Pour satisfaire aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, les moyens de la requête doivent faire connaître, parmi les règles dont la Cour garantit le respect, celles qui seraient violées ainsi que les dispositions qui violeraient ces règles et exposer en quoi ces règles auraient été transgressées par ces dispositions.

B.2.4.2. Dans la cinquième branche du moyen unique, la partie requérante fait valoir que l'article 44/11/3 de la loi sur la fonction de police, tel qu'il a été modifié par l'article 14 de la loi attaquée, viole les normes de référence mentionnées en B.3, en ce que le législateur a remplacé l'obligation de déclarer préalablement à l'Organe de contrôle de l'information policière (ci-après : l'Organe de contrôle) la création de toute nouvelle banque de données par un système qui avertit activement l'Organe de contrôle par le biais du registre unique des activités de traitement des services de police.

La partie requérante n'expose toutefois pas en quoi la disposition attaquée violerait ces normes de référence. Elle se borne à constater qu'une telle restriction extrême des droits des personnes concernées requerrait un contrôle préalable, quoiqu'elle ne précise pas pourquoi la disposition attaquée, qui contient une autre garantie, ne suffirait pas pour protéger ces droits.

Par conséquent, le moyen unique, en sa cinquième branche, est irrecevable.

B.2.4.3. Dans la septième branche du moyen unique, la partie requérante fait valoir que l'article 44/11/9 de la loi sur la fonction de police, tel qu'il a été modifié par l'article 22 de la loi attaquée, viole les normes de référence mentionnées en B.3, en ce qu'il n'impose pas un avis contraignant de l'Organe de contrôle en cas de communication de données à caractère personnel à des autorités publiques.

La partie requérante se contente de souligner qu'une telle garantie « fait défaut en l'espèce », sans préciser en quoi cette garantie serait nécessaire. Elle ne satisfait pas, ainsi, à son obligation d'exposer en quoi ces normes de référence seraient violées par la disposition attaquée.

Par conséquent, le moyen unique, en sa septième branche, est irrecevable.

B.2.4.4. La Cour n'examine également les autres branches du moyen unique et les griefs qui y sont formulés qu'en ce qu'ils satisfont aux exigences mentionnées en B.2.4.1.

B.2.5. La question de savoir si les griefs évoqués trouvent leur origine dans d'autres dispositions que dans celles qui sont attaquées dépend de la portée de celles-ci. L'examen de cette exception d'irrecevabilité se confond avec celui du fond de l'affaire.

Quant au moyen unique

B.3. Le moyen unique est pris de la violation des articles 10, 11 et 22 de la Constitution, lus ou non en combinaison avec les articles 14, 15, 16, 17 et 28 de la directive « police », avec les articles 6 et 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 47 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après : la Charte) et avec les principes généraux de droit de la proportionnalité, de la transparence, de la prévisibilité, de la légalité et de l'égalité.

Selon la partie requérante, la loi attaquée porterait atteinte au droit au respect de la vie privée, au droit à la protection des données à caractère personnel et au droit à un recours effectif, garantis par ces dispositions. Plusieurs mesures instaurées par la loi attaquée ne respecteraient pas le principe de la légalité et seraient disproportionnées.

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

B.4.1. 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.4.2. 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.4.3. 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.4.4. Le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelle et conventionnelle précitées, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée.

La proposition qui a précédé l'adoption de l'article 22 de la Constitution insistait sur « la protection de la personne, la reconnaissance de son identité, l'importance de son épanouissement et celui de sa famille », et elle soulignait la nécessité de protéger la vie privée

et familiale « des risques d'ingérence que peuvent constituer, notamment par le biais de la modernisation constante des techniques de l'information, les mesures d'investigation, d'enquête et de contrôle menées par les pouvoirs publics et organismes privés, dans l'accomplissement de leurs fonctions ou de leurs activités » (*Doc. parl.*, Sénat, S.E. 1991-1992, n° 100-4/2°, p. 3). Cette proposition indiquait également que le législateur « ne pourrait en aucun cas vider de sa substance le droit au respect de la vie privée et familiale, sous peine d'enfreindre la règle constitutionnelle, en plus des règles internationales » (*ibid.*).

Le droit au respect de la vie privée a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles. La jurisprudence de la Cour européenne des droits de l'homme fait apparaître que de la protection de ce droit relèvent notamment les données et informations personnelles suivantes : le nom, l'adresse, les activités professionnelles, les relations personnelles, les empreintes digitales, les images filmées, les photographies, les communications, les données ADN, les données judiciaires (condamnations ou inculpations), les données financières 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.4.5. Le droit au respect de la vie privée n'est toutefois pas absolu. L'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme n'excluent pas une ingérence d'une autorité publique dans l'exercice de ce droit, pourvu que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit. Ces dispositions engendrent de surcroît l'obligation positive, pour l'autorité publique, de prendre des mesures qui assurent le respect effectif de la vie privée, même dans la sphère des relations entre les individus (CEDH, 27 octobre 1994, *Kroon et autres c. Pays-Bas*, § 31; grande chambre, 12 novembre 2013, *Söderman c. Suède*, § 78).

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. Pour juger de cet équilibre, la Cour européenne des droits de l'homme tient compte notamment des dispositions de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après : la Convention n° 108) et de la recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (ci-après : la recommandation n° R (87) 15) (CEDH, 25 février 1997, *Z c. Finlande*, § 95; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 103).

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

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

B.5.1. Lorsque la Charte des droits fondamentaux de l'Union européenne contient des droits correspondant à des droits garantis par la Convention européenne des droits de l'homme, « leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ». Cette disposition aligne le sens et la portée des droits qui sont garantis par la Charte sur les droits correspondants qui sont garantis par la Convention européenne des droits de l'homme.

Les explications relatives à la Charte (2007/C 303/02), publiées au *Journal officiel* du 14 décembre 2007, indiquent que, parmi les articles « dont le sens et la portée sont les mêmes que ceux des articles correspondants dans la CEDH », l'article 7 de la Charte correspond à l'article 8 de la Convention européenne des droits de l'homme.

La Cour de justice de l'Union européenne rappelle à cet égard que « l'article 7 de la Charte, relatif au droit au respect de la vie privée et familiale, contient des droits correspondant à ceux garantis par l'article 8, paragraphe 1, de la [Convention européenne des droits de l'homme (ci-après : la CEDH),] et qu'il convient donc, conformément à l'article 52, paragraphe 3, de la

Charte, de donner audit article 7 le même sens et la même portée que ceux conférés à l'article 8, paragraphe 1, de la CEDH, tel qu'interprété par la jurisprudence de la Cour européenne des droits de l'homme » (CJUE, 17 décembre 2015, C-419/14, *WebMindLicenses Kft.*, point 70; 14 février 2019, C-345/17, *Buivids*, point 65).

En ce qui concerne l'article 8 de la Charte, la Cour de justice considère qu'« ainsi que le prévoit expressément l'article 52, paragraphe 3, seconde phrase, de la Charte, l'article 52, paragraphe 3, première phrase, de celle-ci ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue que la CEDH », et que « l'article 8 de la Charte concerne un droit fondamental distinct de celui consacré à l'article 7 de celle-ci et qui n'a pas d'équivalent dans la CEDH » (CJUE, grande chambre, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige*, point 129).

Il découle de ce qui précède que, dans le champ d'application du droit de l'Union européenne, l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme et l'article 7 de la Charte garantissent des droits fondamentaux analogues, alors que l'article 8 de cette Charte vise spécifiquement la protection des données à caractère personnel.

B.5.2. 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 physique identifiée ou identifiable (CJUE, grande chambre, 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke et Eifert*, point 52; 16 janvier 2019, C-496/17, *Deutsche Post AG*, point 54).

B.6. La directive « police » fixe, dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière, des règles spécifiques relatives 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces », en respectant la nature spécifique de ces activités (article 1er, paragraphe 1, de la directive « police »).

Comme il ressort des articles 2, paragraphe 1, et 9, paragraphes 1 et 2, de la directive « police », des considérants 11, 12 et 34 de celle-ci, de l'article 2, paragraphe 2, point *d)*, du RGPD et du considérant 19 de celui-ci, le traitement des données à caractère personnel par les autorités compétentes aux fins de justice pénale énoncées à l'article 1er, paragraphe 1, de la directive « police », précité, relève de cette directive, et non du RGPD. Le traitement des données à caractère personnel à des fins autres que les fins de justice pénale et qui relève du champ d'application du droit de l'Union, est par contre soumis au RGPD.

B.7. Comme le précise l'article 25 de la loi du 30 juillet 2018, le titre 2 de cette loi transpose la directive « police ».

Comme le précise l'article 27 de la même loi, le titre 2 de la loi du 30 juillet 2018 s'applique aux « traitements de données à caractère personnel effectués par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ». Sont des autorités compétentes au sens du titre 2 : les services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 « organisant un service de police intégré, structuré à deux niveaux », les autorités judiciaires et les autres autorités visées à l'article 26, 7°, de la loi du 30 juillet 2018.

Les services de police sont donc soumis au titre 2 de la loi du 30 juillet 2018 lorsqu'ils traitent des données à caractère personnel en vue de l'une des fins de justice pénale énumérées à l'article 27 de cette loi. Comme il est dit en B.6, les services de police sont en revanche soumis au RGPD et aux mesures d'exécution de celui-ci en droit interne pour les traitements de données à caractère personnel qu'ils effectuent à des fins autres que ces fins de justice pénale, par exemple pour les traitements à des fins de gestion des ressources humaines des services de police (*Doc. parl.*, Chambre, 2017-2018, DOC 54-3126/001, pp. 17 et 69).

L'Organe de contrôle est l'autorité de contrôle des services de police. Il est chargé de surveiller l'application du titre 2 de la loi du 30 juillet 2018, de contrôler le traitement des informations et des données à caractère personnel visées aux articles 44/1 à 44/11/13 de la loi sur la fonction de police y compris celles qui sont incluses dans les banques de données visées

à l'article 44/2 de la même loi, et de toute autre mission organisée par ou en vertu d'autres lois (article 71, § 1er, alinéa 3, de la loi du 30 juillet 2018). Les dispositions relatives à la composition, aux missions, aux compétences et au financement de cet organe forment le titre 7 de la loi du 30 juillet 2018 (articles 231 à 251).

En ce qui concerne l'ordre d'examen des griefs

B.8. La partie requérante critique plusieurs aspects de la loi attaquée, que la Cour examine dans l'ordre suivant :

1. les catégories particulières de données (article 44/1, § 2, de la loi sur la fonction de police);

2. l'interconnexion des banques de données policières (article 44/4 de la loi sur la fonction de police);

3. le traitement des données relatives aux personnes faisant l'objet d'une mesure administrative (article 44/5, § 1er, alinéa 1er, 7°, de la loi sur la fonction de police);

4. la conservation et l'archivage des données (article 44/11/2 de la loi sur la fonction de police);

5. l'accès direct des services de renseignements et de sécurité à la banque de données nationale générale (ci-après : la B.N.G.) (article 44/11/8*bis* de la loi sur la fonction de police).

Quant aux catégories particulières de données (article 44/1, § 2, de la loi sur la fonction de police)

B.9. Dans la première branche du moyen unique, la partie requérante allègue que l'article 44/1, § 2, de la loi sur la fonction de police, tel qu'il a été remplacé par l'article 4, 2°,

de la loi attaquée, est contraire au droit au respect de la vie privée et au droit à la protection des données à caractère personnel, garantis par les dispositions mentionnées en B.3, en ce que, premièrement, les finalités du traitement des données de santé et des données génétiques ne sont pas suffisamment claires, deuxièmement, le délai de conservation des données biométriques et des données de santé est disproportionné, troisièmement, les garanties prévues ne sont pas suffisantes et, quatrièmement, les personnes concernées ne disposent pas d'un droit d'accès aux catégories particulières de données, ni d'une voie de recours effective.

B.10.1. L'article 10 de la directive « police » dispose :

« Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et 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 est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :

a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre;

b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique; ou

c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée ».

Le considérant 37 de la directive « police » indique :

« Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits. Ces données à caractère personnel devraient comprendre les données à caractère personnel qui révèlent l'origine raciale ou ethnique, étant entendu que l'utilisation de l'expression ' origine raciale ' dans la présente directive n'implique pas que l'Union adhère à des théories tendant à établir l'existence de races humaines distinctes. Ces données à caractère personnel ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne s'accompagne de garanties appropriées pour les droits et libertés de la personne concernée fixées par la loi et ne soit permis dans des cas autorisés par la loi; lorsqu'il n'est pas déjà autorisé par une telle loi, qu'il ne soit nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne; ou qu'il ne porte sur des données manifestement rendues publiques par la personne concernée. Des garanties appropriées pour les droits et des libertés de la personne concernée pourraient comprendre la possibilité de ne collecter ces données qu'en rapport avec d'autres données relatives à la personne physique concernée, la possibilité de sécuriser les

données collectées de manière adéquate, des règles plus strictes pour l'accès du personnel de l'autorité compétente aux données et l'interdiction de la transmission de ces données. Il convient également que le traitement de pareilles données soit autorisé par la loi lorsque la personne concernée a expressément marqué son accord au traitement qui est particulièrement intrusif pour elle. Toutefois, l'accord de la personne concernée ne devrait pas constituer en soi une base juridique pour le traitement de ces données à caractère personnel sensibles par les autorités compétentes ».

Il ressort de l'article 10 de la directive « police », lu en combinaison avec le considérant 37 de celle-ci, que les catégories particulières de données à caractère personnel sont les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et droits fondamentaux. Il s'agit des données à caractère personnel qui révèlent « l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, [les] données biométriques aux fins d'identifier une personne physique de manière unique, [les] données concernant la santé ou [les] données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».

B.10.2. L'article 34 de la loi du 30 juillet 2018, qui transpose l'article 10 de la directive « police », dispose :

« § 1er. Le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et 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, n'est autorisé qu'en cas de nécessité absolue et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement dans l'un des cas suivants :

1° lorsque le traitement est autorisé par la loi, le décret, l'ordonnance, le droit de l'Union européenne ou l'accord international;

2° lorsque le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne physique;

3° lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.

§ 2. Les garanties nécessaires visées au paragraphe 1er prévoient au moins que l'autorité compétente ou le responsable de traitement établisse une liste des catégories de personnes, ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées. Cette liste est tenue à la disposition de l'autorité de contrôle compétente.

L'autorité compétente veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées ».

B.11.1. L'article 4, 2°, de la loi attaquée remplace le paragraphe 2 de l'article 44/1 de la loi sur la fonction de police. À la suite de cette modification, l'article 44/1, § 2, de la loi sur la fonction de police dispose :

« En vue d'exercer leurs missions, les services de police peuvent traiter les catégories particulières de données à caractère personnel visées à l'article 34 de la loi relative à la protection des données en complément ou en soutien d'autres catégories de données visées à l'article 44/5.

En plus de la condition visée à l'alinéa 1er :

1° les données biométriques sont traitées uniquement dans le but d'assurer l'identification certaine de la personne concernée visée à l'article 44/5, § 1er, 2° à 7° et § 3 1° à 6°. Les données biométriques des personnes visées au § 3, 7° à 9°, et au § 4 de l'article 44/5 sont traitées uniquement sur la base du consentement de la personne concernée ou lorsqu'elles sont manifestement rendues publiques par la personne concernée ou encore pour sauvegarder les intérêts vitaux de la personne concernée ou d'une autre personne physique. Lorsque le traitement des données biométriques en vue de l'identification unique des personnes concernées, en particulier par le recours aux nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement ou son sous-traitant consulte l'Organe de contrôle;

2° les données relatives à la santé sont traitées uniquement dans le but de comprendre le contexte lié à la personne concernée, ainsi que pour assurer la sécurité et protéger la santé de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention policière. Lorsque des données relatives à la santé sont traitées, il est mentionné si ces données proviennent ou non de professionnels de soins de la santé. Le traitement de données relatives à la santé visé dans cet article n'a jamais pour conséquence de contraindre les personnes concernées à se soumettre à des examens médicaux;

3° le traitement des données génétiques concerne uniquement la collecte des données génétiques et l'enregistrement des mentions administratives liées au profil génétique, à l'exclusion de la comparaison des profils génétiques ou de l'identification du numéro de code ADN et s'effectue dans le cadre de l'exercice des missions de police judiciaire et de l'application de la législation relative à la protection civile.

Lors des traitements de données à caractère personnel visés dans ce paragraphe, les garanties suivantes en matière de protection des données à caractère personnel sont d'application :

1° les catégories de personnes, ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description de leur fonction par rapport au traitement des données visées;

2° la liste des catégories des personnes ainsi désignées pour traiter les données visées dans ce paragraphe est tenue à la disposition de l'Organe de contrôle par le responsable du traitement ou, le cas échéant, par le sous-traitant;

3° les personnes désignées sont tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées;

4° une distinction claire est opérée entre les catégories de personnes visées à l'article 44/5;

5° des mesures techniques ou organisationnelles appropriées sont adoptées pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification ou tout autre traitement non autorisé de ces données;

6° les responsables du traitement indiquent dans leur politique de protection des données les actions à mener pour protéger le traitement de ces catégories de données et pour assurer la qualité des données traitées notamment pour les aspects liés à l'évaluation de leur exactitude, leur exhaustivité, leur fiabilité et leur niveau de mise à jour. Les délégués à la protection des données compétents veillent à assurer le suivi de cette politique.

Le Roi peut prévoir d'autres garanties complémentaires appropriées ».

B.11.2. En vertu de l'article 44/1, § 1er, de la loi sur la fonction de police, tel qu'il a été modifié par l'article 4, 1°, de la loi attaquée, les services de police peuvent, dans le cadre de l'exercice de leurs missions et conformément aux finalités de justice pénale énoncées à l'article 27 de la loi du 30 juillet 2018, mentionné en B.7, traiter des informations et des données à caractère personnel « pour autant que ces dernières présentent un caractère adéquat, pertinent et non excessif au regard des finalités de police administrative et de police judiciaire pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».

L'article 44/1, § 2, de la loi sur la fonction de police, tel qu'il a été remplacé par l'article 4, 2°, de la loi attaquée, fixe le cadre légal applicable aux traitements des catégories particulières de données à caractère personnel effectués par les services de police. En vertu de cette disposition, les catégories particulières de données à caractère personnel sont traitées « en complément ou en soutien » du traitement principal portant sur l'une des catégories de données

énumérées à l'article 44/5 de la loi sur la fonction de police (article 44/1, § 2, alinéa 1er). À cet égard, il est précisé dans les travaux préparatoires :

« Les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont uniquement traitées de manière incidente par rapport à un traitement principal portant sur l'une des catégories de données énumérées à l'art. 44/5. Tel sera par exemple le cas d'une enquête portant sur des agressions homophobes » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 11-12).

Le traitement des catégories particulières de données est, en outre, accompagné des garanties visées à l'article 44/1, § 2, alinéa 3, de la loi sur la fonction de police, parmi lesquelles figurent les deux garanties minimales prévues par l'article 34, § 2, de la loi du 30 juillet 2018. En vertu de l'article 44/1, § 2, alinéa 4, de la loi sur la fonction de police, le Roi peut prévoir d'autres garanties complémentaires appropriées. Le traitement des données biométriques, des données de santé et des données génétiques est soumis, par ailleurs, aux conditions prévues pour chacune de ces catégories particulières de données, par l'article 44/1, § 2, alinéa 2, de la loi sur la fonction de police.

En vertu de l'article 44/3, § 1er, alinéa 1er, de la loi sur la fonction de police, tel qu'il a été modifié par l'article 6, 1°, de la loi attaquée, le traitement des données à caractère personnel « visées à l'article 44/1 [de la loi sur la fonction de police] y compris celui effectué dans les banques de données visées à l'article 44/2 » se fait conformément à la loi du 30 juillet 2018. Le traitement des catégories particulières de données qui sont visées au paragraphe 2 de l'article 44/1 de la loi sur la fonction de police, précité, se fait donc également conformément à la loi du 30 juillet 2018.

En ce qui concerne les finalités du traitement des données de santé et des données génétiques

B.12. La partie requérante allègue, en ce qui concerne les données de santé, que les termes « comprendre le contexte lié à la personne concernée » visés à l'article 44/1, § 2, alinéa 2, 2°, de la loi sur la fonction de police, inséré par l'article 4, 2°, de la loi attaquée, ne sont pas suffisamment clairs. En ce qui concerne les données génétiques, elle estime que les termes

« l'exercice des missions de police judiciaire » et « l'application de la législation relative à la protection civile », visés à l'article 44/1, § 2, alinéa 2, 3°, de la loi sur la fonction de police, inséré par l'article 4, 2°, de la loi attaquée, ne sont pas suffisamment précis.

B.13.1. 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.

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

B.13.2. 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 pouvoir avoir une idée suffisamment claire des données traitées, des personnes concernées par un traitement de données déterminé et des conditions et finalités dudit traitement.

Plus particulièrement lorsque l'intervention de l'autorité présente un caractère secret, la loi doit offrir des garanties suffisantes contre les ingérences arbitraires dans l'exercice du droit au respect de la vie privée, en délimitant le pouvoir d'appréciation des autorités concernées avec une netteté suffisante, d'une part, et en prévoyant des procédures qui permettent un contrôle juridictionnel effectif, d'autre part (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 55; 6 juin 2006, *Segerstedt-Wiberg* c. Suède, § 76; 4 juillet 2006, *Lupsa c. Roumanie*, § 34).

Le niveau requis de précision de la législation concernée – laquelle ne peut du reste parer à toute éventualité – dépend notamment du domaine qu'elle est censée couvrir et du nombre et de la qualité de ses destinataires (CEDH, grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, §§ 95 et 96). Ainsi, la Cour européenne des droits de l'homme a jugé que l'exigence de prévisibilité dans des domaines liés à la sécurité nationale ne pouvait avoir la même portée que dans d'autres domaines (CEDH, 26 mars 1987, *Leander c. Suède*, § 51; 4 juillet 2006, *Lupsa c. Roumanie*, § 33).

1) Les données de santé

B.14.1. En vertu de l'article 26, 14°, de la loi du 30 juillet 2018, les données concernant la santé sont « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris les données à caractère personnel concernant la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».

B.14.2. Le traitement des données de santé par les services de police est soumis aux conditions, citées en B.11.2, applicables à tout traitement de catégories particulières de données en vertu de l'article 44/1, § 2, alinéas 1er et 3, de la loi sur la fonction de police. En outre, en vertu de l'article 44/1, § 2, alinéa 2, 2°, de la même loi, inséré par l'article 4, 2°, de la loi attaquée, le traitement des données de santé par les services polices peut intervenir (1) uniquement « dans le but de comprendre le contexte lié à la personne concernée » et « pour assurer la sécurité et protéger la santé de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention policière », (2) avec la mention que ces données proviennent ou non de professionnels de soins de la santé et (3) sans avoir pour conséquence de contraindre les personnes concernées à se soumettre à des examens médicaux.

Il ressort des travaux préparatoires que cette dernière disposition a été introduite afin de permettre aux interventions, planifiées ou non, de se dérouler en toute sécurité et d'éviter que les fonctionnaires de police et les autres personnes présentes lors d'une intervention courent le risque d'être contaminés par une maladie infectieuse :

« La disposition concernant les données relatives à la santé est insérée en raison du fait que les fonctionnaires de police et les assistants et agents de sécurisation de police, ainsi que les personnes placées sous leur protection, le personnel de secours, les personnes arrêtées, les avocats qui prêtent leur assistance dans le cadre d'auditions (notamment pour la concertation confidentielle) et les experts judiciaires (interprètes) courent toujours le risque d'être contaminés par des maladies hautement contagieuses. Ce risque se pose en cas de bagarres, fouilles, incidents impliquant des morsures, arrestations, …

Au-delà de la gestion émotionnelle, d'autres questions subsistent, comme la grande incertitude quant à une éventuelle contamination. Les tests médicaux concernant certaines maladies infectieuses ne peuvent souvent livrer un résultat certain que des mois après l'infection présumée. En attendant, la personne concernée, tout comme sa famille, reste confrontée à une douloureuse incertitude. Pareille situation peut également engendrer une incapacité de travail.

Dans certains cas, il y a également un intérêt à permettre une intervention rapide en vue d'un traitement médicamenteux prophylactique post-exposition. Par exemple, après un incident impliquant un contact avec une seringue, un traitement à l'aide d'inhibiteurs du VIH peut être nécessaire (de préférence dans les 2 heures, et au maximum dans les 72 heures) afin de réduire au maximum le risque d'infection. Comme le traitement à l'aide d'inhibiteurs du VIH provoque parfois des effets secondaires, il est nécessaire d'effectuer une juste appréciation entre le risque encouru et la charge du traitement.

De surcroît, il peut être utile de savoir, en fonction d'informations obtenues lors de précédentes confrontations, pourquoi un changement d'humeur soudain ou une réaction de panique peut se produire chez une personne concernée. Chez certaines personnes présentant un trouble du développement, certaines situations peuvent en effet provoquer des réactions violentes. Lorsque de telles réactions sont apparues lors d'une précédente intervention, il est important que cet élément d'information puisse être traité. Les informations en ce sens peuvent également s'avérer utiles par rapport à l'enfermement d'une personne. Elles peuvent conduire la police à décider de prévoir des mesures adaptées en cas d'enfermement (surveillance complémentaire, …) dans l'intérêt de la santé de la personne qui fait l'objet d'une privation de liberté administrative ou judiciaire.

Les services de police peuvent dès lors disposer de certaines informations sur la base d'éléments directement obtenus (p.e. : la personne concernée l'a spontanément signalé), ou d'expériences vécues lors de précédentes interventions (p.e. changement d'humeur soudain ou réaction de panique lors de l'enfermement, agression envers d'autres personnes arrêtées, …). Le traitement d'une catégorie de données à caractère personnel tel que prévu à l'article 44/5 [de la loi sur la fonction de police] peut être assorti de mesures à prendre. Cela ne peut toutefois entraîner de mesures discriminatoires ni de mesures excessives de sécurisation (p.e. une tenue de protection trop voyante). Le but est uniquement de permettre aux interventions, planifiées ou non (estimation des risques lorsqu'une personne est transférée en prison ou menée devant un magistrat), de se dérouler en toute sécurité. En particulier, le personnel peut être informé préalablement à l'intervention (p.e. : lorsqu'une équipe d'intervention part effectuer une mission, lors de l'arrestation d'une personne connue, lorsqu'une assistance est fournie à un huissier de justice, …).

Il peut être renvoyé à l'article 2 de la CEDH et à l'obligation positive d'un État de protéger les citoyens lorsqu'il existe une menace réelle contre leur vie (et leur santé). En outre, le législateur prévoit également une possibilité d'obliger un suspect à coopérer à un test sanguin afin de vérifier si une maladie contagieuse a été transmise lors de la commission d'un délit. (articles 524*quater* e.s. Code d'instruction criminelle) » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 13-14).

B.14.3. La proposition de loi à l'origine de la loi attaquée a été inspirée par un avant-projet de loi « relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/003, p. 3).

Dans son avis n° 9/2018 du 12 décembre 2018 sur cet avant-projet de loi, l'Organe de contrôle avait considéré que les termes « dans le but de comprendre le contexte lié à la personne concernée » n'étaient pas suffisamment clairs en ce qu'ils risquaient d'être compris comme renvoyant à des circonstances externes plutôt qu'à l'état de santé de la personne concernée :

« Les possibilités pour les services de police de traiter des données relatives à la santé, outre le caractère complémentaire (et d'appui, […]) du traitement, sont encore réduites par les

termes ‘ et uniquement dans le but de comprendre le contexte lié à la personne concernée, ainsi que pour assurer la sécurité et protéger la santé de toute personne susceptible d’entrer en contact avec les personnes concernées dans le cadre de l’intervention policière. ’ L’auteur du projet doit réfléchir à la question de savoir si tous les traitements de données relatives à la santé réalisés couramment dans la pratique par la police sont ainsi couverts. Le dernier segment (‘ assurer la sécurité et protéger la santé de toute personne susceptible d’entrer en contact avec les personnes concernées dans le cadre de l’intervention policière ’) ne requiert aucune précision, mais vise un cas d’application particulier et vise la protection de tiers (qu’ils soient ou non membres du personnel des services police). Le premier segment (‘ dans le but de comprendre le contexte lié à la personne concernée ’) est par contre sujet à interprétation. Il est ainsi évident que la police doit pouvoir traiter des données relatives à la santé dans le cadre de la constatation de toutes sortes d’infractions contre l’ordre des familles et contre la moralité publique (Livre II, Titre VII du Code pénal), tant concernant un suspect qu’une victime. Il ne s’agit pas tant du ‘ contexte lié à la personne concernée ’ mais simplement par exemple de son état de santé (porteur d’une maladie, patient cardiaque, historique de problèmes psychiatriques, etc.). L’Organe de contrôle estime à cet égard que les termes employés sont dès lors ambigus (il semble plutôt s’agir de circonstances externes), avec toutes les conséquences qui en découlent sur la régularité des futurs actes policiers d’information ou d’instruction, ou de manière plus générale sur la régularité de la procédure. Il semble préférable d’exclure les discussions à ce niveau et il incombe dès lors à l’auteur du projet de clarifier les choses. Cette clarté peut consister simplement à faire référence à la nécessité de traiter des données relatives à la santé pour l’exercice de leurs missions de police administrative ou judiciaire et la protection de la santé de tiers » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/003, p. 40).

B.14.4. En réponse à cette observation, il a été précisé dans les travaux préparatoires :

« Pour répondre à la demande de précision de l’Organe de contrôle sur les traitements des données relatives à la santé point 6 de l’avis n° 9 du 12 décembre 2018), il faut bien comprendre que le contexte lié à la personne concernée s’applique à l’ensemble des missions de police administrative et de police judiciaire et la référence à la ‘ personne concernée ’ vise toutes les catégories de personnes visées à l’article 44/5. Les exemples fournis *supra* [ne] sont aucunement exhaustifs » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, p. 14).

B.14.5. Il ressort des travaux préparatoires cités en B.14.2 que l’article 44/1, § 2, alinéa 2, 2°, de la loi sur la fonction de police a été introduit afin de garantir le déroulement des interventions policières en toute sécurité tant pour la personne concernée et ses proches que pour les personnes qui participent à l’intervention. Par conséquent, la disposition attaquée peut être interprétée en ce sens que les termes « dans le but de comprendre le contexte lié à la personne concernée » portent sur les cas où la sécurité et la santé de la personne concernée elle-

même doivent être garanties, alors que les termes « pour assurer la sécurité et protéger la santé de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention policière » portent sur le fait de garantir la sécurité et la santé des membres du personnel de la police et de toutes les autres personnes qui sont présentes lors de l'intervention, parmi lesquelles d'autres secouristes, les proches de la personne concernée et d'autres personnes présentes.

B.15. Dans cette interprétation, les termes « dans le but de comprendre le contexte lié à la personne concernée » dans l'article 44/1, § 2, alinéa 2, 2°, de la loi sur la fonction de police, inséré par l'article 4, 2°, de la loi attaquée, sont suffisamment clairs afin de permettre à la personne concernée de comprendre les circonstances dans lesquelles un traitement des données à caractère personnel peut avoir lieu.

En ce qu'il est dirigé contre les mots « dans le but de comprendre le contexte lié à la personne concernée », sous réserve de l'interprétation mentionnée en B.14.5, le grief n'est pas fondé.

2) Les données génétiques

B.16.1. En vertu de l'article 26, 12°, de la loi du 30 juillet 2018, les données génétiques sont les « données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou la santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ».

B.16.2. Le traitement des données génétiques par les services de police est soumis aux conditions, citées en B.11.2, applicables à tout traitement de catégories particulières de données en vertu de l'article 44/1, § 2, alinéas 1er et 3, de la loi sur la fonction de police. En outre, en vertu de l'article 44/1, § 2, alinéa 2, 3°, de la loi sur la fonction de police, inséré par l'article 4, 2°, de la loi attaquée, le traitement des données génétiques est défini comme « la collecte des données génétiques et l'enregistrement des mentions administratives liées au profil génétique, à l'exclusion de la comparaison des profils génétiques ou de l'identification du numéro de code

ADN ». La même disposition précise que le traitement des données génétiques ainsi défini s'effectue « dans le cadre de l'exercice des missions de police judiciaire et de l'application de la législation relative à la protection civile ». Selon la partie requérante, ces derniers termes ne sont pas suffisamment précis.

B.16.3. Dans les travaux préparatoires, la disposition attaquée est commentée comme suit :

« Pour finir, concernant les données génétiques, la police se limite à rassembler les traces génétiques (ADN) et le matériel de référence de personnes (loi du 7 novembre 2011 relative à la procédure d'identification au travers de recherche ADN dans des dossiers pénaux) avec les données administratives nécessaires pour la ' *chain of custody* '. La police reçoit des informations sur les traces analysées quant à leur caractère exploitable et les liens potentiels (voir Col 21/2017) » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 14-15).

B.17.1. En ce qu'elle dispose que le traitement des données génétiques par les services de police est limité à la collecte des données génétiques et à l'enregistrement des mentions administratives liées au profil génétique et qu'il s'effectue « dans le cadre de l'exercice des missions de police judiciaire », la disposition attaquée précise que les opérations de traitement précitées ont lieu uniquement dans le cadre de l'exercice, par les services de police, de leurs missions de police judiciaire, à l'exclusion de l'exercice de leurs missions de police administrative.

B.17.2. Les tâches des services de police en matière de protection civile sont délimitées par l'article 17 de la loi sur la fonction de police, lequel dispose :

« En cas de calamité, de catastrophe ou de sinistre au sens de la législation sur la protection civile, les services de police se rendent sur les lieux et avertissent les autorités administratives et judiciaires compétentes.

En attendant l'intervention de ces autorités, ils prennent de commun accord toutes les mesures propres à sauver les personnes en danger, à protéger l'évacuation des personnes et des biens et à empêcher le pillage.

A cette fin, ils peuvent requérir le concours de la population qui est tenue d'obtempérer et de fournir, s'il échet, les moyens nécessaires.

Ils ne quittent les lieux de la calamité, de la catastrophe ou du sinistre qu'après en avoir averti un officier de police administrative et s'être assurés que leur présence n'est plus nécessaire pour exécuter des missions de police administrative et judiciaire ».

L'organisation et les tâches de la protection civile sont en outre réglées par, entre autres, la loi du 15 mai 2007 « relative à la sécurité civile » et par la loi du 31 décembre 1963 « sur la protection civile ».

En ce qu'elle dispose que le traitement des données génétiques par les services de police est limité à la collecte des données génétiques et à l'enregistrement des mentions administratives liées au profil génétique et qu'il s'effectue « dans le cadre […] de l'application de la législation relative à la protection civile », la disposition attaquée autorise dès lors les services de police à collecter des données génétiques et à enregistrer des mentions administratives liées au profil génétique dans le cadre des missions de police administrative et judiciaire qu'ils sont amenés à exercer « en cas de calamité, de catastrophe ou de sinistre au sens de la législation sur la protection civile » en vertu de l'article 17 de la loi sur la fonction de police.

B.17.3. Le législateur a ainsi prévu de manière suffisamment précise les finalités des traitements des données génétiques qui sont susceptibles d'être effectués par les services de police.

Pour le surplus, en vertu de l'article 44/1, § 1er, de la loi sur la fonction de police, les services de police ne peuvent traiter des données génétiques que pour autant que ces données présentent un caractère « adéquat, pertinent et non excessif » au regard de la finalité pour laquelle elles sont obtenues et pour laquelle elles sont traitées ultérieurement. Les services de police sont contrôlés sur ce point par l'Organe de contrôle qui, en vertu de l'article 71, § 1er, alinéa 3, 2°, de la loi du 30 juillet 2018, a notamment pour mission de « contrôler le traitement des informations et des données à caractère personnel visées aux articles 44/1 à 44/11/13 de la loi du 5 août 1992 sur la fonction de police y compris celles incluses dans les banques de données visées à l'article 44/2 de la même loi ».

B.18. En ce qui concerne les termes « dans le cadre de l'exercice des missions de police judiciaire et de l'application de la législation relative à la protection civile », la disposition attaquée satisfait à l'exigence de légalité.

En ce qui concerne le délai de conservation des données biométriques et des données de santé

B.19. La partie requérante allègue, d'une part, que la loi attaquée ne prévoit pas de délai spécifique de conservation pour les données biométriques et, d'autre part, que les délais de conservation des données biométriques et des données de santé sont disproportionnés.

B.20. Il ressort de la jurisprudence de la Cour européenne des droits de l'homme et de celle de la Cour de justice que les données à caractère personnel ne peuvent pas être conservées plus longtemps que nécessaire pour la réalisation de la finalité pour laquelle elles ont été enregistrées sous une forme qui permette l'identification ou qui permette d'établir un lien entre une personne et des faits infractionnels. Pour apprécier la proportionnalité de la durée de conservation par rapport à l'objectif pour lequel les données ont été enregistrées, il est tenu compte de l'existence ou non d'un contrôle indépendant concernant la justification de la conservation des données dans les banques de données sur la base de critères précis, tels que la gravité des faits, le fait que la personne concernée a déjà fait l'objet dans le passé d'une arrestation, la force des soupçons qui pèsent sur une personne et toute autre circonstance particulière (CEDH, grande chambre, 4 décembre 2008, *S. et Marper c. Royaume Uni*, § 103; 18 avril 2013, *M.K. c. France*, § 35; 17 décembre 2009, *B.B. c. France*, § 61; 18 septembre 2014, *Brunet c. France*, §§ 35-40; grande chambre, 25 mai 2021, *Centrum för rättvisa c. Suède*, § 275; grande chambre, 25 mai 2021, *Big Brother Watch c. Royaume-Uni*, § 361; CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, points 137-139).

L'article 5, point *e)*, de la Convention n° 108 et l'article 7 de la recommandation n° R (87) 15 prévoient des garanties similaires.

B.21.1. Les articles 44/9 et 44/10 de la loi sur la fonction de police, tels qu'ils ont été modifiés par les articles 10 et 11 de la loi attaquée, fixent les règles relatives à la durée de

conservation des données à caractère personnel et des informations enregistrées dans la B.N.G., ainsi que les règles relatives à l'archivage de ces données et informations à l'expiration de cette période.

L'article 44/11/2 de cette loi, tel qu'il a été modifié par l'article 13 de la loi attaquée, fixe les règles relatives à la conservation des données contenues dans les banques de données de base.

B.21.2. En vertu de l'article 44/2 de la loi sur la fonction de police, les données à caractère personnel et les informations qui sont traitées dans la B.N.G. et dans les banques de données de base sont celles qui sont visées à l'article 44/1 de la même loi, et donc y compris les catégories particulières de données visées à l'article 44/1, § 2.

B.21.3. La directive « police » n'impose pas aux États membres d'adopter des délais de conservation spécifiques pour les catégories particulières de données.

B.21.4. La partie requérante ne démontre pas que le choix effectué par le législateur de ne pas prévoir de délai de conservation spécifique pour les catégories particulières de données, serait déraisonnable ou entraînerait une conservation de données qui serait disproportionnée aux objectifs qu'il poursuit, lesquels sont expliqués, par catégorie de délai de conservation, dans les travaux préparatoires de la loi du 18 mars 2014 « relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle » (*Doc. parl.*, Chambre, 2013-2014, DOC 53-3105/001, pp. 37-43; voir l'arrêt n° 108/2016 du 14 juillet 2016, B.112.3). Dès lors qu'en vertu de l'article 44/1, § 2, alinéa 1er, de la loi sur la fonction police, les catégories particulières de données à caractère personnel sont traitées en complément ou en soutien du traitement principal portant sur d'autres catégories de données, le législateur n'a pas agi de manière déraisonnable en soumettant les catégories particulières de données à caractère personnel aux mêmes délais de conservation que ceux qui sont applicables aux catégories de données principales qu'elles complètent ou soutiennent.

B.21.5. Pour le surplus, par son arrêt n° 108/2016 du 14 juillet 2016, la Cour a jugé que, sous réserve des interprétations indiquées en B.113.2, B.113.3, B.114.2, B.114.4, B.115.3,

B.115.4 et B.115.8 de cet arrêt, les articles 44/9, 44/10 et 44/11/2 de la loi sur la fonction de police respectent les conditions mentionnées en B.20 quant à la durée de conservation des données à caractère personnel dans des banques de données policières (B.109 à B.116). En l'espèce, il n'y a pas lieu de conclure autrement.

B.22. Les griefs formulés en B.19 ne sont pas fondés.

En ce qui concerne les garanties pour la personne concernée

B.23. La partie requérante allègue que la disposition attaquée est contraire aux dispositions visées dans le moyen en ce qu'elle ne prévoit pas de conditions plus strictes pour l'accès aux données biométriques, aux données de santé et aux données génétiques (premier grief), ni l'interdiction de transmettre ces données (deuxième grief), ni de limiter la collecte des données génétiques « à celles en rapport avec la personne concernée » (troisième grief).

En ce qui concerne les données de santé, la partie requérante critique en outre le fait que la disposition attaquée ne prévoit pas l'obligation de distinguer les données fondées sur des faits et celles qui sont fondées sur des appréciations personnelles (quatrième grief), l'obligation pour le responsable du traitement d'établir « des catégories en fonction du degré d'exactitude ou de fiabilité des informations qu'il traite » (cinquième grief), l'obligation de vérifier l'exactitude des données avant leur transmission ou leur mise à disposition (sixième grief), l'obligation de fournir à l'autorité compétente destinataire les informations lui permettant de s'assurer de l'exactitude des données et de leur niveau de mise à jour (septième grief), des critères précis d'évaluation de la qualité des données (huitième grief), une procédure de validation assortie d'un avertissement actif de l'Organe de contrôle (neuvième grief), l'obligation d'effectuer une analyse d'impact préalable (dixième grief) ainsi que l'autorisation préalable de l'Organe de contrôle avant tout accès à ces données (onzième grief).

Enfin, la partie requérante estime que le traitement de données génétiques et biométriques nécessite des exigences de sécurisation plus strictes (douzième grief).

B.24. Selon l'article 6 de la Convention n° 108, les données à caractère personnel relatives à la santé ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées.

L'article 9 de cette Convention dispose néanmoins qu'il est possible de déroger à l'article 6 lorsqu'une telle dérogation est prévue par la loi et qu'elle constitue, dans une société démocratique, une mesure nécessaire à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État, à la répression des infractions pénales, à la protection de la personne concernée ou aux droits et libertés d'autrui.

Selon la recommandation n° R (87) 15, les données sensibles ne peuvent être traitées que si un tel traitement est absolument nécessaire pour les besoins d'une enquête déterminée.

Ni la Convention n° 108, ni la recommandation n° R (87) 15 ne font par conséquent obstacle au traitement de données sensibles par les services de police lorsqu'un tel traitement est strictement nécessaire à l'exercice de leurs missions.

B.25.1. Comme il est dit en B.11.2, le traitement de toute donnée sensible, quelle que soit la catégorie dont elle relève, qui est effectué par les services de police est soumis aux garanties prévues par l'article 44/1, § 2, alinéas 1er et 3, de la loi sur la fonction de police, ainsi que, conformément à l'article 44/3, § 1er, alinéa 1er, de la même loi, à celles qui sont prévues par la loi du 30 juillet 2018.

Les travaux préparatoires indiquent :

« Comme le rappelle le considérant 37 de la Directive, il convient d'apporter des garanties appropriées pour l'ensemble des données traitées dans le cadre de cet article 4. Une des garanties appropriées consiste bien entendu à ne traiter ces données qu'en complément d'autres données traitées dans le cadre des missions opérationnelles.

Ensuite, les garanties entourant le traitement des données dites sensibles qui étaient mentionnées dans l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements ont été intégralement reprises dans le 44/1, § 2*bis*, alinéa 5, à savoir le fait que :

- la liste des catégories de personnes, ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description de leur fonction par rapport au traitement des données visées;

- la liste des catégories des personnes ainsi désignées pour traiter les données visées dans ce paragraphe est tenue à la disposition de l'Organe de contrôle par le responsable du traitement ou, le cas échéant, par le sous-traitant;

- les personnes désignées sont tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

Trois garanties supplémentaires en matière de protection des droits des personnes concernées ont été ajoutées.

Il s'agit tout d'abord, de faire une distinction entre les catégories de personnes visées à l'article 44/5. De la sorte, les systèmes de traitement des données devront par exemple clairement indiquer si les données relatives aux opinions politiques qui sont traitées concernent un suspect ou une victime qui serait persécutée précisément en raison de celles-ci.

Ensuite, des mesures techniques et organisationnelles doivent être prises contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification ou tout autre traitement non autorisé de ces données. Ces mesures sont très larges et couvrent notamment la sécurité des accès physiques aux locaux où ces données sont traitées et les accès aux données. À titre illustratif, les laboratoires de la police où des données biométriques sont traitées font l'objet de règles de sécurité d'accès physiques ainsi qu'aux données traitées.

Enfin, il est demandé aux responsables du traitement d'indiquer dans leur politique de protection des données les mesures concrètes qu'ils vont prendre pour assurer le suivi de ces catégories de données.

Les délégués à la protection des données compétents assureront le suivi de la mise en œuvre de cette politique dont le respect des mesures prévues pour le traitement des données sensibles. Ils réalisent pour cela, par exemple, des contrôles ciblés sur ces mesures ou généraux sur l'ensemble des points de la politique de sécurité.

Une délégation est réalisée vers le Roi qui pourra prendre d'autres mesures appropriées. Concernant l'avis du Conseil d'État 65.312/2 du 4 mars 2019 sur ce point, il est précisé dans la loi que les garanties que le Roi peut apporter sont complémentaires à celles qui sont déjà prévues dans cet article. Il ne saurait bien entendu pas être question pour le Roi de revoir à la baisse les garanties énoncées par cet article en matière de traitement de catégories particulières de données à caractère personnel mais bien de les renforcer en les complétant si besoin » (*Doc. parl*., Chambre, 2018-2019, DOC 54-3697/001, pp. 15-16).

B.25.2. En vertu de l'article 44/1, § 1er, de la loi sur la fonction de police, les services de police peuvent traiter des informations et des données à caractère personnel pour autant que ces dernières présentent, notamment, un caractère « pertinent et non excessif ». Compte tenu des dispositions précitées de la Convention n° 108, cette disposition doit être comprise en ce sens qu'un traitement des données sensibles n'est possible que s'il est strictement nécessaire à l'exercice des missions confiées aux services de police.

B.25.3.1. En ce que la partie requérante allègue que la disposition attaquée ne prévoit pas des conditions d'accès plus strictes aux données biométriques, aux données de santé et aux données génétiques et une interdiction de transmettre ces données, elle se prévaut du considérant 37 de la directive « police », cité en B.10.1, selon lequel les garanties appropriées pour les droits et des libertés de la personne concernée par un traitement de catégories particulières de données « pourraient comprendre […] des règles plus strictes pour l'accès du personnel de l'autorité compétente aux données et l'interdiction de la transmission de ces données ».

En ce qu'elle allègue que la disposition attaquée ne prévoit pas de limiter la collecte des données génétiques « à celles en rapport avec la personne concernée », elle semble se référer à un autre extrait du même considérant selon lequel les garanties appropriées pour les droits et des libertés de la personne concernée par un traitement de catégories particulières de données « pourraient comprendre la possibilité de ne collecter ces données qu'en rapport avec d'autres données relatives à la personne physique concernée ».

B.25.3.2. La Cour n'est pas compétente pour contrôler des normes législatives au regard du principe d'égalité et de non-discrimination, lu en combinaison seulement avec les considérants du préambule qui précède les dispositions d'une directive de l'Union européenne, étant donné que ces considérants n'ont aucune force obligatoire. Ces considérants ne sont qu'un outil permettant d'interpréter les dispositions normatives de cette directive.

B.25.3.3. Le moyen unique, en sa première branche, premier à troisième griefs, est irrecevable.

B.25.4. En ce qu'il n'expose pas en quoi le fait que la disposition attaquée ne prévoit pas de « catégories en fonction du degré d'exactitude ou de fiabilité des informations que [le responsable du traitement] traite » serait incompatible avec les dispositions visées dans le moyen, le cinquième grief ne satisfait pas aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, citées en B.2.4.1, et n'est dès lors pas recevable.

B.25.5. Le moyen unique, en sa première branche, quatrième, sixième et septième griefs, n'est pas fondé, étant donné que ces aspects sont réglés à l'article 32 de la loi du 30 juillet 2018. La distinction entre les données fondées sur des faits et celles qui sont fondées sur des appréciations personnelles, qui est visée à l'article 32, § 1er, de la loi du 30 juillet 2018, est en outre renforcée en ce qui concerne les données de santé par l'article 44/1, § 2, alinéa 2, 2°, de la loi sur la fonction de police, inséré par l'article 4, 2°, de la loi attaquée. Cette dernière disposition prévoit en effet que « lorsque des données relatives à la santé sont traitées, il est mentionné si ces données proviennent ou non de professionnels de soins de la santé ».

B.25.6. En vertu de l'article 44/1, § 1er, de la loi sur la fonction de police, les services de police ne peuvent traiter les données à caractère personnel que pour autant que celles-ci soient « adéquates ». Cette condition a pour effet que les données à caractère personnel qui sont traitées doivent permettre, dans la mesure du possible, de se former une idée correcte de la personne qu'elles concernent, de sorte qu'il n'est pas permis, notamment, de manipuler les informations disponibles en traitant seulement les aspects qui sont défavorables à l'intéressé.

L'article 28 de la loi du 30 juillet 2018 dispose par ailleurs que les données à caractère personnel doivent être traitées « de manière licite et loyale » et qu'elles doivent être « exactes et, si nécessaire, mises à jour ». En ce qui concerne ce dernier point, l'article 28, 4°, de cette loi prévoit encore que « toutes les mesures raisonnables sont 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 ».

En ce qui concerne spécialement les catégories particulières de données, les responsables du traitement indiquent dans leur politique de protection des données, en vertu de l'article 44/1, § 2, alinéa 3, 6°, de la loi sur la fonction de police, inséré par l'article 4, 2°, de la loi attaquée,

les actions à mener pour protéger le traitement des catégories particulières de données et pour assurer la qualité des données traitées notamment quant aux aspects liés à l'évaluation de leur exactitude, de leur exhaustivité, de leur fiabilité et de leur niveau de mise à jour. Cette précision a été ajoutée par un amendement n° 3 qui a été justifié comme suit :

« L'évaluation de la qualité des données traitées, en particulier lorsqu'il s'agit de catégories de données particulières est un élément très important tant au niveau opérationnel qu'au niveau de la protection des données à caractère personnel. Il appartient aux responsables du traitement de donner des critères et des directives pour apprécier la qualité des données traitées et donc d'encadrer leur utilisation. Les délégués à la protection des données veillent par des actions concrètes à assurer le suivi de ces directives » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/005, p. 4. Voir aussi : DOC 54-3697/006, pp. 4 et 7).

Le législateur a ainsi prévu de manière suffisamment précise les exigences de qualité auxquelles les catégories particulières de données doivent satisfaire pour pouvoir être traitées par les services de police.

Le moyen unique, en sa première branche, huitième grief, n'est pas fondé.

B.25.7. La partie requérante ne démontre pas en quoi le fait que le législateur n'ait pas prévu de procédure de validation assortie d'un avertissement actif de l'Organe de contrôle aurait pour effet que le traitement des données de santé ne serait pas accompagné de garanties appropriées. Le moyen unique, en sa première branche, neuvième grief, n'est pas fondé.

B.25.8. Les articles 58 et 59 de la loi du 30 juillet 2018 déterminent, conformément aux articles 27 et 28 de la directive « police », les cas dans lesquels une analyse d'impact et/ou une consultation de l'Organe de contrôle, préalables au traitement de données à caractère personnel, doivent avoir lieu.

En vertu de l'article 58 et de l'article 59, § 1er, alinéa 1er, 1°, de la loi du 30 juillet 2018, le responsable du traitement doit effectuer une analyse d'impact relative à la protection des données avant un traitement lorsque le type de traitement « en particulier par le recours aux nouvelles technologies » est susceptible d'engendrer un risque élevé pour les droits et libertés

des personnes physiques et, lorsque l'analyse d'impact indique que le traitement présenterait un risque élevé, le responsable du traitement ou son sous-traitant doit consulter l'Organe de contrôle préalablement au traitement « qui fera partie d'un nouveau fichier à créer ».

En vertu de l'article 59, § 1er, alinéa 1er, 2°, de la loi du 30 juillet 2018, le responsable du traitement ou son sous-traitant doit par ailleurs consulter d'office l'Organe de contrôle préalablement au traitement « qui fera partie d'un nouveau fichier à créer » lorsque le type de traitement « en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures » présente des risques élevés pour les libertés et les droits des personnes concernées.

En vertu de l'article 59, § 2, de la loi du 30 juillet 2018, l'Organe de contrôle peut établir une liste des opérations de traitement devant faire l'objet d'une consultation préalable.

Compte tenu du caractère sensible des données de santé, toute opération de traitement de ces données effectuée par les services de police présente des risques élevés pour les droits et libertés des personnes concernées. Par conséquent, la consultation préalable de l'Organe de contrôle est requise avant tout traitement de ces données « qui fera partie d'un nouveau fichier à créer » en vertu de l'article 59, § 1er, alinéa 1er, 2°, de la loi du 30 juillet 2018.

Le moyen unique, en sa première branche, dixième et onzième griefs, n'est pas fondé.

B.25.9. En ce qui concerne les exigences de sécurisation des données, le responsable du traitement et le sous-traitant doivent, en vertu de l'article 60, § 1er, de la loi du 30 juillet 2018, mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données.

L'article 44/1, § 2, alinéa 3, 5°, de la loi sur la fonction de police, inséré par l'article 4, 2°, de la loi attaquée, prévoit en outre que « des mesures techniques ou organisationnelles appropriées sont adoptées pour protéger les [catégories particulières de] données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi

que contre la modification ou tout autre traitement non autorisé de ces données ». Lors des travaux préparatoires, outre l'extrait cité en B.23.1, il a également été dit :

« Le texte impose une politique de sécurité active au niveau de ces données, chaque responsable du traitement étant chargé de faire un plan en matière de protection des données » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/003, p. 7).

Le moyen unique, en sa première branche, douzième grief, n'est pas fondé.

B.25.10. Comme il est dit en B.11.2, le Roi peut, en vertu de l'article 44/1, § 2, alinéa 4, de la loi sur la fonction de police, entourer le traitement des catégories particulières de données d'autres garanties complémentaires appropriées, en plus de celles qui sont prévues par l'alinéa 3 du même article. Dans les travaux préparatoires, il a été précisé :

« Il ne saurait bien entendu pas être question pour le Roi de revoir à la baisse les garanties énoncées par cet article en matière de traitement de catégories particulières de données à caractère personnel mais bien de les renforcer en les complétant si besoin » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, p. 16).

B.26. Les griefs formulés en B.23 ne sont pas fondés.

En ce qui concerne le droit d'accès aux catégories particulières de données et le droit à un recours effectif

B.27. La partie requérante allègue que la disposition attaquée ne prévoit pas que la personne concernée dispose d'un droit d'accès direct aux catégories particulières de données qui la concernent auprès du responsable du traitement, ce qui la prive du droit à un recours effectif. Selon la partie requérante, la loi attaquée serait entachée d'une lacune dès lors qu'elle ne contient pas de disposition spécifique visant à limiter le droit d'accès direct aux données conformément à l'article 38, § 2, de la loi du 30 juillet 2018. L'exercice indirect du droit d'accès par l'intermédiaire de l'Organe de contrôle en vertu de l'article 42 de la loi du 30 juillet 2018 ne permettrait pas davantage à la personne concernée de disposer d'une voie de recours effective, dès lors que l'Organe de contrôle indique uniquement à celle-ci qu'il a procédé aux « vérifications nécessaires ».

B.28.1. Le Conseil des ministres conteste la recevabilité *ratione temporis* du grief. Il fait valoir que le recours en annulation est en réalité dirigé contre le titre II de la loi du 30 juillet 2018 et que le délai de six mois pour introduire un recours en annulation de ces dispositions a expiré.

B.28.2. Pour satisfaire aux exigences de l'article 3, § 1er, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, un recours en annulation doit être introduit dans le délai de six mois suivant la publication de la norme attaquée.

Lorsque, dans une législation nouvelle, le législateur reprend une disposition ancienne et s'approprie de cette manière son contenu, un recours peut être introduit contre la disposition reprise, dans les six mois de sa publication.

Toutefois, lorsque le législateur se limite à une intervention purement légistique ou linguistique ou à une coordination de dispositions existantes, il n'est pas censé légiférer à nouveau et les griefs sont irrecevables *ratione temporis*, en ce qu'ils sont en réalité dirigés contre les dispositions qui existaient déjà antérieurement.

Il convient dès lors de vérifier si le recours est dirigé contre des dispositions nouvelles ou s'il concerne des dispositions non modifiées.

B.28.3. Par la disposition attaquée, le législateur a déterminé le cadre légal applicable aux traitements des catégories particulières de données à caractère personnel effectués par les services de police. Toutefois, cette disposition règle uniquement le traitement des données à caractère personnel, mais pas les droits de la personne concernée. Ce dernier aspect est réglé par l'article 42 de la loi du 30 juillet 2018, lequel n'a pas été modifié par la loi attaquée du 22 mai 2019. Lors de l'adoption de la disposition attaquée, le législateur ne s'est aucunement approprié le contenu de l'article 42 de la loi du 30 juillet 2018 et n'a pas non plus eu l'intention de légiférer à nouveau sur cette matière.

B.28.4. Par conséquent, le moyen, en sa première branche, est irrecevable en ce qu'il porte sur les droits de la personne concernée.

Quant à l'interconnexion des banques de données policières (article 44/4 de la loi sur la fonction de police)

B.29. Dans la deuxième branche du moyen unique, la partie requérante allègue que l'article 44/4 de la loi sur la fonction de police, tel qu'il a été remplacé par l'article 7 de la loi attaquée, n'est pas compatible avec les normes de référence mentionnées en B.3, en ce qu'il méconnaît le principe de la légalité, l'exigence de prévisibilité et le principe de proportionnalité et en ce qu'il ne prévoit ni la consultation préalable de l'Organe de contrôle, ni l'obligation de notifier aux destinataires des données communiquées dans le cadre d'une interconnexion que celles-ci ont fait l'objet d'une rectification ou d'un effacement.

B.30. À la suite de son remplacement par l'article 7 de la loi attaquée, l'article 44/4 de la loi sur la fonction de police dispose :

« § 1er. En matière de police administrative, le responsable du traitement des données à caractère personnel et des informations visées à l'article 44/1, y compris celles incluses dans les banques de données visées à l'article 44/2, § 1er, alinéa 2, 1° et 2°, est le ministre de l'Intérieur.

En matière de police judiciaire, le responsable du traitement des données à caractère personnel et des informations visées à l'article 44/1, y compris celles incluses dans les banques de données visées à l'article 44/2, § 1er, alinéa 2, 1° et 2°, est le ministre de la Justice.

Pour ce qui concerne les banques de données visées à l'article 44/2, § 1er, alinéa 2, 3°, les chefs de corps, le commissaire général, les directeurs généraux ou les directeurs qui ont fixé les objectifs et les moyens relatifs à ces banques de données particulières sont les responsables du traitement.

§ 2. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences et sans préjudice des compétences propres des autorités judiciaires, déterminent par directives contraignantes les mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2.

Les fichiers de journalisation sont établis dans les banques de données visées à l'article 44/2 au moins pour les traitements suivants : la collecte, la modification, la consultation, la communication, y compris les transferts, l'archivage, l'interconnexion et l'effacement.

Les fichiers de journalisation de consultation et de communication permettent d'établir :

1° le motif, la date et l'heure de ces traitements;

2° les catégories de personnes qui ont consulté les données à caractère personnel, ainsi que l'identification de la personne qui a consulté ces données;

3° les systèmes qui ont communiqué ces données;

4° les catégories de destinataires des données à caractère personnel, et si possible, l'identité des destinataires de ces données.

Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres après avis de l'Organe de contrôle, d'autres types de traitements pour lesquels les fichiers de journalisation sont établis.

Des mesures appropriées sont adoptées pour assurer la sécurité des fichiers de journalisation et, en particulier, pour empêcher tout traitement non autorisé et pour assurer l'intégrité des données traitées.

Les procédures d'accès aux fichiers de journalisation garantissent la nécessité et la proportionnalité de l'accès aux données de journalisation en vue d'atteindre les finalités visées à l'article 56, § 2, de la loi relative à la protection des données.

Ces procédures sont soumises à l'avis de l'Organe de contrôle.

Les chefs de corps pour la police locale et le commissaire général, les directeurs généraux et les directeurs pour la police fédérale sont les garants de la bonne exécution de ces directives en ce qui concerne les banques de données visées à l'article 44/2, §§ 1er, et 3.

Le gestionnaire, désigné en droit ou dans les faits est le garant de la bonne exécution de ces directives en ce qui concerne les banques de données visées à l'article 44/2, § 2.

§ 3. Sans préjudice des compétences des autorités judiciaires, les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante, publiée au *Moniteur belge*, les règles d'accès des membres des services de police aux banques de données visées à l'article 44/2, §§ 1er, et 3.

§ 4. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante publiée au *Moniteur belge*, les modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique.

Ces directives déterminent au moins, sur la base du caractère pertinent, adéquat et non excessif, les catégories de banques de données qui peuvent être connectées entre elles, les modalités relatives à l'interconnexion et les règles d'accès des membres des services de police relatives à l'existence d'une information pertinente au sein de ces banques de données interconnectées ou, le cas échéant, aux données elles-mêmes ainsi qu'aux traitements qui en résultent.

§ 5. Les profils et les modalités d'accès visés aux §§ 3 et 4 sont déterminés notamment sur la base :

1° du besoin d'en connaître, en ce compris de la nécessité de croiser ou coordonner les données traitées;

2° des finalités légales de chaque banque de données;

3° des différentes catégories de personnes visées à l'article 44/5;

4° de l'évaluation des données;

5° de l'état de validation des données traitées.

Les accès visés aux §§ 3 et 4 doivent être conçus à la base ou par défaut de telle sorte que les données évaluées et validées apparaissent de manière claire et puissent être exploitées prioritairement.

Les profils d'accès et l'identification des personnes ayant accès sont tenus à la disposition de l'Organe de contrôle.

§ 6. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante publiée au *Moniteur belge* les mesures adéquates, pertinentes et non excessives relatives à l'interconnexion ou la corrélation des banques de données techniques visées à l'article 44/2, § 3, avec les banques de données visées à l'article 44/2, §§ 1er et 2, ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique.

Cette directive tient compte des critères de temps, d'espace et de fréquence des interconnexions et corrélations. Elles déterminent au moins l'autorité qui permet ce genre de mesures, ainsi que les banques de données qui peuvent être connectées entre elles ».

B.31.1. Lorsque l'exercice des missions de police administrative et de police judiciaire nécessite que les services de police structurent les données à caractère personnel et les informations de sorte qu'elles puissent être directement retrouvées, celles-ci sont traitées dans une banque de données policière opérationnelle (article 44/2, alinéa 1er, de la loi sur la fonction de police). La loi sur la fonction de police prévoit trois catégories de banques de données policières opérationnelles : (1) la B.N.G., (2) les banques de données de base et (3) les banques de données particulières (article 44/2, alinéa 2).

La loi sur la fonction de police prévoit, en outre, deux autres catégories de banques de données policières : les banques de données communes (article 44/2, § 2, de la loi sur la fonction de police) et les banques de données techniques (article 44/2, § 3, de la loi sur la fonction de police).

B.31.2. En vertu de l'article 44/7 de la loi sur la fonction de police, la B.N.G. est la banque de données policière qui contient les données et les informations dont l'ensemble des services de police ont besoin pour exercer leurs missions. Elle est par conséquent une banque de données nationale (*Doc. parl.*, Chambre, 2013-2014, DOC 53-3105/001, p. 7), dont les données et les informations proviennent des divers services de police.

Les banques de données de base sont les banques de données policières créées au profit de l'ensemble de la police intégrée et « qui ont pour finalité d'exécuter les missions de police administrative et de police judiciaire en exploitant les données à caractère personnel et informations qui y sont incluses et en informant les autorités compétentes de l'exercice de ces missions » (article 44/11/2, § 1er, de la loi sur la fonction de police).

Les banques de données particulières sont des banques de données que peuvent créer, pour des besoins particuliers, les chefs de corps, le commissaire général, les directeurs généraux et les directeurs, dans des circonstances spécifiques et pour l'exercice de leurs missions et finalités de police administrative et de police judiciaire (article 44/11/3 de la loi sur la fonction de police, tel qu'il a été modifié par l'article 14, 1°, de la loi attaquée). L'article 44/11/3, § 2, de la loi sur la fonction de police définit les besoins particuliers qui peuvent motiver la création d'une banque de données particulière. Sont visées les banques de données « qui contiennent des données ou informations classifiées; celles dont tout ou partie des données ne peuvent pas être centralisées dans la B.N.G. pour des raisons techniques (par exemple, la difficulté technique d'intégrer des représentations d'œuvres d'art perdues ou volées) ou fonctionnelles (par exemple, les banques de données relatives aux phénomènes de police judiciaire ou de police administrative dont les fonctionnalités ne sont pas (toutes) disponibles dans la B.N.G.) ou encore celles qui ne revêtent qu'un intérêt local » (*Doc. parl.*, Chambre, 2013-2014, DOC 53-3105/001, pp. 7-8).

Lorsque l'exercice conjoint, par tout ou partie des autorités, organes, organismes, services, directions ou commission visés à l'article 44/11/3*ter*, chacun dans le cadre de ses compétences légales, des missions de prévention et de suivi du terrorisme ou de l'extrémisme, lorsqu'il peut mener au terrorisme, nécessite que ceux-ci structurent les données à caractère personnel et les informations relatives à ces missions afin qu'elles puissent être directement retrouvées, ces

données à caractère personnel et ces informations sont traitées dans une ou plusieurs banques de données communes (article 44/2, § 2, de la loi sur la fonction de police).

Lorsque, dans le cadre de l'exercice des missions de police administrative et judiciaire, des outils techniques sont utilisés pour collecter automatiquement des données à caractère personnel et des informations de nature technique, structurées de telle sorte qu'elles puissent être directement retrouvées, ces données sont traitées dans une banque de données technique (article 44/2, § 3, de la loi sur la fonction de police).

B.31.3. L'article 44/4, § 1er, de la loi sur la fonction de police, inséré par l'article 7 de la loi attaquée, désigne le responsable du traitement des données à caractère personnel traitées par les services de police. Le ministre de l'Intérieur est ainsi le responsable du traitement pour les données et informations traitées en matière de police administrative. Le ministre de la Justice est le responsable du traitement pour les données et informations traitées en matière de police judiciaire. Ils sont conjointement responsables lorsque les données sont traitées dans le cadre de ces deux finalités (*Doc. parl*., Chambre, 2018-2019, DOC 54-3697/001, p. 17).

En ce qui concerne les banques de données, le ministre de l'Intérieur ou le ministre de la Justice est le responsable du traitement, selon la finalité de police administrative ou judiciaire concernée, pour les données et informations incluses dans la B.N.G. et dans les banques de données de base. Les chefs de corps, le commissaire général, les directeurs généraux ou les directeurs qui ont fixé les objectifs et les moyens relatifs aux banques de données particulières sont les responsables de traitement pour les données et informations incluses dans les banques de données particulières.

Les travaux préparatoires indiquent :

« La désignation claire d'un responsable du traitement est la clef de voûte permettant d'articuler tout le système d'application des principes de protection des données, qui reposent en grande partie sur les options et les directives prises par les responsables du traitement » (*Doc. parl*., Chambre, 2018-2019, DOC 54-3697/001, p. 18).

B.31.4. En vertu de l'article 44/4, § 2, alinéa 2, de loi sur la fonction de police, inséré par l'article 7 de la loi attaquée, et de l'article 56, § 1er, de la loi du 30 juillet 2018, des fichiers de

journalisation sont établis dans les banques de données policières au moins pour les traitements énumérés à l'article 44/4, § 2, alinéa 2, dont celui de l'interconnexion. Ces fichiers de journalisation permettent de déterminer : 1° le motif, la date et l'heure de ces traitements; 2° les catégories de personnes qui ont consulté les données à caractère personnel, ainsi que l'identification de la personne qui a consulté ces données; 3° les systèmes qui ont communiqué ces données; 4° les catégories de destinataires des données à caractère personnel, et si possible, l'identité des destinataires de ces données (article 44/4, § 2, alinéa 3).

Les fichiers de journalisation correspondent ainsi à « un répertoire qui permet de rendre compte des différents traitements effectués sur des données des différentes entités contenues dans une banque de données » en identifiant notamment la personne qui a réalisé le traitement :

« Lorsqu'il s'agit d'établir des journaux relatifs aux traitements effectués dans les banques de données policières opérationnelles, ceux-ci doivent en principe permettre non seulement d'identifier la catégorie de personne qui a réalisé les traitements mais aussi d'identifier la personne qui a réalisé les traitements visés. Il peut s'agir d'une identification directe dans le cas où l'identité d'un membre du personnel des services de police est directement enregistrée dans les journaux ou via un identifiant unique, connu des services de police qui permet de relier une personne à un code (par exemple via un numéro de matricule) ou indirecte dans l'hypothèse où un code chiffré individuel est attribué à la personne qui traite (par exemple consulte) les données dans l'hypothèse où son identité réelle doit être protégée. Dans ce dernier cas, seul le service d'origine de cette personne et l'autorité de contrôle compétente sont alors capables *in fine* d'identifier une personne physique.

Cependant, lorsque des données issues de ces mêmes banques de données sont transmises vers un destinataire, l'identification de ce destinataire n'est possible que lorsqu'il s'agit d'une personne physique clairement identifiée. Si cette communication ou ce transfert concerne une personne morale ou ' un *single point of contact* technique ' (SPOC), chargé d'assurer le dispatching en interne de son organisation, les fichiers de journaux de la police ne contiendront qu'une trace de l'envoi vers cette personne morale ou ce SPOC technique. Il s'agira bien entendu dans ce cas pour ce destinataire de prendre les mesures techniques et organisationnelles requises et par exemple de pouvoir à son tour tracer via des fichiers de journaux l'utilisation des données qui sera subséquemment réalisée » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 19-20).

L'article 44/4, § 2, alinéa 5, de la loi sur la fonction de police prévoit que des mesures appropriées doivent être adoptées afin d'assurer la sécurité des fichiers de journalisation, l'intégrité des données des fichiers de journalisation étant particulièrement importante dans le cadre du contrôle de la licéité des traitements (*ibid.*, p. 20).

En vertu de l'article 56, § 3, de la loi du 30 juillet 2018, le responsable du traitement et le sous-traitant mettent les fichiers de journalisation à la disposition de l'Organe de contrôle, sur demande de celui-ci.

B.31.5. En vertu de l'article 44/4, § 2, alinéa 1er, de la loi sur la fonction de police, inséré par l'article 7 de la loi attaquée, les ministres de l'Intérieur et de la Justice, chacun dans le cadre de ses compétences, déterminent au moyen de « directives contraignantes » les mesures nécessaires en vue d'assurer la gestion et la sécurité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2, c'est-à-dire dans les banques de données policières opérationnelles, dans les banques de données communes et dans les banques de données techniques.

En vertu de l'article 44/4, § 3, § 4, alinéa 1er, et § 6, de la loi sur la fonction de police, inséré par l'article 7 de la loi attaquée, les mêmes ministres déterminent par « directive générale et contraignante publiée au *Moniteur belge* », (1) les règles d'accès des membres des services de police aux banques de données policières opérationnelles et aux banques de données techniques (article 44/4, § 3), (2) les modalités relatives à l'interconnexion des banques de données policières entre elles ou avec d'autres banques de données auxquelles les services de police ont accès (article 44/4, § 4, alinéa 1er), ainsi que (3) les mesures adéquates, pertinentes et non excessives relatives à l'interconnexion ou à la corrélation des banques de données techniques avec les banques de données policières opérationnelles et les banques de données communes, ou avec d'autres banques de données auxquelles les services de police ont accès (article 44/4, § 6).

B.32.1. Le Conseil des ministres soulève l'irrecevabilité de la deuxième branche du moyen unique pour tardiveté, au motif que l'article 7 de la loi attaquée introduit, dans l'article 44/4 de la loi sur la fonction de police, des modifications d'ordre purement légistique.

B.32.2. Comme il est dit en B.28.2, il convient de vérifier si le recours est dirigé contre des dispositions nouvelles ou s'il concerne des dispositions non modifiées.

B.32.3. Les griefs de la partie requérante sont principalement dirigés contre les paragraphes 3 et 4 de l'article 44/4 de la loi sur la fonction de police, insérés par l'article 7 de la loi attaquée.

Le paragraphe 3 de l'article 44/4 introduit une règle qui n'existait pas dans l'article 44/4 de la loi sur la fonction de police tel qu'il était applicable avant sa modification par l'article 7 de la loi attaquée.

Par ailleurs, le paragraphe 4 de l'article 44/4 de la loi sur la fonction de police reprend en partie le contenu de l'ancien paragraphe 3 de l'article 44/4 de la loi sur la fonction de police (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, p. 21). Par un amendement n° 5 déposé lors de la discussion en commission, le terme « directive » envisagé dans la proposition de loi initiale a été remplacé par les termes « directive générale et contraignante publiée au *Moniteur belge* » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, p. 57; DOC 54-3697/005, p. 6; DOC 54-3697/006, pp. 4 et 8). Par cette modification, le législateur a exprimé sa volonté de légiférer à nouveau à propos de la règle visée à l'article 44/4, § 4, de la loi sur la fonction de police, tel qu'il a été inséré par l'article 7 de la loi attaquée.

L'exception est rejetée.

En ce qui concerne l'habilitation conférée aux ministres de l'Intérieur et de la Justice pour déterminer les règles d'accès aux banques de données policières et les modalités d'interconnexion de celles-ci

B.33. Selon la partie requérante, la disposition attaquée méconnaît le principe de légalité en ce que le législateur a conféré aux ministres de l'Intérieur et de la Justice des compétences excessives en ce qui concerne les règles d'accès aux banques de données policières et les modalités d'interconnexion de celles-ci.

B.34. Le grief de la partie requérante étant dirigé contre l'article 44/4, § 3 et § 4, de la loi sur la fonction de police, inséré par l'article 7 de la loi attaquée, la Cour limite son examen à cette disposition.

B.35.1. Il ressort des travaux préparatoires que le choix de déléguer aux ministres de l'Intérieur et de la Justice le soin de déterminer les règles d'accès aux banques de données policières opérationnelles et aux banques de données techniques ainsi que les modalités d'interconnexion de l'ensemble des banques de données policières a été justifié par la volonté d'assurer l'homogénéité et la prévisibilité de la gestion de l'information policière et par le fait que ces mesures relèvent de la compétence du responsable du traitement (*Doc. parl*., Chambre, 2018-2019, DOC 54-3697/001, pp. 18, 24 et 25; DOC 54-3697/005, p. 6).

La précision selon laquelle les ministres précités déterminent ces règles d'accès et ces modalités d'interconnexion par « directives générales et contraignantes publiées au *Moniteur belge* » a été introduite par voie d'amendement « afin d'assurer la transparence requise » (*ibid.*, DOC 54-3697/005, p. 6).

B.35.2. L'article 44/4, § 4, alinéa 2, de la loi sur la fonction de police prévoit que les directives portant sur les modalités d'interconnexion des banques de données déterminent au moins, « sur la base du caractère pertinent, adéquat et non excessif », « les catégories de banques de données qui peuvent être connectées entre elles, les modalités relatives à l'interconnexion et les règles d'accès des membres des services de police relatives à l'existence d'une information pertinente au sein de ces banques de données interconnectées ou, le cas échéant, aux données elles-mêmes ainsi qu'aux traitements qui en résultent ». Il est dit dans les travaux préparatoires :

« Un alinéa a également été inséré dans le paragraphe 3*bis*, [devenu § 4] afin de permettre aux deux ministres de tutelle de déterminer les critères (p. ex. : octroyer les profils d'accès en fonction des besoins, sécurisation, …) auxquels doit satisfaire une telle interconnexion ainsi que de déterminer quelles banques de données peuvent être interconnectées » (*Doc. parl*., Chambre, 2018-2019, DOC 54-3697/001, p. 23).

Le texte initial de la proposition de loi disposait :

« Ces directives déterminent au moins, sur la base du caractère pertinent, adéquat et non excessif, les catégories de banques de données qui peuvent être connectées entre elles, les modalités relatives à l'interconnexion et les règles d'accès des membres des services de police aux traitements qui en résultent » (*Doc. parl*., Chambre, 2018-2019, DOC 54-3697/001, p. 57).

L'insertion des mots « relatives à l'existence d'une information pertinente au sein de ces banques de données interconnectées ou, le cas échéant, aux données elles-mêmes ainsi qu' » a été proposée par l'amendement n° 6 à la proposition de loi afin d'intégrer le principe selon lequel l'accès à l'existence d'une information pertinente doit être dissocié de l'accès à cette information en tant que telle (*ibid.*, DOC 54-3697/005, pp. 7-8).

B.35.3. L'article 44/4, § 5, alinéa 1er, de la loi sur la fonction de police précise que les profils et les modalités d'accès visés aux paragraphes 3 et 4 sont déterminés notamment sur la base 1) du « besoin d'en connaître, en ce compris de la nécessité de croiser ou coordonner les données traitées »; 2) des finalités légales de chaque banque de données; 3) des différentes catégories de personnes visées à l'article 44/5; 4) de l'évaluation des données; 5) de l'état de validation des données traitées. Il est dit dans les travaux préparatoires :

« Afin d'encadrer la portée des directives visées à l'article 3 et 3*bis* [devenus §§ 3 et 4], un paragraphe 3*ter* [devenu § 5] est inséré. La détermination des profils et des modalités d'accès doit tenir compte d'un ensemble de facteurs tels la proportionnalité de l'accès et le besoin d'en connaître, la finalité légale de chaque traitement, la sensibilité ou non des données, … Les éléments d'évaluation fixés à l'article 239 de la loi relative à la protection des données seront également en compte dans cette détermination » (*ibid*., DOC 54-3697/001, p. 24).

En vertu de l'article 44/4, § 5, alinéa 3, de la fonction de police, les profils d'accès et l'identification des personnes disposant d'un accès sont tenus à la disposition de l'Organe de contrôle. Il est dit dans les travaux préparatoires :

« Dans le cadre de leur mission d'autorité de contrôle, les membres de l'Organe de contrôle et de son service d'enquête ont un accès illimité aux traitements effectués par les services de police (cfr article 244 de la loi relative à la protection des données). À ce titre, ils peuvent consulter les profils d'accès et avoir connaissance de la liste des membres du personnel disposant d'un accès » (*ibid*.).

B.35.4. En vertu de l'article 44/4, § 5, alinéa 2, de la loi sur la fonction de police, les accès visés aux paragraphes 3 et 4 doivent être conçus « à la base ou par défaut de telle sorte que les

données évaluées et validées apparaissent de manière claire et puissent être exploitées prioritairement ». Il est précisé dans les travaux préparatoires :

« Sur la base des principes du *privacy by design* ou *by default*, les différents accès aux banques de données policières qu'elles soient interconnectées ou non doivent être conçus de sorte que les données évaluées et validées apparaissent de manière claire et puissent être exploitées prioritairement. Ceci est particulièrement important dans des situations de contrôle pouvant avoir des effets sur les droits et libertés des personnes.

Il va de soi qu'il peut être nécessaire de bien juger si une vérification doit être faite lors d'interventions policières dont le but consiste à identifier des personnes, de contrôler la détention d'armes ou d'autres questions de sécurité de cette nature. C'est une première évaluation qui doit être faite, par exemple, dans le cas d'un contrôle sur la voie publique ou de contrôles aléatoires lorsque l'identité d'un suspect ou d'un inculpé n'est pas encore établie. Dans ces cas, une information non validée est importante. Pour faire son évaluation, le fonctionnaire de police doit pouvoir prendre en compte toutes les sources disponibles » (*ibid.*).

B.35.5. Compte tenu de cette nouvelle réglementation des droits d'accès aux banques de données policières, le législateur a abrogé, par l'article 13, 2°, de la loi attaquée, l'article 44/11/2, § 2, alinéa 1er, de la loi sur la fonction de police qui prévoyait que les données à caractère personnel et les informations traitées dans les banques de données de base sont en principe uniquement accessibles aux services de police et seulement directement consultables par les services de police qui les ont enregistrées ou par ceux qui doivent, en raison de leurs missions légales, coordonner les données et informations (*ibid.*, DOC 54-3697/001, p. 29).

B.36. Comme il est dit en B.13.1, l'article 22 de la Constitution garantit à tout citoyen qu'il ne peut y avoir ingérence dans l'exercice du droit au respect de la vie privée qu'en vertu de règles adoptées par une assemblée délibérante démocratiquement élue, même si une délégation octroyée à un autre pouvoir reste possible pour autant que l'habilitation soit définie en des termes suffisamment précis et porte sur l'exécution de mesures dont les éléments essentiels ont été préalablement fixés par le législateur.

La Cour européenne des droits de l'homme n'a pas jugé que le traitement des données à caractère personnel et l'accès aux données traitées doivent être réglés par le pouvoir législatif. Elle a seulement souligné que ce traitement et cet accès doivent avoir une base claire, accessible

et prévisible dans la réglementation interne (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, §§ 47-63).

La Cour de justice exige elle aussi seulement que « la base légale qui permet l'ingérence dans [le droit au respect de la vie privée doive] définir elle-même la portée de la limitation de l'exercice du droit concerné » (CJUE, 6 octobre 2020, C-623/17, *Privacy International*, point 65). Elle n'exige pas que tous les aspects de cette limitation soient réglés par une loi formelle.

B.37. Il ressort des termes de l'article 44/4, § 3, de la loi sur la fonction de police que les banques de données policières opérationnelles et les banques de données techniques sont uniquement accessibles aux membres des services de police. Leurs profils et modalités d'accès sont notamment déterminés sur la base du « besoin d'en connaître, en ce compris de la nécessité de croiser ou coordonner les données traitées », des finalités légales de chaque banque de données ainsi que de l'évaluation et de l'état de validation des données traitées (article 44/4, § 5, alinéa 1er, de la loi sur la fonction de police).

Le législateur a en outre établi le contenu minimal des directives portant sur les modalités d'interconnexion des banques de données en prévoyant notamment que les règles d'accès aux banques de données interconnectées doivent dissocier l'accès à l'existence d'une information pertinente et l'accès à cette information en tant que telle (article 44/4, § 4, alinéa 2) et que les accès à la banque de donnée « source » et aux banques de données interconnectées doivent être conçus de telle sorte que les données évaluées et validées puissent être exploitées en priorité (article 44/4, § 5, alinéa 2).

Il a par ailleurs été précisé dans les travaux préparatoires que les conditions et restrictions d'usage qui sont déterminées pour chaque membre du personnel en fonction de son profil d'utilisateur à l'égard de la banque de données « source » s'appliquent à l'égard des banques de données interconnectées :

« Il convient en particulier de souligner expressément que les restrictions et conditions pour l'usage d'une quelconque donnée sont déterminées par les droits d'utilisation tels qu'ils ont été octroyés personnellement à chaque membre du personnel (en fonction de son profil d'utilisateur) par rapport au type de banque de données pouvant être consulté à la base. Par conséquent, les restrictions, et donc les dispositions et possibilités en matière de contrôle par

rapport à l'utilisation de données à caractère personnel sont toujours déterminées vis-à-vis de la ' banque de données source ' et sont fixées de façon immuable pour l'utilisateur de l'' interconnexion '. Le contrôle et les restrictions d'usage sont donc techniquement liés au fichier ou à la source de base, et non à l'application qui facilite l'utilisation des données issues d'une banque de données au moyen d'une interconnexion ou d'un traitement » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, p. 23).

Le législateur a également fixé les mesures de contrôle applicables. Les profils d'accès et l'identification des personnes disposant d'un accès à la banque de données « source » et aux banques de données interconnectées sont en effet tenus à la disposition de l'Organe de contrôle (article 44/4, § 5, alinéa 3, de la loi sur la fonction de police et article 244 de la loi du 30 juillet 2018). Par ailleurs, le motif de l'interconnexion et l'identification de la personne qui a consulté les données à caractère personnel, entre autres, apparaissent dans les fichiers de journalisation qui sont accessibles sur demande par l'Organe de contrôle (article 44/4, § 2, alinéas 2 et 3, de la loi sur la fonction de police et article 56, § 3, de la loi du 30 juillet 2018).

B.38. Le législateur a ainsi fixé les éléments essentiels à respecter lors de l'élaboration des directives portant sur les règles d'accès aux banques de données policières et sur les modalités d'interconnexion de celles-ci.

Étant donné la nature largement technique des règles d'accès aux banques de données policières et de leurs modalités d'interconnexion, il n'est pas dénué de justification raisonnable que les ministres de l'Intérieur et de la Justice, en leur qualité de responsables du traitement, soient habilités à déterminer celles-ci, dans le respect des éléments essentiels fixés à l'article 44/4 de la loi sur la fonction de police, afin de pouvoir répondre de manière uniforme et souple aux évolutions techniques qui se produisent.

En vertu de l'article 239 de la loi du 30 juillet 2018, l'Organe de contrôle doit du reste veiller, par le biais d'enquêtes de fonctionnement, à ce que le contenu des banques de données et la procédure de traitement des données et informations conservées soient conformes aux règles prescrites par les articles 44/1 à 44/11/13 de la loi sur la fonction de police. L'Organe de contrôle, qui peut agir d'initiative en la matière, peut également y être invité par, notamment, l'Autorité de protection des données, la Chambre des représentants et les autorités judiciaires

(article 237 de la loi du 30 juillet 2018). Dans l'hypothèse où les directives établies par les ministres de l'Intérieur et de la Justice ne seraient pas conformes à l'article 44/4 de la loi sur la fonction de police, il appartient à l'Organe de contrôle, le cas échéant à la demande des organes et des autorités mentionnés dans l'article 237 de la loi du 30 juillet 2018, de prendre les initiatives nécessaires en vue de faire disparaître cette illégalité.

Les directives relatives aux règles d'accès et aux modalités d'interconnexion des banques de données sont par ailleurs publiées au *Moniteur belge*. Elles bénéficient ainsi de la même publicité que la loi attaquée qui en fixe les éléments essentiels. Le législateur a ainsi entouré les habilitations visées en B.31.5 d'une garantie particulière afférente au droit au respect de la vie privée.

Le cas échéant, il appartient au juge compétent d'examiner si l'utilisation, faite par les ministres de l'Intérieur et de la Justice, de ces habilitations est conforme à l'article 44/4 de la loi sur la fonction de police et aux dispositions constitutionnelles et conventionnelles invoquées dans le moyen.

B.39. La disposition attaquée satisfait aux exigences mentionnées en B.36.

En ce qui concerne la prévisibilité des notions de « catégories de banques de données », de « modalités relatives à l'interconnexion » et de « règles d'accès »

B.40. Selon la partie requérante, la disposition attaquée manque de prévisibilité en ce qu'elle ne précise pas les notions de « règles d'accès », de « modalités relatives à l'interconnexion » et de « catégories de banques de données ».

B.41. Comme il est dit en B.13.2, l'exigence de prévisibilité en matière de protection des données implique que la loi prévoie de manière suffisamment précise les circonstances dans lesquelles les traitements de données à caractère personnel sont autorisés.

B.42.1. En vertu de l'article 44/4, § 3, de la loi sur la fonction de police, les ministres de l'Intérieur et de la Justice déterminent « les règles d'accès » des membres des services de police aux banques de données policières opérationnelles et aux banques de données techniques.

B.42.2. Le terme « accès » n'étant pas défini dans la loi attaquée ni dans les travaux préparatoires, il doit être interprété conformément à la signification qu'il a dans le langage courant.

Dans le langage courant, « l'accès » désigne, dans un contexte informatique, « la recherche et l'obtention des informations consécutivement à un traitement ». Par conséquent, l'article 44/4, § 3, de la loi sur la fonction de police habilite les ministres de l'Intérieur et de la Justice à déterminer les règles permettant aux membres des services de police de rechercher et d'obtenir des informations dans les banques de données policières opérationnelles et dans les banques de données techniques.

B.42.3. En vertu de l'article 44/4, § 4, alinéa 1er, de la loi sur la fonction de police, les ministres de l'Intérieur et de la Justice déterminent « les modalités relatives à l'interconnexion » des banques de données policières opérationnelles, des banques de données communes et des banques de données techniques entre elles ou avec d'autres banques de données auxquelles les services de police ont accès.

Le terme « modalité » n'est pas défini dans la loi attaquée ni dans les travaux préparatoires. Dans le langage courant, la « modalité » est la « forme particulière d'un acte, d'un fait, d'une pensée, d'un être ou d'un objet ».

En ce qui concerne le terme « interconnexion », il y a lieu de se référer à l'article 26, 2°, de la loi du 30 juillet 2018 qui définit le « traitement » comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction des données ».

Lorsqu'elle porte sur des banques de données, l'« interconnexion » est ainsi une opération de traitement effectuée à l'aide de procédés automatisés et appliquée à des ensembles de données à caractère personnel.

Il ressort par ailleurs des travaux préparatoires que l'interconnexion de banques de données visée à l'article 44/4, § 4, de la loi sur la fonction de police vise à relier entre elles les différentes banques de données policières ainsi que les autres banques de données auxquelles les services de police ont accès afin de permettre le traitement des données à caractère personnel qui résultent de cette mise en relation :

« Le paragraphe 3 est également remplacé, et un paragraphe 3*bis* et un paragraphe 3*ter* sont ajoutés, afin de donner un cadre légal clair aux applications existantes sur le terrain ainsi qu'au concept total ' *i-Police* ', en permettant également, outre les interconnexions de banques de données, davantage de traitements dans ces banques de données.

[…]

Le paragraphe 3*bis* reprend le contenu de l'ancien paragraphe 3 tout en l'adaptant à la formulation utilisée au paragraphe 4, tel qu'inséré par la loi ' caméra ' du 21 mars 2018. Ce paragraphe vise donc désormais l'interconnexion de banques de données avec les traitements qui en découlent.

L'article 44/4 de la [loi sur la fonction de police] avait été introduit précédemment par la loi du 18 mars 2014 afin de, notamment, donner aux ministres de tutelle la possibilité de permettre à la police d'interconnecter les banques de données policières sur le terrain, ainsi que d'autres banques de données auxquelles la police a accès.

Bien que l'exposé des motifs de la loi précitée ne le précise pas, il semble logique qu'une interconnexion entre des banques de données ne soit utile que si les données interconnectées peuvent également être traitées. Le concept d'interconnexion implique également les traitements subséquents » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 20-21).

Les travaux préparatoires indiquent également :

« La police doit en effet pouvoir collecter des informations sur le terrain avec les outils ICT modernes disponibles, et ce d'une manière et efficiente. Par exemple, lors du constat d'un accident de roulage, un fonctionnaire de police peut contrôler sur place les plaques d'immatriculation et consulter les données relatives au contrôle technique; lors du constat d'une effraction, la police peut vérifier qui habite à une adresse déterminée; lors du contrôle d'identité d'une personne dans le cadre d'un contrôle de circulation ou lors d'une mission d'assistance à un huissier de justice, la consultation de la B.N.G. ou du Registre national peut s'avérer nécessaire; lors du contrôle d'un musicien de rue, il peut s'avérer nécessaire de vérifier si la personne concernée est titulaire d'une autorisation de la commune; … Pour des raisons d'efficience opérationnelle, toutes ces consultations doivent pouvoir être effectuées sur le

terrain par un membre des services de police au départ d'un ' environnement unique '. Si ces données ne peuvent pas être fournies de façon ' interconnectée ', cela implique la consultation séparée de toutes les sources de données dans lesquelles des informations peuvent être disponibles. La communication permanente par radio, peut représenter une lourde charge pour le réseau radio, en particulier en situation de crise. C'est non seulement la perte de temps, mais surtout le risque d'une importante perte de qualité (en raison de manipulations trop nombreuses) qui justifient de mettre ces données à disposition de manière ' intégrée '. L'interconnexion de données issues de plusieurs sources (validées de façon autonome) et leur traitement dans un outil facile d'utilisation pour l'utilisateur final, sont inhérents au travail policier actuel, moderne, efficient et, surtout, sûr et sécurisé » (*ibid*., pp. 22-23).

Il résulte de ce qui précède que l'article 44/4, § 4, de la loi sur la fonction de police habilite les ministres de l'Intérieur et de la Justice à déterminer les manières dont les différentes banques de données policières sont reliées entre elles ou avec les autres banques de données auxquelles les services de police ont accès, afin de permettre le traitement des données à caractère personnel issues de cette mise en relation.

B.42.4. En vertu de l'article 44/4, § 4, alinéa 2, de la loi sur la fonction de police, les directives relatives aux modalités d'interconnexion des banques de données déterminent au moins les « catégories de banques de données » qui peuvent être connectées entre elles.

Il ressort du renvoi, par l'article 44/4, § 4, alinéa 1er, de la loi sur la fonction de police, aux banques de données « visées à l'article 44/2 » ainsi que des travaux préparatoires cités en B.46.2, que les « catégories de banques de données » visées à l'article 44/4, § 4, alinéa 2, de la même loi sont les banques de données policières opérationnelles (divisées elles-mêmes en trois sous-catégories : la B.N.G, les banques de données de base et les banques de données particulières), les banques de données communes et les banques de données techniques.

B.43. En ce qu'il porte sur la signification des termes contenus dans l'article 44/4, §§ 3 et 4, de la loi sur la fonction de police, tel qu'il a été inséré par l'article 7 de la loi attaquée, le moyen unique, en sa deuxième branche, n'est pas fondé.

En ce qui concerne le principe de proportionnalité

B.44. Selon la partie requérante, l'interconnexion des banques de données policières, prévue par la disposition attaquée, aurait des effets disproportionnés sur l'exercice du droit au respect de la vie privée.

B.45.1. Le principe 5.1 de la recommandation n° R (87) 15 dispose :

« La communication de données entre services de police en vue d'une utilisation à des fins de police ne devrait être permise que s'il existe un intérêt légitime à cette communication dans le cadre des attributions légales de ces services ».

B.45.2. Comme il a été dit en B.4.5, une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement reposer sur une disposition législative suffisamment précise, mais aussi répondre à un besoin social impérieux dans une société démocratique et être proportionnée au but légitime poursuivi.

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, du caractère distinctif de la réglementation 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° 27/2020 du 20 février 2020, B.8.3; arrêt n° 108/2016 du 14 juillet 2016, B.12.2; arrêt n° 29/2018 du 15 mars 2018, B.14.4; 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). Les dispositifs de fichage mis en place par les autorités pour contribuer à la répression et à la prévention de certaines infractions ne sauraient être mis en œuvre dans une logique excessive de maximalisation des informations qui y sont placées. Sans le respect d'une nécessaire proportionnalité au regard des objectifs légitimes qui leur sont attribués, les avantages qu'ils apportent seraient obérés par les atteintes graves qu'ils causeraient aux droits et libertés que les États doivent assurer en vertu de la Convention européenne des droits de l'homme aux personnes placées sous leur juridiction (CEDH, 22 juin 2017, *Aycaguer c. France,* § 34).

En ce qui concerne le respect du principe de proportionnalité, il ressort de la jurisprudence constante de la Cour de justice que la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du « strict nécessaire » (arrêts du 16 décembre 2008, *Satakunnan Markkinapörssi* et *Satamedia*, C-73/07, point 56; 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, points 51 et 52; 6 octobre 2015, *Schrems*, C-362/14, point 92, 21 décembre 2016, *Tele2 Sverige* et *Watson e.a.*, C-203/15 et C-698/15, points 96 et 103; 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, point 130).

B.46.1. Le traitement effectué par les services de police des données à caractère personnel issues d'une interconnexion de banques de données est entouré des garanties qui s'appliquent à tout traitement de données à caractère personnel effectué par les services police.

En vertu de l'article 44/1, § 1er, de la loi sur la fonction de police, les services de police ne peuvent en effet traiter des données à caractère personnel que pour autant que ces données « présentent un caractère adéquat, pertinent et non excessif au regard des finalités de police administrative et de police judiciaire pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ». Dans la mesure où certaines données relatives à une personne obtenues grâce à l'interconnexion de banques de données ne seraient pas pertinentes par rapport aux objectifs de police administrative ou judiciaire poursuivis, elles ne peuvent dès lors pas être traitées par les services de police. Il en va de même notamment pour les données qui seraient

« excessives » par rapport aux objectifs poursuivis. En ce qui concerne les données issues de banques de données interconnectées, cette exigence résulte également de l'article 44/4, § 4, alinéa 2, de la loi sur la fonction de police qui prévoit que les règles d'accès des membres des services de police aux banques de données interconnectées portent sur l'existence d'une information « pertinente » au sein de celles-ci (et, le cas échéant, sur l'accès à cette information en tant que telle). En outre, en vertu de l'article 44/4, § 5, alinéa 1er, de la loi sur la fonction de police, les profils et les modalités d'accès aux banques de données interconnectées sont déterminés notamment sur la base du « besoin d'en connaître, en ce compris de la nécessité de croiser ou coordonner les données traitées ».

En vertu de l'article 144 de la loi du 7 décembre 1998, inséré par l'article 31 de la loi attaquée, chaque responsable du traitement, chaque zone de police, le commissariat général, chaque direction générale et chaque direction de la police fédérale doivent désigner un « délégué à la protection des données », qui est entre autres chargé d'informer et de conseiller le responsable du traitement et les personnes qui procèdent au traitement sur leurs obligations en matière de protection de la vie privée, de contrôler le respect de la réglementation et des règles internes du responsable du traitement en la matière et de coopérer avec l'Organe de contrôle (article 65 de la loi du 30 juillet 2018). Les délégués exercent leur fonction en toute indépendance.

Les services de police sont contrôlés par l'Organe de contrôle qui, en vertu de l'article 239 de la loi du 30 juillet 2018, a notamment pour mission de veiller à ce que le contenu des banques de données et la procédure de traitement des données et informations qui y sont conservées soient conformes aux règles prescrites par les articles 44/1 à 44/11/13 de la loi sur la fonction de police. Il ressort en outre de l'article 239, § 3, 2° et 3°, de la loi du 30 juillet 2018 que le pouvoir de contrôle de l'Organe de contrôle a trait notamment au respect des dispositions relatives à la réception et à la communication des données et des informations par les autorités et services légalement habilités. L'Organe de contrôle est donc compétent pour vérifier que la communication de données entre services de police effectuée grâce à l'interconnexion des banques de données est conforme à l'article 44/4 de la loi sur la fonction de police.

Les pouvoirs des services de police sont également limités par des dispositions législatives qui réglementent la période pendant laquelle des données à caractère personnel restent

disponibles dans les banques de données policières et l'archivage de ces données, la période d'archivage et l'accès à ces archives (articles 44/9, 44/10 et 44/11/2, §§ 2 et suivants, de la loi sur la fonction de police).

Enfin, en vertu de l'article 44/3, § 1er, alinéa 1er, de la loi sur la fonction de police, les données à caractère personnel doivent être traitées conformément à la loi du 30 juillet 2018, de sorte que les garanties prévues dans cette loi sont également d'application.

B.46.2. Le traitement par les services de police des données à caractère personnel issues d'une interconnexion de banques de données est en outre entouré de garanties particulières.

Comme il est dit en B.37, les profils et les modalités d'accès aux banques de données interconnectées sont déterminés notamment sur la base du « besoin d'en connaître, en ce compris de la nécessité de croiser ou coordonner les données traitées », des finalités légales de chaque banque de données ainsi que de l'évaluation et de l'état de validation des données traitées (article 44/4, § 5, alinéa 1er, de la loi sur la fonction de police). Ces accès doivent être conçus de telle sorte que les données évaluées et validées puissent être exploitées en priorité (article 44/4, § 5, alinéa 2). Les règles d'accès aux banques de données interconnectées doivent par ailleurs dissocier l'accès à l'existence d'une information pertinente et l'accès à cette information en tant que telle (article 44/4, § 4, alinéa 2).

Pour ce qui est du contrôle, les profils d'accès et l'identification des personnes disposant d'un accès sont tenus à la disposition de l'Organe de contrôle (article 44/4, § 5, alinéa 3, de la loi sur la fonction de police et article 244 de la loi du 30 juillet 2018). Par ailleurs, le motif de l'interconnexion et l'identification de la personne qui a consulté les données à caractère personnel, entre autres, apparaissent dans les fichiers de journalisation qui sont accessibles sur demande de l'Organe de contrôle (article 44/4, § 2, alinéas 2 et 3, de la loi sur la fonction de police et article 56, § 3, de la loi du 30 juillet 2018).

La publication au *Moniteur belge* des directives relatives aux modalités d'interconnexion des banques de données constitue également une garantie contre les risques d'abus et une condition indispensable à l'exercice éventuel de voies de recours.

B.46.3. Enfin, en vertu de l'article 59, § 1er, alinéa 1er, 2°, de la loi du 30 juillet 2018, cité en B.25.8, le responsable du traitement ou son sous-traitant doit consulter l'Organe de contrôle préalablement au traitement qui fera partie d'un nouveau fichier à créer lorsque le type de traitement « en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures » présente des risques élevés pour les libertés et les droits des personnes concernées. Il en résulte que les ministres de l'Intérieur et de la Justice doivent consulter l'Organe de contrôle avant d'autoriser toute interconnexion de banques de données et tout traitement impliquant une interconnexion.

Cette consultation préalable de l'Organe de contrôle est notamment requise en cas de concrétisation du projet « I-Police » auquel il est fait référence dans les travaux préparatoires (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 3 et 20-23) et à propos duquel l'Organe de contrôle a déjà indiqué dans son avis n° 9/2018 du 12 décembre 2018, précité, qu'il n'est pas acquis que la disposition attaquée constitue une base légale suffisante à son développement :

« L'Organe de contrôle formule des réserves explicites quant à la question de savoir si l'avant-projet offre bien une base légale (suffisante) pour instaurer le futur concept d'‘ i-police ’, ce que l'Exposé des motifs s'empresse de supposer à tort […]. À l'heure d'aujourd'hui, il n'est pas encore suffisamment évident de savoir ce que comportera précisément le concept précité (en réalité), empêchant *hic* et *nunc* [l'Organe de contrôle] d'évaluer sa compatibilité avec la [loi sur la fonction de police, la loi du 30 juillet 2018] et le RGPD » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/003, p. 42).

B.47. Compte tenu de ce qui est dit en B.46.3, le moyen unique, en sa seconde branche, n'est pas fondé en ce qu'il dénonce le caractère disproportionné de la mesure introduite par l'article 44/4, § 4, de la loi sur la fonction de police, inséré par l'article 7 de la loi attaquée.

En ce qui concerne la consultation préalable de l'Organe de contrôle et l'obligation de notification en cas de rectification ou d'effacement

B.48. En ce que la partie requérante allègue que la disposition attaquée ne prévoit pas la consultation de l'Organe de contrôle préalablement au traitement des données à caractère

personnel qui fera partie d'un nouveau fichier à créer, son grief n'est pas fondé dès lors que cet aspect est réglé par l'article 59, § 1er, de la loi du 30 juillet 2018, précité.

Compte tenu de ce qui est dit en B.46.3, il n'y a pas lieu de poser à la Cour de justice de l'Union européenne la question préjudicielle suggérée par la partie requérante.

B.49. En ce que la partie requérante allègue que la disposition attaquée ne prévoit pas de notifier aux destinataires des données que celles-ci ont fait l'objet d'une rectification ou d'un effacement, son grief n'est pas fondé étant donné que cet aspect est réglé par l'article 39, § 6, de la loi du 30 juillet 2018.

Quant au traitement des données relatives aux personnes faisant l'objet d'une mesure administrative (article 44/5, § 1er, alinéa 1er, 7°, de la loi sur la fonction de police)

B.50. Dans la troisième branche du moyen unique, la partie requérante allègue que les termes « mesure administrative » employés à l'article 44/5, § 1er, alinéa 1er, 7°, de la loi sur la fonction de police, inséré par l'article 8, 1°, de la loi attaquée, ne sont pas suffisamment clairs.

B.51. L'article 44/5, § 1er, alinéa 1er, 7°, de la loi sur la fonction de police, inséré par l'article 8, 1°, de la loi attaquée, dispose :

« Les données à caractère personnel traitées dans les banques de données visées à l'article 44/2, § 1er, alinéa 2, 1° et 2°, aux fins de police administrative sont les suivantes :

[…]

7° les données relatives aux personnes faisant l'objet d'une mesure administrative prise par une autorité administrative compétente et que les services de police sont chargés de suivre par ou en vertu de la loi, du décret ou de l'ordonnance ».

En vertu de cette disposition, les données à caractère personnel relatives aux « personnes faisant l'objet d'une mesure administrative prise par une autorité administrative compétente et

que les services de police sont chargés de suivre par ou en vertu de la loi, du décret ou de l'ordonnance » sont traitées dans la B.N.G. ou dans les banques de données de base, à des fins de police administrative.

B.52.1. Dans les travaux préparatoires, cette nouvelle catégorie a été commentée comme suit :

« La disposition 7° est avant tout insérée à l'article 44/5, § 1er, parce que les nouvelles règles en matière de protection des données imposent de définir les catégories de données à caractère personnel.

La disposition visée au 7° porte sur les mesures administratives prises par une autorité administrative compétente à l'égard d'une personne ou d'un établissement, à l'égard desquelles les services de police doivent assurer un contrôle et un suivi en vertu de la loi. Il s'agit concrètement entre autres, mais pas exclusivement, des décisions prises par les autorités de police administrative (le ministre de l'Intérieur, le gouverneur ou le bourgmestre) dans le cadre de législations particulières telles que la nouvelle loi communale (articles 129, 134-135), loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques et des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes (article 9*bis*), la loi du 24 mars 1987 relative à la santé des animaux (mesure visant à prévenir et à combattre des maladies animales, comme la mise en place d'une zone de protection censée empêcher la propagation de la peste porcine africaine), mais également de sanctions prises par d'autres autorités compétentes, par exemple dans le cadre de la loi du 24 juin 2013 relative aux sanctions administratives communales (suspension ou retrait d'une autorisation ou d'un permis, fermeture temporaire ou définitive d'un établissement) ou par la cellule Football du SPF Intérieur (interdiction administrative de stade, interdiction administrative de périmètre, interdiction temporaire de quitter le territoire) dans le cadre de la loi du 21 décembre 1998 relative à la sécurité lors des matches de football (loi football).

Il est en effet parfaitement logique que la police puisse traiter les données relatives à ces personnes dans les banques de données de base et la B.N.G., et puisse consulter ces banques de données dans la mesure où elle doit également pouvoir suivre et contrôler effectivement le bon respect de ces mesures.

Pour répondre au point 9 de l'avis de l'Organe de contrôle, la base légale qui permet à police de constater les sanctions administratives simples n'est pas la loi sur la fonction de police mais bien les lois, décret ou ordonnances y relatifs. Le traitement réalisé par la police à cet effet se limite à les constater. Par ailleurs, la police peut les constater dans ses outils de traitements mais elle doit les effacer dès lors que l'envoi est réalisé vers le fonctionnaire sanctionnateur » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 25-26).

Dans son avis n° 9/2018 du 12 décembre 2018, précité, auquel il est fait référence dans les travaux préparatoires, l'Organe de contrôle avait suggéré de reformuler le point 7 en y insérant le terme « sanction » :

« [L'Organe de contrôle] propose de faire la clarté et de compléter le point 7° par le terme ' sanction ' et de reformuler légèrement comme suit : ' les données relatives aux personnes faisant l'objet d'une mesure administrative ou d'une sanction administrative prise par une autorité administrative compétente et que les services de police doivent surveiller par ou en vertu de la loi ou dont ils assurent le respect. ' De cette manière, on sait clairement qu'il ne s'agit pas uniquement de décisions prises par une autorité policière administrative (bourgmestre, gouverneur, ministre de l'Intérieur) mais par toute administration qui peut prendre une mesure ou une sanction dont la surveillance du respect ou de l'application relève des missions de la police, et ce par ou en vertu de la loi » (*Doc. parl*., Chambre, 2018-2019, DOC 54-3697/003, p. 43).

B.52.2. Il ressort des termes de la disposition attaquée et des travaux préparatoires que les données concernant les mesures ou les sanctions administratives imposées par une autorité administrative compétente, policière ou non, dont les services de police sont légalement chargés de contrôler le respect, peuvent être traitées par les services de police.

Les termes « mesures administratives » peuvent être raisonnablement interprétés comme désignant notamment les sanctions administratives.

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

Quant à la conservation et à l'archivage des données (article 44/11/2 de la loi sur la fonction de police)

B.53. Dans la quatrième branche du moyen unique, la partie requérante allègue que le système de conservation et d'archivage des données prévu à l'article 44/11/2 de la loi sur la fonction de police, tel qu'il a été modifié par l'article 13 de la loi attaquée, est disproportionné.

B.54. À la suite de sa modification par la disposition attaquée, l'article 44/11/2 de la loi sur la fonction de police dispose :

« § 1er. Les banques de données de base sont les banques de données policières créées au profit de l'ensemble de la police intégrée et qui ont pour finalité d'exécuter les missions de police administrative et de police judiciaire en exploitant les données à caractère personnel et

informations qui y sont incluses et en informant les autorités compétentes de l'exercice de ces missions.

Ces banques de données sont développées et gérées par la direction de la direction générale de la gestion des ressources et de l'information de la police fédérale, visée à l'article 44/11, § 1er, alinéa 1er.

§ 2. Les données relatives aux missions de police administrative sont accessibles durant cinq ans à partir du jour de leur enregistrement.

Les données relatives aux missions de police judiciaire sont accessibles durant quinze ans à partir du jour de leur enregistrement.

§ 3. Après l'écoulement du délai de quinze ans visé au § 2, alinéa 2, les données à caractère personnel et les informations relatives uniquement aux missions de police judiciaire sont consultables :

1° pendant un nouveau délai de quinze ans et ce, uniquement sur la base du numéro de notice du procès-verbal, du numéro de rapport d'information ou du numéro de dossier;

2° pendant un nouveau délai de trente ans et ce, uniquement dans le cadre d'une enquête relative à des crimes.

§ 4. Par dérogation au § 2, alinéa 2, et au § 3, les données et informations relatives aux missions de police judiciaire relatives à des faits non concrets sont accessibles durant cinq ans à partir de leur enregistrement.

§ 5. Par dérogation au § 2, alinéa 2, et au § 3, les données et informations traitées dans les banques de données de base relatives aux infractions visées à l'arrêté royal du 1er décembre 1975 portant règlement général sur la police de la circulation routière et de l'usage de la voie publique sont accessibles durant cinq ans à partir de leur enregistrement.

§ 6. Les données et informations traitées dans les banques de données de base relatives à la gestion des enquêtes menées dans le cadre d'une information au sens de l'article 28*bis* du Code d'instruction criminelle ou d'une instruction judiciaire au sens de l'article 56 du Code d'instruction criminelle pour laquelle des devoirs d'enquête ont été prescrits à la police sont disponibles durant trente ans à partir du moment où la fin de l'enquête a été communiquée par le magistrat compétent à la police.

Le procureur général compétent peut, dans des circonstances exceptionnelles, décider de manière motivée qu'à l'échéance de ce délai toute ou partie des données d'une enquête contenue dans une banque de données de base relative aux enquêtes doivent être conservées pendant une nouvelle période renouvelable de maximum dix ans.

§ 7. Sans préjudice de la loi du 24 juin 1955 relative aux archives, les données à caractère personnel et les informations sont effacées, après l'écoulement des délais visés au présent article.

§ 8. Tous les traitements réalisés dans les banques de données de base font l'objet d'une journalisation qui est conservée pendant quinze ans à partir du traitement réalisé dans les banques de données de base. Le responsable du traitement peut, si nécessaire, prolonger ce délai de maximum quinze ans ».

B.55.1. L'article 13 de la loi attaquée vise principalement à abroger l'ancien alinéa 1er du paragraphe 2 de l'article 44/11/2 de la loi sur la fonction de police, compte tenu de la nouvelle réglementation des droits d'accès aux banques de données policières désormais visée à l'article 44/4, §§ 3 et suivants, de la loi sur la fonction de police.

La disposition attaquée prévoit par ailleurs un délai maximal pour la conservation des fichiers de journalisation dans un nouveau paragraphe 8, inséré à l'article 44/11/2 de la loi sur la fonction de police (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 29-30).

B.55.2. Comme la partie requérante l'indique elle-même, l'article 13 de la loi attaquée ne modifie pas les règles relatives à la conservation des données contenues dans les banques de données de base qui étaient prévues par la version antérieure de l'article 44/11/2 de la loi sur la fonction de police.

B.55.3. Le grief de la partie requérante est uniquement dirigé contre les règles relatives à la conservation des données contenues dans les banques de données de base prévues à l'article 44/11/2, §§ 2 à 7, de la loi sur la fonction de police, et non contre la règle nouvelle introduite au paragraphe 8 de cette disposition.

Le grief de la partie requérante est par conséquent dirigé contre des règles qui n'ont pas été modifiées par la disposition attaquée.

B.55.4. Le moyen unique, en sa quatrième branche, est irrecevable.

Quant à l'accès direct des services de renseignement et de sécurité à la B.N.G. (article 44/11/8bis de la loi sur la fonction de police)

B.56. Dans la sixième branche du moyen unique, la partie requérante fait valoir que l'accès direct des services de renseignement et de sécurité à la B.N.G. prévu par l'article 44/11/8*bis* de la loi sur la fonction de police, inséré par l'article 21 de la loi attaquée, ne respecte pas le principe de légalité et qu'il porte une atteinte disproportionnée au droit au respect à la vie privée et au droit à la présomption d'innocence.

B.57. Les articles 44/11/7 à 44/11/12 de la loi sur la fonction de police font partie de la sous-section 8 (« La communication des données et l'accès à la B.N.G. ») de la section 1*bis* de cette loi.

La sous-section en question fait une distinction entre (1) la communication de données et d'informations provenant des banques de données policières, par quoi il convient d'entendre la transmission par quelque support que ce soit de données à caractère personnel à partir de ces banques de données, (2) l'accès direct à la B.N.G., par quoi il faut comprendre une liaison automatisée à cette banque de données, et (3) l'interrogation directe de la B.N.G., par quoi il faut comprendre un accès direct limité (article 44/11/4).

Contrairement à l'« accès direct » et à l'« interrogation directe », la « communication de données et d'informations » réglée par la loi attaquée concerne non seulement les données personnelles et informations contenues dans la B.N.G. mais également celles qui sont contenues dans les banques de données de base et dans des banques de données particulières (article 44/11/4, § 1er, de la loi sur la fonction de police). En outre, contrairement à l'accès direct et à l'interrogation directe, la communication de données et d'informations ne s'opère pas au moyen d'une connexion automatisée, de sorte que cette communication doit en principe être précédée d'une demande ciblée de la part des autorités, organismes et personnes visés.

Les articles 44/11/7 à 44/11/12 de la loi sur la fonction de police règlent les modalités d'accès direct à la B.N.G. et d'interrogation directe de celle-ci et les modalités de la communication de données provenant des banques de données policières. Ils prévoient à cet égard des délégations attribuées au Roi ou au ministre compétent.

B.58. Dans le régime antérieur à celui de la loi attaquée, les services de renseignement et de sécurité disposaient d'un droit d'« interrogation directe » de la B.N.G. « dans le cadre de l'exercice de leurs missions légales » (article 44/11/12, § 1er, 2°, lu en combinaison avec l'article 44/11/9, § 1er, 1°, de la loi sur la fonction de police, insérés, respectivement, par les articles 35 et 32 de la loi du 18 mars 2014, précités). Les données provenant des banques de données policières pouvaient également leur être « communiquées » en vertu de l'article 44/11/9, § 1er, 1°, de la loi sur la fonction de police, inséré par l'article 32 de la loi du 18 mars 2014, précité. En revanche, les services de renseignement et de sécurité ne faisant pas partie des autorités visées dans les articles 44/7 et 44/8 de la loi sur la fonction de police, ils ne disposaient pas d'un « accès direct » à la B.N.G. (article 44/11/12, § 1er, 1°, lu en combinaison avec les articles 44/11/7 et 44/11/8 de la loi sur la fonction de police, insérés, respectivement, par les articles 35, 30 et 31 de la loi du 18 mars 2014, précités).

B.59.1. L'article 20 de la loi attaquée a supprimé, dans l'article 44/11/8 de la loi sur la fonction de police, précité, les mots « et à l'Organe pour la coordination de l'analyse de la menace ». À la suite de cette modification, l'article 44/11/8 de la loi sur la fonction de police dispose :

« Les données à caractère personnel et les informations peuvent aussi être communiquées au Comité permanent P et à son Service d'enquêtes, au Comité Permanent R et à son Service d'enquêtes, à l'Organe de contrôle, à l'Inspection générale de la police fédérale et de la police locale pour leur permettre d'exercer leurs missions légales ».

L'article 22, 1°, de la loi attaquée a supprimé le point 1° de l'article 44/11/9, § 1er, de la loi sur la fonction de police précité. À la suite de cette modification, l'article 44/11/9, § 1er, de la loi sur la fonction de police, dispose :

« Selon les modalités déterminées par les directives des ministres de l'Intérieur et de la Justice, chacun dans le cadre de ses compétences, les données à caractère personnel et les informations peuvent également être communiquées aux organes et services suivants pour leur permettre d'exercer leurs missions légales :

1° la Cellule de traitement des informations financières;

2° l'Office des étrangers;

3° les services d'enquête et recherche et l'administration surveillance, contrôle et constatation de l'Administration générale des douanes et accises ».

L'article 21 de la loi attaquée a inséré, entre les articles 44/11/8 et 44/11/9 de la loi sur la fonction de police ainsi modifiés, un nouvel article 44/11/8*bis* qui dispose :

« Selon les modalités déterminées par les directives des ministres de l'Intérieur et de la Justice, chacun dans le cadre de ses compétences, les données à caractère personnel et les informations peuvent aussi être communiquées à l'Organe pour la coordination de l'analyse de la menace et aux services de renseignement et de sécurité, sans préjudice de l'article 14 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, pour leur permettre d'exercer leurs missions légales.

Les modalités de communication vers la police des données des services de renseignement sont déterminées dans un instrument juridique dont la date d'entrée en vigueur est simultanée à celle de l'accès direct des services de renseignement et de sécurité à la B.N.G. ».

Enfin, l'article 24, 2°, de la loi attaquée a remplacé, dans l'article 44/11/12, § 1er, 1°, de la loi sur la fonction de police, les mots « à l'article 44/11/7 et 44/11/8 » par les mots « aux articles 44/11/7, 44/11/8 et 44/11/8*bis* ». À la suite de cette modification, l'article 44/11/12 de la loi sur la fonction de police dispose :

« § 1er. Le Roi détermine, par arrêté délibéré en Conseil des Ministres, après avis de l'Organe de contrôle :

1° les modalités d'accès direct aux données à caractère personnel et informations contenues dans la B.N.G. pour les autorités visées aux articles 44/11/7, 44/11/8 et 44/11/8*bis* dans le cadre de l'exercice de leurs missions légales;

2° les modalités d'interrogation directe de la B.N.G. pour les autorités visées à l'article 44/11/9, dans le cadre de l'exercice de leurs missions légales.

§ 2. Les modalités d'interrogation directe ou d'accès direct, visées au présent article portent au moins sur :

a) le besoin d'en connaître;

b) les catégories de membres du personnel qui sur la base de l'exécution de leurs missions disposent d'un accès direct à ou d'une possibilité d'interroger directement la B.N.G.;

c) les traitements automatisés qui sont effectués sur la base des données et informations de la B.N.G.;

d) l'obligation du respect du secret professionnel par toutes les personnes qui prennent directement ou indirectement connaissance des données et informations de la B.N.G.;

e) les mesures de sécurité dont notamment :

1° la sécurité des infrastructures et des réseaux;

2° l'obligation de journalisation de toutes les transactions et de conserver ces données de journalisation pendant dix ans minimum;

f) l'obligation de suivre une formation préalablement à l'obtention de l'accès direct ou du droit à l'interrogation directe;

g) l'évaluation de la fiabilité, du milieu et des antécédents des membres du personnel visés au point *b)* ».

B.59.2. Dans les travaux préparatoires, la disposition à l'origine de l'article 21 de la loi attaquée est commentée comme suit :

« Articles 20 (modification de l'article 44/11/8) et 21 (introduction article 44/11/8*bis*)

L'OCAM est supprimé de l'article 44/11/8 et est inséré à l'article 44/11/8*bis*. Combiné à la suppression du point 1° de l'article 44/11/9, § 1er, qui concerne les services de renseignement (voir infra les modifications portées par l'article 21 [lire : 22]), il s'agit de modifications techniques qui permettent de regrouper dans un seul article deux services clairement identifiés, à savoir d'une part l'OCAM et d'autre part les services de renseignement, afin de pouvoir leur conférer dans l'article 44/11/12 un accès direct à la B.N.G. En soi, le principe reste inchangé dans cet article puisque ces deux services gardent comme par le passé la possibilité de recevoir communication de l'ensemble des données et informations pertinentes dans le cadre de l'exercice de leurs missions.

Comme c'est le cas pour les destinataires visés à l'art. 44/11/9, § 1er, il appartient aux ministres de l'Intérieur et de la Justice de déterminer les modalités de communication de ces données aux destinataires visés à l'art. 44/11/8*bis* » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, p. 37).

B.59.3. Il en ressort que l'article 44/11/8*bis*, alinéa 1er, de la loi sur la fonction de police, inséré par l'article 21 de la loi attaquée, regroupe dans un seul article la règle concernant la communication de données et d'informations provenant des banques de données policières à l'Organe pour la coordination de l'analyse de la menace et aux services de renseignement et de sécurité, qui était auparavant inscrite dans deux dispositions distinctes : l'article 44/11/8 de la loi sur la fonction de police et l'article 44/11/9, § 1er, 1°, de la loi sur la fonction de police, tel qu'ils étaient applicables avant leur modification respective par les articles 20 et 22 de la loi attaquée.

Par ailleurs, en vertu de l'article 44/11/12, § 1er, 1°, de la loi sur la fonction de police, tel qu'il a été modifié par l'article 24, 2°, de la loi attaquée, lu en combinaison avec

l'article 44/11/8*bis*, alinéa 1er, de la loi sur la fonction de police, inséré par l'article 21 de la loi attaquée, le Roi détermine, par arrêté délibéré en Conseil des ministres, après avis de l'Organe de contrôle, les modalités d'« accès direct » aux données à caractère personnel et informations contenues dans la B.N.G. « pour les autorités visées aux articles 44/11/7, 44/11/8 et 44/11/8*bis* », et donc notamment pour les services de renseignement et de sécurité visés à l'article 44/11/8*bis*, alinéa 1er, dans le cadre de l'exercice de leurs missions légales. Ces modalités doivent porter au moins sur les points mentionnés à l'article 44/11/12, § 2.

B.60.1. Le Conseil des ministres soulève l'irrecevabilité de la sixième branche du moyen unique au motif que l'extension de l'accès direct à la B.N.G. au profit des services de renseignement et de sécurité est prévue par l'article 24 de la loi attaquée, et non par l'article 21 de celle-ci qui est la seule disposition attaquée.

B.60.2. Il ressort des travaux préparatoires cités en B.59.2 et du renvoi, par l'article 44/11/12, § 1er, 1°, de la loi sur la fonction de police, tel qu'il a été modifié par l'article 24, 2°, de la loi attaquée, à l'article 44/11/8*bis* de la loi sur la fonction de police, inséré par l'article 21 de celle-ci, que l'accès direct des services de renseignement et de sécurité à la B.N.G. résulte de la lecture combinée de ces deux dispositions.

L'identification, dans la requête, de l'une de ces dispositions seulement n'a pas empêché le Conseil des ministres de répondre aux griefs formulés par la partie requérante, de sorte que les droits de défense n'ont pas été affectés.

Le moyen unique, en sa sixième branche, est recevable. La Cour examine le grief de la partie requérante en ce qu'il est dirigé contre les deux dispositions précitées lues conjointement.

B.61. La partie requérante fait valoir tout d'abord que le droit d'accès direct à la B.N.G. prévu par les dispositions attaquées au profit des services de renseignement et de sécurité n'est pas compatible avec le principe de la légalité formelle.

B.62.1. En vertu de l'article 44/11/12, § 1er, 1°, de la loi sur la fonction de police, lu en combinaison avec l'article 44/11/8*bis*, alinéa 1er, de la même loi, insérés par les dispositions attaquées, les autorités visées aux articles 44/11/7, 44/11/8 et 44/11/8*bis* qui peuvent recevoir

un accès direct à la B.N.G. sont les autorités judiciaires, les autorités de police administrative, le Comité permanent P et son service d'enquêtes, le Comité permanent R et son service d'enquêtes, l'Organe de contrôle, l'Inspection générale de la police fédérale et de la police locale, l'Organe pour la coordination de l'analyse de la menace et les services de renseignement et de sécurité.

B.62.2. Il en ressort que le législateur a désigné les autorités qui peuvent prétendre à un accès direct à la B.N.G., parmi lesquelles figurent désormais les services de renseignement et de sécurité, et a également prévu que ces possibilités ne peuvent leur être accordées que « dans le cadre de l'exercice de leurs missions légales ».

Les modalités de cet accès direct et de ce droit d'interrogation directe doivent être fixées par le Roi, en vertu de l'article 44/11/12, § 1er, après avis de l'Organe de contrôle.

L'article 44/11/12, § 2, de la loi sur la fonction de police dispose à cet égard expressément que ces modalités doivent porter au moins sur : « le besoin d'en connaître »; les catégories de membres du personnel qui, sur la base de l'exécution de leurs missions, disposent d'un accès direct à la B.N.G. ou d'une possibilité de l'interroger directement; l'évaluation de la fiabilité, du milieu et des antécédents de ces personnes; les traitements automatisés qui sont effectués sur la base des données et informations de la B.N.G.; l'obligation du respect du secret professionnel par toutes les personnes qui prennent directement ou indirectement connaissance des données et informations de la B.N.G.; les mesures de sécurité dont certaines sont expressément définies et l'obligation de suivre une formation préalablement à l'obtention de l'accès direct ou du droit à l'interrogation directe.

B.63.1. Comme la Cour l'a jugé par son arrêt n° 108/2016, eu égard à la diversité des autorités visées dans les articles 44/11/7, 44/11/8 et 44/11/8*bis* de la loi sur la fonction de police, le législateur pouvait estimer qu'il convenait d'habiliter le Roi à fixer les modalités relatives à l'accès direct, pour mettre ainsi sur pied une réglementation tenant compte des missions légales spécifiques que remplissent ces autorités et des caractéristiques spécifiques qui y sont liées (B.66.4).

Compte tenu du fait que le législateur a désigné les autorités qui entrent en considération pour obtenir un accès direct à la B.N.G. et qu'il a fixé les éléments essentiels des modalités en question dans l'article 44/11/12, § 2, de la loi sur la fonction de police, la délégation conférée au Roi par l'article 44/11/12, § 1er, ne viole pas le principe de la légalité formelle garanti par l'article 22 de la Constitution.

Dès lors que l'article 44/11/12, § 1er, de la loi sur la fonction de police prévoit que le Roi ne peut adopter ces modalités qu'après avoir reçu l'avis de l'Organe de contrôle, le législateur a en outre entouré la délégation concernée de garanties particulières afférentes au droit au respect de la vie privée.

B.63.2. Pour le surplus, en ce que le grief de la partie requérante semble se référer aux modalités de communication des données des services de renseignement et de sécurité à la police, visées à l'article 44/11/8*bis*, alinéa 2, de la loi sur la fonction de police, inséré par l'article 21 de la loi attaquée, il n'est pas suffisamment développé pour être intelligible. Il est, par conséquent, irrecevable.

B.64. La partie requérante fait valoir ensuite que l'accès direct à la B.N.G. par les services de renseignement et de sécurité ne respecte pas le principe de finalité et qu'il constitue une ingérence disproportionnée dans le droit au respect de la vie privée.

B.65.1. L'article 5.2.i. de la recommandation n° R (87) 15, intitulé « Communication à d'autres organes publics », dispose :

« La communication de données à des organes publics ne devrait être permise que, si dans un cas déterminé :

a. il y a obligation ou autorisation légales claires ou autorisation de l'autorité de contrôle, ou si

b. ces données sont indispensables au destinataire pour accomplir sa tâche légale propre et pour autant que le but de la collecte ou du traitement exécuté par ce destinataire n'est pas incompatible avec celui prévu à l'origine et que les obligations légales de l'organe communiquant ne s'y opposent pas ».

B.65.2. Comme il est dit en B.4.5, une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement reposer sur une disposition législative suffisamment précise, mais aussi répondre à un besoin social impérieux dans une société démocratique et être proportionnée au but légitime poursuivi.

B.66.1. En vertu de l'article 44/1 de la loi sur la fonction de police et à l'article 27 de la loi du 30 juillet 2018, les finalités du traitement des données à caractère personnel collectées par les services de police sont, de manière générale, la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales; ces traitements sont régis par le titre 2 de la loi du 30 juillet 2018.

En vertu de l'article 44/7, alinéa 1er, de la loi sur la fonction de police, les finalités de traitement des données contenues dans la B.N.G. sont, en particulier : l'identification des personnes visées à l'article 44/5, §§ 1er et 3; l'identification des personnes ayant accès à la B.N.G.; la coordination et le croisement des données à caractère personnel et informations policières; la vérification au niveau national des antécédents de police administrative et de police judiciaire; l'aide aux contrôles effectués par les services de police par l'indication des mesures à prendre soit sur la base d'une décision des autorités de police administrative ou des autorités de police judiciaire compétentes, soit en fonction de l'existence des antécédents de police administrative ou de police judiciaire et l'appui à la définition et à la réalisation de la politique policière et de sécurité.

En vertu de l'article 29, § 2, de la loi du 30 juillet 2018 (qui transpose l'article 9, paragraphe 1, de la directive « police »), les données à caractère personnel collectées par les services de police dans la B.N.G. pour les finalités précitées ne peuvent pas être traitées ultérieurement à d'autres fins « à moins que cette finalité ne soit permise conformément à la loi, au décret, à l'ordonnance, au droit de l'Union européenne ou à l'accord international ».

B.66.2. En autorisant les services de renseignement et de sécurité à accéder aux données contenues dans la B.N.G, les dispositions attaquées permettent que ces données soient traitées pour des finalités autres que les fins de police précitées, à savoir pour les missions des services de renseignement visées aux articles 7 et 11 de la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité ».

Il en ressort que les finalités de renseignement poursuivies par le traitement ultérieur des données contenues dans la B.N.G. qui avaient été initialement collectées à des fins de police sont prévues par la loi, conformément à l'article 29, § 2, de la loi du 30 juillet 2018.

Les activités des services de renseignements et de sécurité échappant au champ d'application du droit de l'Union, ces traitements sont régis uniquement par le titre 3 de la loi du 30 juillet 2018 (articles 2, paragraphe 3, point *a)*, et 9, paragraphe 1, deuxième phrase, de la directive « police »; considérant 14 de celle-ci; *Doc. parl.*, Chambre, 2017-2018, DOC 54-3126/001, pp. 743 et 794).

B.67.1. Dans les travaux préparatoires, la mesure attaquée a été justifiée par les missions légales des services de renseignement et de sécurité (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 9-41).

En vertu des articles 7 et 11 de la loi du 30 novembre 1998, les missions légales des services de renseignement et de sécurité consistent, en substance, à rechercher, à analyser et à traiter le renseignement relatif, notamment, à toute activité qui menace ou pourrait menacer la sûreté intérieure ou extérieure de l'État, et à en informer les ministres compétents.

B.67.2. Ces objectifs constituent des buts d'intérêt général susceptibles de justifier une ingérence dans le droit au respect de la vie privée.

B.68. Il convient d'examiner encore si l'ingérence dans le droit au respect de la vie privée qui résulte des dispositions attaquées est suffisamment précise, proportionnée et limitée au « strict nécessaire ».

B.69.1. Comme il est dit en B.57, la loi attaquée fait une distinction entre (1) la communication de données et d'informations provenant des banques de données policières, par quoi il convient d'entendre la transmission par quelque support que ce soit de données à caractère personnel provenant de ces banques de données, (2) l'accès direct à la B.N.G., par quoi il faut comprendre une liaison automatisée à cette banque de données, et (3) l'interrogation directe de la B.N.G., par quoi il faut comprendre un accès direct limité (article 44/11/4 de la loi sur la fonction de police).

Il ressort des travaux préparatoires de la loi du 18 mars 2014 « relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle » que le législateur a instauré cette distinction « parce que l'immixtion dans la vie privée n'est pas la même selon qu'il s'agit d'une communication de données ou d'un accès direct à celles-ci » (*Doc. parl.*, Chambre, 2013-2014, DOC 53-3105/001, p. 54). Le législateur a donc estimé que, lorsqu'il est permis aux autorités, services, organismes et personnes mentionnés dans la loi d'obtenir des données provenant des banques de données policières, il faut tenir compte de l'effet de la transmission de ces données sur la vie privée et de la nature des autorités, services, organismes et personnes à qui ces données sont transférées. Il a considéré à cet égard que l'accès direct a une incidence plus importante sur la vie privée que l'interrogation directe et la communication et qu'une interrogation directe compromet davantage la vie privée qu'une communication.

B.69.2. Dans les travaux préparatoires, la mesure attaquée a été justifiée par les missions légales des services de renseignement et de sécurité et par la méthode de recherche et d'analyse des informations propre à ces services, mais aussi par l'insuffisance des formes existantes de « communication de données et d'informations » contenues dans les banques de données policières et d'« interrogation directe » de la B.N.G. :

« L'article 44/11/12 a été adapté pour permettre un accès direct [à] la B.N.G. au profit des services de renseignement.

L'accès direct à la B.N.G. est un point important pour la correcte réalisation des missions légales dévolues aux services de renseignement et de sécurité.

De manière générale, pour pouvoir réaliser leurs missions, les services de renseignement et de sécurité doivent pouvoir mettre en œuvre leur loi organique, et en particulier son article 14, de la manière la plus efficace possible.

Certains types de données et informations policières contenues dans la B.N.G. sont essentiels aux services de renseignement et de sécurité pour réaliser leurs missions de protection, de détection, de prévention et d'entrave des menaces à la ' sécurité nationale ' ou à l'État, qu'il s'agisse de terrorisme ou d'espionnage et d'ingérence.

En effet, les menaces sur lesquelles travaillent les services de renseignement et de sécurité trouvent souvent leurs prémisses dans des faits infractionnels ou de menaces à l'ordre public, référencés par la Police dans la B.N.G. et d'autre part, ces menaces peuvent avoir un impact potentiel sur la sécurité/l'ordre public.

L'information policière peut donc pour les services de renseignement et de sécurité, signifier le point de départ d'une enquête de renseignement dans des domaines où il y a notamment une responsabilité partagée (ex. terrorisme ou extrémisme).

Par ailleurs, l'information policière constitue pour les enquêtes de renseignement une information contextuelle historique indispensable des antécédents judiciaires et administratifs concernant des individus ou des données à caractère personnel permettant d'enrichir les informations du renseignement et de répondre aux questions investigatives visant à identifier des personnes, à les localiser (par exemple, tel individu a été verbalisé à tel endroit pour un excès de vitesse permet de le localiser à un moment précis), d'établir des liens entre elles et de définir leurs activités en vue d'évaluer si elles représentent une menace au sens de l'article 8 et de l'art. 11 de la Loi organique des services de renseignement et de sécurité du 30 novembre 1998 (LRS) et d'aider à la prise de décisions politiques, administratives et judiciaires.

D'un point de vue méthodologique, les finalités des services de renseignement et de sécurité impliquent que la formulation d'hypothèses de recherche est au départ très large et se restreint progressivement au travers de la sélection de données à chaque étape du questionnement investigatif pour détecter des targets et des menaces potentielles. Pour les services de renseignement et de sécurité, c'est sur l'utilisation des données, leur sélection, au fil des étapes de la recherche qu'est évaluée la proportionnalité. C'est cette sélection de données pertinentes, dans le contexte de la recherche, qui doit être traitée par les services de renseignements et de sécurité avec la plus grande discrétion.

Il est tellement évident que les données policières sont essentielles à l'exécution des missions des services de renseignement et de sécurité que le principe de l'accès à ces données policières pour les services de renseignement et de sécurité est inscrit dans la [loi sur la fonction de police] depuis 2014 et dans la LRS depuis 2010.

Toutefois, si le besoin est reconnu, la forme actuelle de la communication des données n'est pas idoine et l'appel de la Commission d'enquête parlementaire ' attentats ' dans ses recommandations d'améliorer le partage d'informations doit être comprise dans ce sens.

En effet, actuellement, bien que les échanges d'informations entre les services de police et les services de renseignement soient constants, ils sont réalisés par des mécanismes *ad hoc* au travers de relais formels comme les deux officiers de liaison VSSE auprès de la Police fédérale, ou l'officier de liaison de SGRS ou de contacts ponctuels entre enquêteurs dans des dossiers concrets ou à l'occasion de plateformes de travail (comme entre autres, les LTF et les groupes de travail du Plan R) ou via les mécanismes d'assistance technique ou d'accords informels pris sur la transmission systématique de certains documents sous format mail (par exemple, RIR/RAR en matière de terrorisme), mais souvent aussi à la demande d'un enquêteur des

services de renseignement et de sécurité qui transmet sa question investigative à un interlocuteur policier, choisi souvent sur base géographique ou thématique. Si ces échanges sont nombreux, ils ne sont pas standardisés et normalisés. Ils ne concernent souvent que des dossiers où une collaboration existe et permettent difficilement de faire des liens transversaux. Ils requièrent de nombreuses opérations manuelles et par conséquent mobilisent beaucoup de ressources humaines. En termes de sécurité (discrétion des recherches) et de protection des données (minimisation), ces échanges nécessitent en outre des mesures afin de répondre aux obligations de traçabilité et aux nouvelles obligations légales de protection des enquêtes, des sources et de l'identité des agents de renseignement prévues entre autres par la loi relative à la protection des données.

En n'ayant pas accès direct à l'ensemble des informations policières pertinentes pour leurs missions, les services de renseignement et de sécurité se voient forcés de confier/déléguer/transférer de manière inadéquate la recherche, c'est-à-dire la sélection des données, d'un investigateur des services de renseignement et de sécurité - en principe, seul à être investi de cette mission - à potentiellement de multiples interlocuteurs de la Police qui détiennent chacun une partie de la connaissance/de l'accès, en fonction de leur rôle par rapport à l'objet de l'enquête, avec un résultat incertain en ce qui concerne la pertinence.

Par ailleurs, la communication de données ne permet pas aux services de renseignement et de sécurité de s'appuyer sur les informations policières et de les valoriser pleinement dans le cadre renseignement comme base contextuelle pour détecter des menaces potentielles et initier des enquêtes nouvelles.

C'est pourquoi, pour des raisons d'efficacité dans la détection des menaces, de sécurité, d'économie, d'enrichissement et de coordination, et pour préserver la présomption d'innocence et le droit au respect de la vie privée, il est nécessaire qu'un accès direct automatisé à la B.N.G. soit accordé aux services de renseignement et de sécurité » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 39-41).

« Premièrement, pour ce qui concerne la nécessité de conférer un accès direct à la B.N.G. et non une interrogation directe, il s'agit de rappeler que l'interrogation directe est un modèle sous la forme d'un HIT (entité connue)/NO HIT (entité pas connue) avec en cas de HIT un peu d'informations complémentaires dans la réponse fournie. Ceci ne permet pas aux services de renseignement de remplir utilement leurs missions légales. En effet, le modèle de HIT/NO HIT est essentiellement un modèle binaire. On interroge la B.N.G. à propos d'une entité (une personne, un numéro, une plaque, par exemple) et on reçoit une réponse (partielle) uniquement pour ladite entité. Ce dont les services de renseignement ont besoin pour pouvoir remplir correctement leurs missions, c'est une vue sur le modèle relationnel qui est sous-jacent à la construction de la B.N.G. c'est-à-dire voir l'ensemble des liens entre les entités (voir que telle personne est en lien avec tels faits et que ces faits sont en liens avec d'autres personnes, qui par ailleurs sont connues et liées à des rapports d'informations). Seul un accès direct à la B.N.G. permet aisément d'accéder à ce modèle relationnel. Il ne s'agit bien entendu pas en conférant un accès direct de mettre les services de renseignement sur le même pied que les autorités judiciaires ou de police administrative. En effet, l'accès direct à la B.N.G. ne change en rien la portée des missions légales des services de renseignement mais permet simplement de leur donner ce dont ils ont besoin pour les exercer au mieux.

Deuxièmement, l'Organe de contrôle a des doutes quant à la proportionnalité d'un accès direct pour les services de renseignement. Cependant, force est de constater que dans le cadre des dossiers relatifs au terrorisme, au radicalisme et à l'extrémisme, … il est nécessaire de connaître, dans le respect des règles de gestion de la B.N.G., tous les antécédents d'une personne, du plus anodin, au plus grave pour se former une image de la dangerosité de la personne ou pour enquêter sur elle (par exemple un PV de roulage tel jour à tel endroit signifie que la voiture immatriculée au nom de cette personne se trouve tel jour à tel endroit). Le législateur a voulu que les services de renseignement puissent travailler de manière exploratoire (ils ne sont pas tenus comme la police à des infractions) et c'est donc logique qu'ils puissent tout voir en ce qui concerne la B.N.G.. C'est aux services de renseignement qu'il appartient ensuite de faire le tri et il n'est pas opérationnellement défendable que ce tri soit fait préalablement. Il est aussi important de noter que l'accès direct ne porte que sur la B.N.G. et pas sur toute l'information des services de police (il n'y a par exemple pas d'accès direct possible pour les banques de données de base). Cet accès direct ne constitue pas une violation de la présomption d'innocence puisque comme mentionné *supra*, les services de renseignement travaillent, bien entendu dans le cadre de leurs missions légales, avec un modèle exploratoire : ce n'est donc pas parce qu'une personne fait l'objet de recherche de la part de services de renseignement qu'elle est coupable. En ce qui concerne l'immixtion dans la vie privée que constitue une consultation d'une banque de données, c'est une question transversale à toutes les consultations et elle n'est pas propre aux services de renseignement » (*Doc. parl.*, Chambre, 2018-2019, DOC 54-3697/001, pp. 43-44).

B.69.3. Les missions légales des services de police diffèrent de celles des services de renseignement et de sécurité. Ces missions sont toutefois compatibles entre elles en tant qu'elles participent, de manière générale, à la sécurité nationale.

Compte tenu du fait que l'accès direct à la B.N.G. qui est accordé aux services de renseignement et de sécurité a pour but de permettre à ces services de disposer d'un accès le plus large possible aux informations disponibles dans le cadre de leurs missions légales - lesquelles s'exercent, comme il a été souligné dans les travaux préparatoires, dans le respect de la présomption d'innocence -, il n'est pas disproportionné en regard des objectifs poursuivis par le législateur d'attribuer à ces services un accès direct à la B.N.G.

Le Comité permanent P, le Comité permanent R et l'Organe de contrôle ont en outre pour mission de contrôler les services de police et les services de renseignements et de sécurité. Les missions confiées par la loi du 30 juillet 2018 au Comité permanent R et à l'Organe de contrôle concernent précisément le fait de veiller à ce que les services de renseignement et de sécurité et les services de police respectent les dispositions de cette loi et ce, en vue de garantir le droit au respect de la vie privée. En vertu de l'article 1er de la loi du 18 juillet 1991 « organique du

contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace », le contrôle qu'exercent le Comité permanent P et le Comité permanent R porte en particulier sur « la protection des droits que la Constitution et la loi confèrent aux personnes ». En vertu de l'article 236, § 3, de la loi du 30 juillet 2018, l'Organe de contrôle est chargé, en particulier, de contrôler le respect des règles d'accès direct à la B.N.G.

B.69.4. Compte tenu de la compatibilité des finalités de traitement poursuivies par les services de police et par les services de renseignement et de sécurité, d'une part, et du contrôle exercé par Comité permanent P, par le Comité permanent R et par l'Organe de contrôle de l'information policière, d'autre part, les dispositions attaquées ont ménagé un juste équilibre entre le droit au respect de la vie privée et les objectifs poursuivis en matière de protection de la sécurité nationale.

B.69.5. Le moyen unique, en sa sixième branche, n'est pas fondé.

Par ces motifs,

la Cour,

sous réserve de l'interprétation mentionnée en B.14.5 et compte tenu de ce qui est dit en B.46.3, rejette le 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 10 mars 2022.

Le greffier, Le président,

P.-Y. Dutilleux P. Nihoul