Numéro du rôle : 7023
Arrêt n° 27/2020 du 20 février 2020

A R R Ê T

En cause : le recours en annulation de 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 », introduit par l'ASBL « Liga voor Mensenrechten ».

La Cour constitutionnelle,

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

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 15 octobre 2018 et parvenue au greffe le 16 octobre 2018, l'ASBL « Liga voor Mensenrechten », assistée et représentée par Me D. Pattyn, avocat au barreau de Flandre occidentale, a introduit un recours en annulation de 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 » (publiée au *Moniteur belge* du 16 avril 2018).

Le Conseil des ministres, assisté et représenté par Me S. Sottiaux et Me E. Cloots, avocats au barreau d'Anvers, et Me H. Graux et Me M. Van Der Sype, 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 18 décembre 2019, la Cour, après avoir entendu les juges-rapporteurs L. Lavrysen et J.-P. Moerman, en remplacement du juge honoraire J.-P. Snappe, 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 15 janvier 2020 et l'affaire mise en délibéré.

Aucune demande d'audience n'ayant été introduite, l'affaire a été mise en délibéré le 15 janvier 2020.

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

II. *En droit*

- A -

A.1. La partie requérante, l'ASBL « Liga voor Mensenrechten », demande l'annulation de 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 » (ci-après : la loi du 21 mars 2018).

Quant à la recevabilité

A.2. Le Conseil des ministres affirme que le recours de la partie requérante est en réalité dirigé contre plusieurs dispositions spécifiques de la loi du 21 mars 2018. Il ressort de l'exposé des moyens que le premier moyen vise les articles 6, 9, 11, 35, 60, 69, 70, 71, 75 et 80 de la loi du 21 mars 2018, alors que le second moyen est dirigé contre les articles 6, 9, 12, 28, 35, 48, 49, 50, 60, 69, 70, 71, 75, 80, 84 et 85 de la loi. En ce qu'elle demande l'annulation de l'ensemble de la loi du 21 mars 2018, la requête doit être rejetée pour cause d'irrecevabilité.

Le Conseil des ministres soulève ensuite l'irrecevabilité partielle des moyens en ce que la partie requérante invoque la violation directe d'articles de la Convention européenne des droits de l'homme et de la Charte des droits fondamentaux de l'Union européenne ainsi que de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », étant donné que la Cour n'est pas compétente pour exercer un contrôle direct au regard de ces dispositions.

A.3. La partie requérante conteste l'exception d'irrecevabilité. Elle souligne qu'elle allègue, pour chaque moyen et chaque branche, la violation des articles 10, 11 et 22 de la Constitution. La Cour peut prendre en compte des dispositions de droit international qui garantissent des droits et libertés analogues. Lorsqu'est invoquée la violation d'un droit fondamental, la Cour peut en outre exercer un contrôle au regard des articles 10 et 11 de la Constitution. En effet, toute violation d'un droit fondamental emporte également la violation du principe d'égalité et de non-discrimination.

La partie requérante ajoute qu'elle n'invite pas la Cour à contrôler directement la loi attaquée au regard de la loi précitée du 30 juillet 2018, mais seulement au regard de cette loi lue en combinaison avec le droit de l'Union, dont elle constitue l'exécution ou la transposition, et avec les articles 10, 11 et 22 de la Constitution.

A.4. Dans son mémoire en réplique, le Conseil des ministres persiste en ses griefs relatifs à l'irrecevabilité partielle des moyens. Il ressort clairement de la requête que la partie requérante invoque directement la violation de dispositions de la Convention européenne des droits de l'homme et de la Charte, au lieu d'invoquer la violation des articles 10, 11 et 22 de la Constitution, lus en combinaison avec d'autres dispositions de conventions internationales et européennes. Qui plus est, la Cour ne peut exercer de contrôle au regard de la loi du 30 juillet 2018, puisqu'elle peut uniquement effectuer son contrôle au regard de dispositions législatives si et pour autant que celles-ci contiennent des règles répartitrices de compétence.

Quant au premier moyen

A.5. La partie requérante prend un premier moyen de la violation, par les articles 6, 9, 11, 35, 60, 69, 70, 71, 75 et 80 de la loi du 21 mars 2018, des articles 10, 11 et 22 de la Constitution, lus ou non en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne et avec les articles 4, 5, 6 et 7 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 (UE) 2016/680). Le moyen porte sur les délais de conservation des informations et données à caractère personnel enregistrées.

Selon la partie requérante, la loi du 21 mars 2018 constitue une ingérence dans le droit au respect de la vie privée, en ce qu'elle prévoit la possibilité de conserver durant douze mois les informations et les données à caractère personnel collectées grâce aux caméras de police et la possibilité de conserver durant trois mois des images enregistrées par des caméras de surveillance.

Cette ingérence est disproportionnée par rapport aux buts légitimes poursuivis. En premier lieu, le délai de conservation dans le cadre de l'utilisation des caméras de police porte de manière générale sur toutes les informations et données à caractère personnel qui sont collectées par l'utilisation de caméras, alors que le délai de conservation dans le cadre de l'utilisation ordinaire de caméras est différencié de manière limitée. Ensuite, la loi du 21 mars 2018 ne contient pas de règles claires et précises, ni d'exigences minimales qui permettent de déterminer le délai de conservation concret. Le Roi dispose d'un pouvoir d'appréciation étendu pour les « lieux qui, en raison de leur nature, sont sujets à un risque particulier pour la sécurité ». Enfin, la loi du 21 mars 2018 n'interdit aucun traitement dérivé ou indirect des données conservées par les autorités concernées, même après l'expiration des délais de conservation et d'accès.

A.6. Selon le Conseil des ministres, l'utilisation normale des caméras de surveillance sur la voie publique ou à des endroits accessibles au public ne constitue pas en soi une ingérence dans le droit au respect de la vie privée, mais l'existence d'une ingérence doit être appréciée cas par cas par les juridictions compétentes. Il en va d'autant plus ainsi s'il s'agit de caméras utilisées pour la reconnaissance des plaques d'immatriculation, au lieu des caméras de surveillance ordinaires.

Si la loi du 21 mars 2018 constituait néanmoins une ingérence dans le droit au respect de la vie privée, cette ingérence est, à l'estime du Conseil des ministres, limitée. Les images et les informations susceptibles d'être obtenues à la suite de l'utilisation de caméras ne sont en effet pas intrinsèquement privées. Lorsqu'une personne se déplace sur la voie publique ou dans un lieu accessible au public, elle ne saurait avoir d'attentes raisonnables en matière de respect de la vie privée. Il en est d'autant plus ainsi lorsque des caméras sont utilisées en vue de la reconnaissance des plaques d'immatriculation. L'ingérence dans le droit au respect de la vie privée est de ce fait, selon le Conseil des ministres, d'un tout autre ordre que l'ingérence que la directive sur la conservation des données constituait dans ce même droit.

En tout état de cause, l'ingérence dans le droit au respect de la vie privée est objectivement justifiée. Elle est prévue par une disposition législative suffisamment précise et poursuit des objectifs légitimes, plus précisément garantir la sécurité nationale et la sûreté publique, défendre l'ordre et prévenir les infractions pénales et protéger les droits et libertés d'autrui.

Enfin, l'ingérence est proportionnée aux buts poursuivis. En ce qui concerne l'utilisation de caméras de police, le législateur a prévu plusieurs garanties. En premier lieu, le délai de conservation de principe de douze mois est un délai maximum et les données collectées ne peuvent être conservées plus longtemps que nécessaire. En deuxième lieu, le délai de conservation maximum de douze mois est réduit, dans certains cas d'utilisation non visible de caméras. En troisième lieu, les services de police sont tenus de déterminer préalablement la durée de conservation nécessaire pour atteindre leurs objectifs. En quatrième lieu, l'accès aux données et aux informations collectées n'est en principe possible qu'au cours du premier mois de conservation, l'accès étant ensuite subordonné à des circonstances et habilitations particulières. En cinquième lieu, l'accès aux données et aux informations collectées doit toujours être motivé, tant au cours du premier mois d'observation qu'ultérieurement. En sixième lieu, plusieurs mécanismes de contrôle ont été prévus afin d'assurer que les services de police respectent les conditions légales de manière effective.

Pour l'utilisation ordinaire de caméras, il existe également un certain nombre de garanties. En premier lieu, le délai de trois mois est seulement un délai maximum. En deuxième lieu, le délai de conservation de trois mois au maximum représente une exception au délai général de conservation d'un seul mois et ne peut être applicable qu'aux lieux qui, en raison de leur nature, emportent un risque particulier pour la sécurité. Enfin, la liste de tels lieux doit être soumise pour avis à l'Autorité de protection des données.

A.7. Dans son mémoire en réponse, la partie requérante ajoute que la loi du 21 mars 2018 ne contient pas de dispositions législatives suffisamment précises. La loi est à ce point complexe qu'elle ne satisfait pas aux exigences de prévisibilité et d'accessibilité.

A.8. Dans son mémoire en réplique, le Conseil des ministres conteste le fait que les délais de conservation n'aient pas été prescrits par une disposition législative suffisamment précise. En premier lieu, l'argument est irrecevable, puisqu'il s'agit d'un moyen nouveau et que la partie requérante étend ainsi de manière inadmissible son recours en annulation. Quoi qu'il en soit, l'argument est fallacieux. Les délais de conservation sont, dans une certaine mesure, complexes, mais cette complexité est inévitable si l'on veut trouver un juste équilibre entre, d'une part, le droit au respect de la vie privée et, d'autre part, les objectifs légitimes poursuivis par le législateur. Les délais de conservation sont suffisamment prévisibles, car ils sont réglés de manière particulièrement détaillée. Le législateur a opté pour des délais maximaux concrets qui diffèrent selon le type d'utilisation des caméras, au lieu de reproduire la norme ouverte contenue dans des normes européennes et internationales.

En ce qui concerne le second moyen

A.9. La partie requérante prend un second moyen de la violation, par les articles 6, 9, 12, 28, 35, 48, 49, 50, 61, 84, 85 et 86 de la loi du 21 mars 2018, des articles 10, 11, 12, 14 et 22 de la Constitution, lus ou non en combinaison avec les articles 6, 7 et 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 47, 48 et 52 de la Charte des droits fondamentaux de l'Union européenne, avec les articles 4, 5, 6 et 7 de la directive (UE) 2016/680, avec le principe général du droit à un procès équitable et avec le droit de défense ainsi qu'avec le principe de légalité en matière pénale. Le moyen porte sur le traitement des informations et données à caractère personnel collectées.

Dans la première branche, la partie requérante fait valoir que la loi du 21 mars 2018 entraîne une ingérence disproportionnée dans le droit au respect de la vie privée en ce qu'elle autorise l'utilisation non visible de caméras de police, en ce qu'elle donne aux services de renseignement et de sécurité accès aux données conservées sur la base de la loi, en ce qu'elle habilite les services de police et les services de renseignement et de sécurité à mettre ces données en corrélation avec d'autres données définies dans la loi et en ce qu'elle habilite les services de renseignement et de sécurité à procéder, via cet accès et cette corrélation, à une observation en utilisant des moyens techniques. En effet, la loi du 21 mars 2018 n'autorise pas seulement le traitement de données en vue de lutter contre la criminalité grave ou pour des raisons graves d'ordre public ou de sécurité publique.

Dans la deuxième branche, la partie requérante soutient que la loi attaquée est également disproportionnée en ce que l'accès aux données n'est pas soumis à un contrôle préalable effectué par une juridiction ou par une autorité administrative indépendante.

Dans la troisième branche, la partie requérante estime que la loi du 21 mars 2018 viole le principe de légalité. Les ministres de l'Intérieur et de la Justice, ainsi que le Roi, reçoivent des habilitations étendues et illimitées afin de prendre des mesures en ce qui concerne les interconnexions et les corrélations avec les banques de données techniques et l'accès direct, par les services de renseignement et de sécurité, aux données collectées grâce à l'usage de caméras de police.

Enfin, la partie requérante estime, dans la quatrième branche, que la loi du 21 mars 2018 est contraire au principe d'égalité et de non-discrimination. La mise en corrélation de données obtenues grâce à l'utilisation de caméras de police et l'observation au sens de l'article 47*sexies* du Code d'instruction criminelle sont comparables. Or, la mise en corrélation de données n'est pas soumise aux mêmes garanties, sans qu'existe pour ce faire une justification objective et raisonnable. Le principe de légalité en matière pénale serait ainsi également violé. Étant donné que la loi du 21 mars 2018 ne prévoit pas davantage un contrôle juridictionnel effectif de la mise en corrélation de données et de l'accès à ces données, celle-ci viole aussi le droit à un procès équitable et le droit de défense.

A.10. Le Conseil des ministres affirme que la première branche est irrecevable en ce qu'elle indique uniquement les règles qui seraient violées par la loi du 21 mars 2018 et non en quoi ces règles seraient violées. La partie requérante ne procède qu'à un examen partiel, étant donné qu'elle ne tient pas compte de tous les motifs de justification de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme. En tout état de cause, le droit au respect de la vie privée n'est pas violé. Une ingérence peut être admissible non seulement en vue de lutter contre la criminalité grave, mais également en cas de raison grave d'ordre public ou de sécurité publique. L'ingérence poursuit plusieurs objectifs légitimes, à savoir garantir la sécurité nationale et la sûreté publique, défendre l'ordre et prévenir les infractions pénales et protéger les droits et libertés d'autrui. Ensuite, l'ingérence est prescrite par une disposition législative suffisamment précise. Elle est

également proportionnée aux buts légitimes poursuivis en raison des diverses garanties, de l'approche différenciée et des mesures de contrôle prévues par la loi du 21 mars 2018.

La deuxième branche est partiellement irrecevable parce que la partie requérante développe uniquement des arguments concernant la violation alléguée du droit au respect de la vie privée et n'indique pas en quoi la loi du 21 mars 2018 violerait le principe d'égalité et de non-discrimination. En tout état de cause, un contrôle préalable effectué par une juridiction ou par une entité administrative indépendante n'est pas une exigence absolue pour avoir accès aux données et la loi du 21 mars 2018 prévoit suffisamment de garanties pour ce qui est de l'utilisation de caméras par les services de police.

Contrairement à ce que prétend la partie requérante dans la troisième branche, il n'est nullement question d'habilitations étendues et illimitées aux ministres de l'Intérieur et de la Justice, ainsi qu'au Roi. Les habilitations sont décrites en des termes suffisamment précis et sont limitées à la mise en œuvre de mesures dont les éléments essentiels ont été fixés au préalable par le législateur. Elles ne confèrent aucun pouvoir réglementaire aux ministres.

La quatrième branche est irrecevable en ce qu'elle est prise de la violation de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme et avec les articles 7 en 8 de la Charte des droits fondamentaux de l'Union européenne. En effet, la partie requérante développe uniquement des arguments concernant le principe d'égalité et de non-discrimination. Ce principe n'est pas violé parce que la différence de traitement entre la mise en corrélation de données obtenues grâce à l'usage de caméras de police et l'observation au sens de l'article 47*sexies* du Code d'instruction criminelle est raisonnablement justifiée. La différence de traitement repose sur un critère objectif, car l'observation a lieu dans des circonstances différentes. Elle poursuit un but légitime, étant donné que la corrélation a pour objet de soutenir le travail de la police et de le rendre plus efficace. La distinction est pertinente, car la corrélation exploite des informations qui ont déjà été soumises à un contrôle. Enfin, la différence de traitement est proportionnée en raison des restrictions, des autorisations et des garanties prévues par la loi du 21 mars 2018. Par ailleurs, un contrôle juridictionnel n'est pas nécessaire au moment de la corrélation et de l'accès aux données, étant donné que la loi du 21 mars 2018 garantit déjà un contrôle suffisant. Pour cette raison, le droit de défense et le droit à un procès équitable ne sont pas davantage violés.

A.11. Dans son mémoire en réponse, la partie requérante réfute le fait que les garanties citées par le Conseil des ministres assurent la proportionnalité de l'ingérence ou offrent une protection suffisante contre les abus et l'arbitraire. La partie requérante conteste également qu'il existe une justification raisonnable à la différence de traitement entre la mise en corrélation de données et l'observation, ce qui implique que les garanties applicables dans le cadre d'une observation au sens de l'article 47*sexies* du Code d'instruction criminelle sont entièrement vidées de leur substance.

A.12. En ce qui concerne ce dernier point, le Conseil des ministres se réfère au rôle de l'Organe de contrôle, visé dans la loi précitée du 30 juillet 2018, qui a pour mission de contrôler, au moyen d'enquêtes, si le contenu des banques de données, de même que la procédure de traitement des données contenues dans ces banques de données, satisfont aux exigences légales.

- B -

Quant aux dispositions attaquées

B.1. La partie requérante demande l'annulation de 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 » (ci-après : la loi du 21 mars 2018).

Il ressort du contenu de la requête que les griefs sont uniquement dirigés contre les articles 6, 9, 11, 12, 28, 35, 48, 49, 50, 60, 61, 69, 70, 71, 75, 80, 84, 85 et 86 de la loi attaquée. La Cour limite son examen à ces dispositions.

S'il devait apparaître de l'examen plus approfondi des moyens que seuls certains des articles précités ou seules certaines parties de ces dispositions sont critiqués, l'examen sera, le cas échéant, limité à ces dispositions.

B.2.1. La loi du 21 mars 2018 modifie la réglementation sur l'utilisation et l'installation de caméras de surveillance. La loi tente « de garantir au mieux la vie privée des citoyens, tout en maintenant un équilibre avec les réalités et les besoins pratiques du terrain » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-2855/001, p. 5).

Ainsi qu'il ressort de l'intitulé, la loi attaquée modifie quatre autres lois.

B.2.2. La loi du 21 mars 2018 modifie en premier lieu la loi du 5 août 1992 « sur la fonction de police » (ci-après : la loi du 5 août 1992). Elle tend à retirer les caméras des services de police du champ d'application de la loi du 21 mars 2007 « réglant l'installation et l'utilisation de caméras de surveillance » (ci-après : la loi du 21 mars 2007) afin de régler leur utilisation dans la loi du 5 août 1992 et entend ainsi « élaborer un régime particulier pour l'utilisation de caméras par les services de police, tant dans le cadre de leurs missions de police administrative que de police judiciaire » (*ibid.*, p. 3).

La loi du 21 mars 2018 règle l'autorisation conférée aux services de police pour installer et utiliser des caméras ainsi que le traitement des données collectées. Elle autorise dans certains cas l'utilisation non visible de caméras et encadre l'utilisation des données recueillies par des caméras de reconnaissance automatique des plaques d'immatriculation (ANPR) (*ibid.*, pp. 3 et 4).

Les modifications apportées à la loi du 5 août 1992 figurent dans le chapitre 2 de la loi du 21 mars 2018 (articles 2 à 62).

B.2.3. La loi du 21 mars 2018 modifie également la loi précitée du 21 mars 2007, d'une part, pour lever certains doutes et difficultés d'application de certaines dispositions de la loi du 21 mars 2007 et, d'autre part, pour adapter la loi aux développements au niveau européen (*ibid.*, p. 4).

La loi du 21 mars 2007 est applicable à l'installation et à l'utilisation de caméras de surveillance dans le but de prévenir, de constater ou de déceler des infractions contre les personnes ou les biens (article 3, alinéa 1er, 1°) ou de prévenir, de constater ou de déceler des incivilités au sens de l'article 135 de la Nouvelle loi communale, de contrôler le respect des règlements communaux ou de maintenir l'ordre public (article 3, alinéa 1er, 2°).

La loi du 21 mars 2018 insère dans la loi du 21 mars 2007 de nouvelles règles en vue de l'utilisation de caméras de surveillance mobiles intelligentes et des mesures particulières dans des situations où elles sont justifiées par la nature des lieux et le risque pour la sécurité, notamment en vue de conserver les images durant trois mois au lieu d'un mois, de filmer le périmètre d'un lieu et de donner aux services de police accès aux images en temps réel (*ibid.*, pp. 4 et 5).

Les modifications de la loi du 21 mars 2007 figurent dans le chapitre 3 de la loi du 21 mars 2018 (articles 63 à 83).

B.2.4. La loi du 21 mars 2018 modifie ensuite la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité » (ci-après : la loi du 30 novembre 1998). Dans l'intérêt de l'exercice de leurs missions et sous certaines conditions, les services de renseignement et de sécurité peuvent avoir accès aux caméras que peuvent utiliser les services de police et aux banques de données contenant les données à caractère personnel et les informations de celles-ci (*ibid.*, p. 5).

Les modifications de la loi du 30 novembre 1998 figurent dans le chapitre 4 de la loi du 21 mars 2018 (articles 84 à 86).

B.2.5. Enfin, la loi du 21 mars 2018 modifie la loi du 2 octobre 2017 « réglementant la sécurité privée et particulière », en réglant la compétence des agents de gardiennage pour visionner les images des caméras installées sur la voie publique (*ibid.*, p. 5).

Ces modifications figurent dans le chapitre 5 de la loi du 21 mars 2018 (article 87), qui n'est pas visé par la requête.

Quant à la recevabilité

B.3.1. Le Conseil des ministres conteste la recevabilité du recours en annulation en ce que la Cour est invitée à se prononcer sur la compatibilité de la loi attaquée avec des articles de la Convention européenne des droits de l'homme et de la Charte des droits fondamentaux de l'Union européenne et avec la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ».

B.3.2. Les dispositions internationales au regard desquelles la Cour ne peut exercer un contrôle direct sont invoquées en combinaison avec des dispositions constitutionnelles au regard desquelles la Cour peut exercer un contrôle direct, de sorte que toutes ces dispositions doivent être lues conjointement.

B.3.3. La Cour n'est toutefois pas compétente pour contrôler des dispositions législatives au regard d'autres dispositions législatives qui ne sont pas des règles répartitrices de compétences.

Le grief pris de la violation la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » est irrecevable.

Quant au fond

B.4.1. Le premier moyen est pris de la violation des articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne et avec les articles 4, 5, 6 et 7 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 (UE) 2016/680).

B.4.2. Le second moyen est pris de la violation des articles 10, 11, 12, 14 et 22 de la Constitution, lus ou non en combinaison avec les articles 6, 7 et 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 47, 48 et 52 de la Charte des droits fondamentaux de l'Union européenne, avec les articles 4, 5, 6 et 7 de la directive (UE) 2016/680, avec le principe général du droit à un procès équitable et du droit de défense et avec le principe de légalité en matière pénale.

B.4.3. Les deux moyens portent en substance sur le droit au respect de la vie privée. Ils visent les délais de conservation des informations et des données à caractère personnel enregistrées (premier moyen) et le traitement de ces informations et données (première et deuxième branches du second moyen).

Le second moyen (troisième et quatrième branches) porte en outre sur le principe de légalité et sur le principe d'égalité et de non-discrimination.

Quant au droit au respect de la vie privée

B.5. Selon la partie requérante, la possibilité prévue par la loi du 21 mars 2018 de conserver durant douze mois les informations et données à caractère personnel recueillies par les caméras de police et de conserver durant trois mois les images enregistrées par des caméras de surveillance constitue une ingérence disproportionnée dans le droit au respect de la vie privée (premier moyen). Le traitement des informations et données à caractère personnel recueillies, prévu par la loi attaquée, constituerait également une ingérence disproportionnée dans le droit au respect de la vie privée (première et deuxième branches du second moyen).

B.6.1. 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.6.2. 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.6.3. 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.6.4. 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.

Ce droit a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles. La jurisprudence de la Cour européenne des droits de l'homme fait apparaître que les images de caméras, même si elles sont prises dans des lieux publics, relèvent de la protection de ce droit dès que les images sont enregistrées et traitées (voy. notamment CEDH, 18 octobre 2016, *Vukota-Bojić c. Suisse*, §§ 55-56; grande chambre, 17 octobre 2019, *López Ribalda e.a. c. Espagne*, §§ 89-90). Tel est notamment le cas lorsque les images permettent d'identifier des personnes et de savoir qui se trouve où et à quel moment.

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

B.7.1. L'article 7 de la Charte des droits fondamentaux de l'Union européenne dispose :

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

B.7.2. L'article 8 de la Charte des droits fondamentaux de l'Union européenne dispose :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

B.7.3. L'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, dispose :

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

B.7.4. L'article 52, paragraphe 3, de la Charte des droits fondamentaux de l'Union européenne, dispose :

« Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ».

B.7.5. La directive (UE) 2016/680 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 à la protection contre les menaces pour la sécurité publique et à la prévention de telles menaces, en respectant la nature spécifique de ces activités.

La partie requérante mentionne cette directive dans les deux moyens mais elle ne tire aucun grief concret de cette directive.

B.7.6. Par son arrêt n° 96/2018 du 19 juillet 2018, la Cour a, dans le cadre de recours en annulation dirigés contre la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques », posé trois questions préjudicielles à la Cour de justice de l'Union européenne concernant l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ».

L'enregistrement et le traitement d'images de caméras filmées dans la rue et dans le domaine public diffèrent cependant fondamentalement, en ce qui concerne le caractère privé des données, de l'enregistrement et du traitement de données de communication électronique, si bien que la Cour ne doit pas attendre la réponse à ces questions préjudicielles pour se prononcer sur l'actuel recours.

L'enregistrement et le traitement d'images de caméras constituent, de par la nature de ces images, une ingérence dans la vie privée moins intrusive que l'enregistrement et le traitement de données de communication électronique. En effet, d'une part, les attentes en matière de respect de la vie privée sont moins importantes dans l'espace public que dans la sphère privée et, d'autre part, les images affectent moins en règle générale la vie privée que les données de communication.

Ce dernier constat est conforté par le fait que la loi attaquée exclut l'enregistrement et le traitement d'images qui portent atteinte à l'intimité d'une personne ou qui tendent à recueillir des informations sur l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à une organisation syndicale, son état de santé, sa vie sexuelle ou son orientation sexuelle (article 25/3, § 3, inséré par l'article 8 de la loi du 21 mars 2018).

B.7.7. Le droit au respect de la vie privée n'est pas absolu. Les dispositions constitutionnelles et conventionnelles n'excluent pas une ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée, mais exigent que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit.

Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait ménagé 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 : 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).

Il découle de la nature différente des mesures, mentionnée en B.7.6, que la marge d'appréciation du législateur est plus étendue à l'égard de mesures d'enregistrement et de traitement d'images de caméras qu'à l'égard du même type de mesures qui concernent des données de communication.

B.8.1. La loi attaquée prévoit différents délais de conservation, qui sont clairement précisés dans les dispositions citées ci-après.

B.8.2. La conservation et l'enregistrement d'informations et de données à caractère personnel que la police recueille au moyen de caméras contribuent à garantir la sécurité publique, à protéger l'ordre public, à prévenir les infractions et à protéger les droits et libertés d'autrui. La mesure répond donc à un besoin social impérieux dans une société démocratique.

B.8.3. Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient de tenir compte notamment de leur caractère automatisé, des techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées, 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° 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).

B.8.4. Il ressort de la jurisprudence de la Cour européenne des droits de l'homme 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, la Cour européenne des droits de l'homme tient 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).

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

B.9.1. En ce qui concerne l'utilisation visible de caméras par la police, l'article 25/6 de la loi du 5 août 1992, inséré par l'article 11 de la loi du 21 mars 2018, dispose :

« Les informations et données à caractère personnel collectées au moyen de caméras, peuvent être enregistrées et conservées pour une durée n'excédant pas douze mois à compter de leur enregistrement, sauf si un autre délai est prévu dans la section 12 du présent chapitre ».

En ce qui concerne l'utilisation non visible de caméras par la police, l'article 46/12, alinéa 1er, de la loi du 5 août 1992, inséré par l'article 60 de la loi du 21 mars 2018, dispose :

« Les informations et données à caractère personnel collectées au moyen de caméras non visibles peuvent être enregistrées et conservées pour une durée n'excédant pas douze mois à compter de leur enregistrement, sauf si un autre délai est prévu dans la section 12 du chapitre IV ».

Ces dispositions sont également applicables aux services de police, lorsqu'ils ont accès en temps réel aux images de caméras de surveillance installées par d'autres responsables du traitement, en application de la loi du 21 mars 2007 ou d'autres lois, si cet accès implique un enregistrement des images au sein des services de police mêmes (article 25/1, § 2, de la loi du 5 août 1992, tel qu'il a été inséré par l'article 6 de la loi du 21 mars 2018).

En ce qui concerne les caméras de reconnaissance automatique des plaques d'immatriculation, l'article 44/11/3*decies* de la loi du 5 août 1992, inséré par l'article 35 de la loi du 21 mars 2018, dispose :

« § 1er. Les banques de données techniques créées suite à l'utilisation de caméras intelligentes de reconnaissance automatique de plaques d'immatriculation ou de systèmes intelligents de reconnaissance automatique de plaques d'immatriculation contiennent les données suivantes, si elles apparaissent sur les images des caméras :

1° la date, le moment et l'endroit précis du passage de la plaque d'immatriculation,

2° les caractéristiques du véhicule lié à cette plaque,

3° une photo de la plaque d'immatriculation à l'avant du véhicule et le cas échéant, à l'arrière,

4° une photo du véhicule,

5° le cas échéant, une photo du conducteur et des passagers,

6° les données de journalisation des traitements.

§ 2. Les données à caractère personnel et informations visées au paragraphe 1er peuvent être conservées pour une durée n'excédant pas douze mois à compter de leur enregistrement.

Dès que ces données entrent dans les conditions pour alimenter une banque de données visée à l'article 44/2 § 1er, 1° et 2°, elles y sont copiées et conservées, après validation manuelle dans un délai d'un mois après la réunion de ces conditions.

[…] ».

Les banques de données visées à l'article 44/2, § 1er, 1° et 2°, sont la Banque de données nationale générale et les banques de données de base. La Banque de données nationale générale est la banque de données policière qui contient les données et les informations dont les services de police ont besoin pour exercer leurs missions. Il s'agit par conséquent d'une banque de données nationale dont les données et les informations proviennent de divers services de police (voy. l'arrêt n° 108/2016 du 14 juillet 2016). 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).

B.9.2. Le délai de conservation de douze mois prévu par les dispositions précitées est un délai maximum, ainsi qu'il ressort des mots « n'excédant pas » et comme l'ont expressément confirmé les travaux préparatoires :

« Le fait qu'il s'agit d'un délai maximum permet de rencontrer le principe de proportionnalité, comme le remarque le Conseil d'État, dans son avis n° 62.006/2 du 9 octobre 2017 […]. En effet, de la même manière que les services de police doivent veiller au respect du principe de proportionnalité dans leur choix et leur manière d'utiliser des caméras, le délai de conservation des images est également un traitement qui doit respecter le principe de proportionnalité et correspondre aux finalités visées par les services de police » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-2855/001, p. 28).

Le délai de conservation de douze mois délimite ainsi clairement l'application du principe de proportionnalité par les services de police.

B.9.3. En ce qui concerne l'utilisation par la police de caméras non visibles, le législateur a lui-même prévu, à l'article 46/12 de la loi du 5 août 1992, plusieurs exceptions au délai de conservation maximum de douze mois, à savoir lorsque les informations et les données sont collectées dans le cadre de la préparation d'actions de police judiciaire et de maintien de l'ordre au cours de ces actions (article 46/12, alinéa 2, de la loi du 5 août 1992), dans le cadre de l'exécution de missions spécialisées de protection de personnes (article 46/12, alinéa 3) et dans le cadre de l'exécution de missions de transfert de détenus (article 46/12, alinéa 4).

Dans ces situations, les informations et les données ne peuvent être conservées que pendant la durée de l'action ou de la mission et elles ne peuvent être conservées et utilisées plus longtemps qu'afin de prouver des faits punissables constatés par hasard ou pour en identifier les auteurs. Ainsi qu'il ressort des travaux préparatoires, cette prolongation n'est possible que lorsque les faits punissables ont été constatés pendant le délai originaire sur la base de ces données (*ibid.*, p. 56).

B.9.4. En ce qui concerne l'utilisation par la police de caméras visibles, le législateur a soumis l'installation et l'utilisation des caméras concernées à l'autorisation de principe préalable du conseil communal, lorsqu'il s'agit d'une zone de police, ou du ministre de l'Intérieur ou de son délégué, pour les services de la police fédérale (article 25/4, § 1er, de la loi du 5 août 1992, inséré par l'article 9 de la loi du 21 mars 2018).

La demande d'autorisation doit prendre en compte une analyse d'impact et de risques au niveau de la protection de la vie privée et au niveau opérationnel, notamment quant aux catégories de données à caractère personnel traitées, à la proportionnalité des moyens mis en œuvre, aux objectifs opérationnels à atteindre et à la durée de conservation des données nécessaire pour atteindre ces objectifs (article 25/4, § 2, alinéa 2, de la loi du 5 août 1992, inséré par l'article 9 de la loi du 21 mars 2018).

B.9.5. En ce qui concerne les caméras de reconnaissance automatique des plaques d'immatriculation, les données peuvent être conservées dans la Banque de données nationale générale et dans les banques de données de base (article 44/11/3*decies*, § 2, alinéa 2, de la loi du 5 août 1992, inséré par l'article 35 de la loi du 21 mars 2018).

Les articles 44/9 et 44/10 de la loi du 5 août 1992 fixent les règles relatives à la durée de conservation des données à caractère personnel et des informations dans la Banque de données nationale générale et 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 fixe les règles relatives à la conservation des données contenues dans les banques de données de base. Par son arrêt n° 108/2016, précité, la Cour a rejeté le recours en annulation de ces dispositions (B.112-B.116).

B.9.6. Le délai de conservation doit ensuite être distingué du délai d'accès. L'accès aux données concernées est réglé différemment pour les missions de police administrative et pour les missions de police judiciaire. Les missions de police administrative portent en substance sur le maintien de l'ordre public. Les missions de police judiciaire portent en substance sur la recherche et la constatation d'infractions.

L'accès aux données à caractère personnel et aux informations recueillies par l'utilisation tant visible que non visible de caméras est autorisé au cours d'une période d'un mois à compter de leur enregistrement, à condition qu'il soit motivé sur le plan opérationnel et nécessaire pour l'exercice d'une mission précise. Cet accès porte sur les missions de police administrative. Après le premier mois de conservation, l'accès à ces données à caractère personnel et informations n'est possible qu'à des fins de police judiciaire, moyennant une décision écrite et motivée du procureur du Roi ou, pour ce qui concerne l'utilisation non visible de caméras, du juge d'instruction (articles 25/7 et 46/13 de la loi du 5 août 1992, insérés respectivement par les articles 12 et 61 de la loi du 21 mars 2018).

En cas de reconnaissance automatique des plaques d'immatriculation, le législateur a établi une distinction encore plus détaillée. L'article 44/11/3*decies*, §§ 3 et 4, de la loi du 5 août 1992, inséré par l'article 35 de la loi du 21 mars 2018, dispose :

« § 3. Le traitement des données à caractère personnel et informations visées au paragraphe 1er, pour des recherches ponctuelles dans le cadre des missions de police administrative, dans le respect des finalités visées à l'article 44/11/3*septies*, est autorisé pendant une période d'un mois à compter de leur enregistrement, à condition qu'il soit motivé sur le plan opérationnel et nécessaire pour l'exercice d'une mission précise. La décision est prise soit par un directeur ou les officiers de police administrative qu'il désigne, lorsqu'il s'agit d'un service qui appartient à la police fédérale, soit par le chef de corps ou les officiers de police administrative qu'il désigne, lorsqu'il s'agit d'une zone de police.

Le traitement des données à caractère personnel et informations visées au paragraphe 1er pour des recherches ponctuelles dans le cadre des missions de police judiciaire, dans le respect des finalités visées à l'article 44/11/3*septies*, est autorisé pendant toute la période de conservation des données, à condition qu'il soit motivé sur le plan opérationnel et nécessaire pour l'exercice d'une mission précise. La décision est prise soit par un directeur ou les officiers de police judiciaire qu'il désigne, lorsqu'il s'agit d'un service qui appartient à la police fédérale,

soit par le chef de corps ou les officiers de police judiciaire qu'il désigne, lorsqu'il s'agit d'une zone de police, soit par le procureur du Roi. Après le premier mois de conservation, la décision est prise par le procureur du Roi et ne peut concerner que des infractions de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde.

§ 4. Dans le respect des finalités visées à l'article 44/11/3*septies*, les données à caractère personnel et informations visées au paragraphe 1er peuvent être mises en corrélation avec :

1° des listes auxquelles les services de police ont légalement accès ou des extraits de banques de données policières nationales ou internationales auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique;

2° des critères d'évaluation préétablis.

Le contenu des listes ou des extraits de banques de données visés à l'alinéa 1er, 1°, utilisés en vue d'une corrélation, est soumis à l'autorisation :

1° pour les missions police administrative : soit d'un directeur ou des officiers de police administrative qu'il désigne, lorsqu'il s'agit d'un service qui appartient à la police fédérale, soit du chef de corps ou des officiers de police administrative qu'il désigne, lorsqu'il s'agit d'une zone de police;

2° pour les missions de police judiciaire : soit d'un directeur ou des officiers de police judiciaire qu'il désigne, lorsqu'il s'agit d'un service qui appartient à la police fédérale, soit du chef de corps ou des officiers de police judiciaire qu'il désigne, lorsqu'il s'agit d'une zone de police, soit par le procureur du Roi.

Les critères d'évaluation visés à l'alinéa 1er, 2°, sont établis après approbation du délégué à la protection des données, ne peuvent viser l'identification d'un individu et doivent être ciblés, proportionnés et spécifiques. Ils ne peuvent être fondés sur des données qui révèlent l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à une organisation syndicale, son état de santé, sa vie ou son orientation sexuelle.

Les listes ou extraits de banques de données, ou les critères d'évaluation préétablis à mettre en corrélation avec les données à caractère personnel et informations visées au paragraphe 1er peuvent être préparés dans le but de réaliser cette corrélation en temps réel, au moment de la collecte des données par les caméras intelligentes ou les systèmes intelligents de reconnaissance automatique de plaques d'immatriculation, ou après enregistrement des données.

Lorsque la corrélation visée à l'alinéa 1er, 1° et 2°, est réalisée dans le cadre de l'exercice des missions de police administrative, elle ne peut avoir lieu :

1° qu'en temps réel ou pendant une période d'un mois à partir de l'enregistrement des données;

2° qu'après notification à l'Organe de contrôle, lorsqu'il s'agit d'une corrélation avec des listes ou extraits de banques de données visées à l'alinéa 1er, 1°.

Lorsque la corrélation visée à l'alinéa 1er, 1° et 2°, est réalisée dans le cadre de l'exercice des missions de police judiciaire, elle peut avoir lieu en temps réel ou pendant toute la durée de conservation des données. Après le premier mois de conservation, elle ne peut avoir lieu que moyennant l'autorisation du procureur du Roi et ne peut concerner que des infractions de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde ».

B.9.7. En ce qui concerne spécifiquement l'obligation de motivation de l'accès, les travaux préparatoires précisent :

« Les règles prévues au niveau du délai de conservation et au niveau de l'accès aux données enregistrées se complètent pour rencontrer cette nécessité de proportionnalité. Il sera donc important de motiver opérationnellement l'accès aux données, même pendant le premier mois. Par ailleurs, l'accès aura lieu conformément aux règles générales en matière de protection de la vie privée qui, comme mentionné plus haut, est d'application. Il sera donc nécessaire de faire état de son ' besoin d'en connaître ' (' *need to know* '). Les fonctionnaires de police n'y auront donc accès que si elles sont nécessaires à l'exercice d'une mission donnée (intérêt opérationnel). Bien entendu, l'objectif n'est pas que, dans le cadre d'une même enquête, les fonctionnaires de police accèdent, de manière systématique et autonome, aux données à caractère personnel recueillies, dans le délai d'un mois à compter de leur enregistrement. Ceci consisterait en effet à contourner les règles plus strictes qui s'appliquent aux données après le premier mois de conservation. Les fonctionnaires de police veilleront en particulier au respect de ces règles, entre autres à l'aide du login qui est conservé pour chaque accès » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-2855/001, pp. 29-30).

Par conséquent, tout accès aux données concernées doit être expressément motivé, dans le respect du principe de proportionnalité. De surcroît, après le premier mois de conservation, l'autorisation spéciale d'un magistrat est en règle générale requise, lequel contrôle le respect du principe précité.

B.9.8. Enfin, le législateur a prévu des mécanismes de contrôle afin de sécuriser les données et informations collectées.

Les accès sont journalisés et la motivation concrète des accès est enregistrée (article 25/7, § 1er, alinéa 3, de la loi du 5 août 1992, inséré par l'article 12 de la loi du 21 mars 2018). « Une trace sera donc conservée de tous les accès à ces informations et des raisons de ces accès » (*ibid.*, p. 30).

Par ailleurs, chaque service de police tient un registre numérique contenant toutes les utilisations de caméras et la police fédérale conserve un registre national de la géolocalisation de toutes les caméras fixes utilisées par les services de police. Ces registres sont, à la demande, mis à disposition de l'Organe de contrôle de l'information policière mentionné en B.21.4, des autorités de police administrative et de police judiciaire et du fonctionnaire de la protection des données, visé à l'article 144 de la loi du 7 décembre 1998 « organisant un service de police intégré, structuré à deux niveaux » (articles 25/8 et 46/14 de la loi du 5 août 1992, insérés respectivement par les articles 13 et 62 de la loi du 21 mars 2018). L'utilisation non visible de caméras, limitée à certaines circonstances, est soumise en règle à la tutelle spéciale de l'Organe de contrôle précité ou est placée sous l'autorité d'un magistrat (articles 46/5 à 46/11 de la loi du 5 août 1992, insérés par les articles 49, 50, 52, 53, 55, 56 et 58 de la loi du 21 mars 2018).

Enfin, tout traitement de données dans les banques de données techniques dans lesquelles sont enregistrées les informations provenant de la reconnaissance automatique des plaques d'immatriculation fait l'objet « d'une journalisation conservée pendant dix ans à partir du traitement réalisé dans les banques de données techniques » (article 44/11/3*novies* de la loi du 5 août 1992, inséré par l'article 34 de la loi du 21 mars 2018). Ce traitement se fait conformément à la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » (article 44/3, § 1er, de la loi du 5 août 1992, modifié par l'article 6 de la loi du 22 mai 2019 « modifiant diverses dispositions en ce qui concerne la gestion de l'information policière »). Préalablement à la création de la banque de données technique, le responsable doit soumettre pour avis au fonctionnaire chargé de la protection des données le projet afférent à cette banque de données, accompagné « d'une analyse d'impact et de risques au niveau de la protection de la vie privée et au niveau opérationnel, notamment quant aux catégories de données à caractère personnel traitées, à la proportionnalité des moyens mis en œuvre, aux objectifs opérationnels à atteindre et à la durée de conservation des données nécessaire pour atteindre ces objectifs » (article 44/11/3*octies* de la loi du 5 août 1992, inséré par l'article 33 de la loi du 21 mars 2018).

B.9.9. Au cours des discussions relatives au projet de loi en commission de la Chambre, le ministre compétent a résumé comme suit ce qui précède :

« Durant l'audition, la Commission de la protection de la vie privée a fait remarquer que la durée de conservation de 12 mois pourrait être trop longue. Le ministre souligne que cette question a d'ailleurs donné lieu à un débat animé au sein de la Commission de la protection de la vie privée. Il est vrai qu'un équilibre délicat a dû être trouvé entre les intérêts en présence. D'une part, les services de police ont un besoin opérationnel de pouvoir analyser des images plus d'un mois en arrière, en vue de faire certains constats. D'autre part, le citoyen est assuré du fait que les informations ne seront pas demandées à la légère. Ainsi, les données, issues des caméras, datant de plus d'un mois ne peuvent être consultées qu'à des fins judiciaires et en accord avec le procureur du Roi. Sur avis de la Commission de la protection de la vie privée, il a été décidé d'introduire un seuil (peine d'un an d'emprisonnement concernant les données ANPR). Tout accès nécessite de s'identifier et de compléter les raisons de la demande afin de permettre un contrôle ultérieur.

La proportionnalité est en outre garantie, du fait de l'obligation d'une analyse d'impact et de risque préalable à l'installation de chaque caméra. Dès lors, des caméras ne peuvent pas être placées n'importe où dans le but d'alimenter les banques de données.

Enfin, le ministre ajoute que la durée de conservation de 12 mois constitue une durée maximale : il n'est donc pas obligatoire de conserver les données autant de temps. Le Conseil d'État était également d'avis que ce constat permet de rencontrer le principe de proportionnalité. Il s'agit également de la même durée que celle appliquée pour les données de communication (articles 46*bis* et 88*bis* du Code d'instruction criminelle) » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-2855/003, pp. 74-75).

Il ressort en outre des travaux préparatoires que l'accès aux données et informations collectées est soumis aux règles générales en matière de protection des personnes physiques pour ce qui est du traitement des données à caractère personnel (*Doc. parl.*, Chambre, 2017-2018, DOC 54-2855/001, p. 29).

B.9.10. Il découle de ce qui précède qu'en ce qui concerne la réglementation de l'utilisation des caméras dans la loi du 5 août 1992 et la réglementation de la conservation et de la protection des données collectées par ces caméras, le législateur a ménagé, par les restrictions et garanties qu'il a prévues en matière de délai de conservation, un juste équilibre entre le droit au respect de la vie privée et les objectifs poursuivis en matière de maintien de l'ordre et de prévention des infractions.

B.10.1. La loi du 21 mars 2007, telle qu'elle a été modifiée par la loi attaquée, règle l'utilisation de caméras par d'autres personnes que les fonctionnaires de police. Elle établit une distinction entre les caméras de surveillance fixes et les caméras de surveillance mobiles et prévoit un régime distinct selon la nature du lieu où la caméra est utilisée :

(i) dans un lieu ouvert : tout lieu non délimité par une enceinte et accessible librement au public, dont les voies publiques gérées par les autorités publiques gestionnaires de voirie (article 2, 1°, de la loi du 21 mars 2007);

(ii) dans un lieu fermé accessible au public : tout bâtiment ou lieu délimité par une enceinte, destiné à l'usage du public, où des services peuvent lui être fournis (article 2, 2°);

(iii) dans un lieu fermé non accessible au public : tout bâtiment ou lieu délimité par une enceinte, destiné uniquement à l'usage des utilisateurs habituels (article 2, 3°).

B.10.2. En ce qui concerne l'utilisation de caméras de surveillance fixes et de caméras de surveillance fixes temporaires dans un lieu ouvert, l'article 5, § 4, de la loi du 21 mars 2007 disposait déjà, avant la modification opérée par la loi du 21 mars 2018, que l'enregistrement d'images est exclusivement autorisé afin de réunir des preuves de nuisances ou de faits constitutifs d'infractions ou générateurs de dommages et de rechercher et d'identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes (alinéa 3).

Ensuite, ce même paragraphe disposait déjà que si ces images ne contribuent pas à apporter la preuve d'une infraction, d'un dommage ou d'une nuisance ou ne permettent pas d'identifier un auteur, un perturbateur de l'ordre public, un témoin ou une victime, elles ne peuvent être conservées plus d'un mois (alinéa 4).

À ce dernier alinéa, qui devient l'alinéa 5, l'article 69, 14°, de la loi du 21 mars 2018 ajoute la phrase suivante :

« Ce délai est prolongé à trois mois pour les lieux présentant un risque particulier pour la sécurité, déterminés par le Roi par arrêté royal délibéré en Conseil des ministres, dont le projet est soumis pour avis à l'Autorité de protection des données ».

B.10.3. En ce qui concerne l'utilisation de caméras de surveillance fixes et de caméras de surveillance fixes temporaires dans un lieu fermé accessible au public, l'article 6, § 3, de la loi du 21 mars 2007 disposait déjà, avant la modification opérée par la loi du 21 mars 2018, que l'enregistrement d'images est exclusivement autorisé dans le but de réunir des preuves de nuisances ou de faits constitutifs d'infractions ou générateurs de dommages ou de rechercher et identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes (alinéa 2).

Ensuite, ce même paragraphe disposait déjà que si ces images ne peuvent contribuer à apporter la preuve d'une infraction, d'un dommage ou d'une nuisance ou ne peuvent permettre d'identifier un auteur des faits, un perturbateur de l'ordre public, un témoin ou une victime, elles ne peuvent être conservées plus d'un mois (alinéa 3).

À ce dernier alinéa, l'article 70, 10°, de la loi du 21 mars 2018 ajoute la phrase suivante :

« Ce délai est prolongé à trois mois pour les lieux qui, par leur nature, présentent un risque particulier pour la sécurité, déterminés par le Roi par arrêté royal délibéré en Conseil des ministres, dont le projet est soumis pour avis à l'Autorité de protection des données ».

B.10.4. En ce qui concerne l'utilisation de caméras de surveillance fixes et de caméras de surveillance fixes temporaires dans un lieu non accessible au public, l'article 7, § 3, de la loi du 21 mars 2007 dispose que l'enregistrement d'images n'est autorisé que dans le but de réunir la preuve de nuisances, de faits constitutifs d'infractions ou générateurs de dommages, de rechercher et d'identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes (alinéa 2).

Ensuite, ce même paragraphe disposait déjà, avant la modification opérée par la loi du 21 mars 2018, que si ces images ne peuvent contribuer à apporter la preuve d'une infraction, d'un dommage ou d'une nuisance ou ne peuvent permettre d'identifier un auteur des faits, un perturbateur de l'ordre public, un témoin ou une victime, elles ne peuvent être conservées plus d'un mois (alinéa 3 actuel).

À ce dernier alinéa, l'article 71, 16°, de la loi du 21 mars 2018 ajoute la phrase suivante :

« Ce délai est prolongé à trois mois pour les lieux qui, par leur nature, présentent un risque particulier pour la sécurité, déterminés par le Roi par arrêté royal délibéré en Conseil des ministres, dont le projet est soumis pour avis à l'Autorité de protection des données ».

B.10.5. En ce qui concerne l'utilisation de caméras de surveillance mobiles, utilisées par ou pour le compte des autorités communales, tant dans des lieux fermés que dans des lieux ouverts, la loi attaquée établit un régime comparable.

L'article 7/3, § 4, de la loi du 21 mars 2007, inséré par l'article 75 de la loi du 21 mars 2018, dispose :

« L'enregistrement d'images n'est autorisé que dans le but de réunir la preuve d'incivilités, de faits constitutifs d'infraction ou générateurs de dommages, de rechercher et d'identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes.

Si ces images ne peuvent contribuer à apporter la preuve d'une infraction, d'un dommage ou d'une incivilité ou ne peuvent permettre d'identifier un auteur des faits, un perturbateur de l'ordre public, un témoin ou une victime, elles ne peuvent être conservées plus d'un mois. Ce délai est prolongé à trois mois pour les lieux qui, par leur nature, présentent un risque particulier pour la sécurité, déterminés par le Roi par arrêté royal délibéré en Conseil des ministres, dont le projet est soumis pour avis à l'Autorité de protection des données ».

B.10.6. Un régime analogue s'applique dès lors pour les formes précitées d'utilisation de caméras. Le délai de conservation maximum d'un mois peut, pour certains lieux, être prolongé jusqu'à trois mois.

Il ressort des dispositions citées que ce régime est soumis à des restrictions.

En premier lieu, l'enregistrement d'images n'est autorisé que dans le but précis de recueillir des preuves d'incivilités ou de faits qui sont constitutifs d'infractions ou générateurs de dommages et de rechercher et d'identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes.

Ensuite, le délai de conservation ordinaire reste d'un mois au maximum et la possibilité de prolonger ce délai est limitée aux lieux qui, par leur nature, présentent un risque particulier pour la sécurité. Il appartient au Roi de déterminer ces lieux. Il ressort des travaux préparatoires que la mesure vise entre autres les lieux tels les gares, les aéroports et les infrastructures portuaires, « ou d'autres lieux susceptibles de constituer une cible pour les terroristes, comme les lieux où les agents de gardiennage peuvent exercer leurs compétences situationnelles, tels que les sites nucléaires, les institutions internationales, les domaines militaires, etc. » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-2855/001, pp. 18 et 77 et DOC 54-2855/003, p. 11).

Le législateur a limité de manière suffisamment claire l'habilitation au Roi précitée, et ce non seulement du point de vue du contenu; il a également entouré l'élaboration des arrêtés royaux de garanties spéciales : ils doivent être délibérés en Conseil des ministres et être soumis pour avis à l'Autorité de protection des données.

Enfin, il s'agit d'un délai qui a valeur de limite ultime pour les responsables du traitement des images lorsqu'ils appliquent le principe de proportionnalité.

B.10.7. Les travaux préparatoires résument comme suit ce qui précède et exposent également le motif de la mesure :

« Enfin, en ce qui concerne la durée de conservation des images, il est proposé de l'allonger d'un à trois mois, dans certains cas spécifiques. Après dix années d'application de cette loi, l'on constate en effet que ce délai maximum d'un mois n'est parfois pas suffisamment long et empêche, dans des cas où les images auraient pu être décisives, d'obtenir une preuve ou d'identifier des auteurs de faits ou des témoins. L'objectif n'est bien évidemment pas d'obliger les responsables du traitement à conserver les images pendant une durée de trois mois, mais d'offrir la possibilité, quand cela se justifie du point de vue de la proportionnalité, de les conserver pendant trois mois. C'est pourquoi cette possibilité n'est prévue que pour les lieux présentant un risque particulier pour la sécurité, déterminés par le Roi, par un arrêté royal délibéré en Conseil des ministres et dont le projet sera soumis pour avis à l'Autorité de protection des données. En dehors de ces cas qui seront déterminés par le Roi, le délai de conservation reste inchangé » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-2855/001, p. 75).

B.10.8. Il ressort de ce qui précède qu'en ce qui concerne les règles de l'utilisation des caméras prévues dans la loi du 21 mars 2007, les restrictions et les garanties contenues dans ce régime en matière de délai de conservation ont permis au législateur de ménager un juste équilibre entre le droit au respect de la vie privée et les buts poursuivis en matière de maintien de l'ordre et de prévention des infractions.

B.11. Le premier moyen n'est pas fondé.

B.12. Dans la première branche du second moyen, la partie requérante invoque une atteinte disproportionnée au droit au respect de la vie privée en ce que les mesures contenues dans la loi attaquée ne seraient pas limitées aux cas de criminalité grave ou aux raisons graves d'ordre public ou de sécurité nationale. Elle vise plus particulièrement (i) l'autorisation d'utiliser des caméras de police non visibles, (ii) l'accès des services de police et des services de renseignement et de sécurité aux données conservées sur la base de la loi attaquée, (iii) l'autorisation donnée aux services de police et aux services de renseignement et de sécurité de mettre ces données en corrélation avec d'autres données décrites dans la loi et (iv) l'autorisation donnée aux services de renseignement et de sécurité de procéder, via cet accès et cette corrélation, à une observation en utilisant des moyens techniques.

Dans la deuxième branche du second moyen, la partie requérante invoque une atteinte disproportionnée au droit au respect de la vie privée en ce que les autorisations et habilitations précitées n'auraient pas été soumises au contrôle préalable d'une juridiction ou d'une autorité administrative indépendante.

B.13.1. L'utilisation de caméras de police non visibles en raison de circonstances particulières est autorisée par l'article 46/4 de la loi du 5 août 1992, inséré par l'article 48 de la loi attaquée :

« Par dérogation à l'article 25/3, les caméras fixes temporaires et mobiles, le cas échéant intelligentes, peuvent être utilisées de manière non visible, dans les lieux ouverts et les lieux fermés accessibles au public, moyennant une autorisation préalable, lorsque les circonstances ne permettent pas aux fonctionnaires de police d'être identifiables ou sont de nature à rendre inopérante l'utilisation de caméras de manière visible, et qu'il s'agit d'une des situations suivantes :

1° les situations visées à l'article 22, alinéa 2;

2° le recueil de l'information de police administrative visée à l'article 44/5, § 1er, alinéa 1er, 2° et 3°, pour autant qu'il s'agisse de :

a) personnes radicalisées au sens de l'article 3, 15°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

b) personnes à l'égard desquelles il existe des indices fondés et très sérieux qu'elles souhaitent se rendre sur un territoire où des groupes terroristes, tels que définis à l'article 139 du Code pénal, sont actifs dans des conditions telles qu'elles peuvent présenter à leur retour en Belgique une menace sérieuse d'infraction terroriste telle que définie à l'article 137 du Code pénal ou que ces personnes ont l'intention de commettre hors du territoire national des infractions terroristes telles que définies à l'article 137 du Code pénal;

3° l'utilisation sur un moyen de transport de police, non identifiable comme tel, pour la lecture automatique de plaques d'immatriculation, en vue de détecter des véhicules signalés ».

Les situations visées par l'article 22, alinéa 2, concernent les mesures tendant à disperser divers attroupements : (1) les attroupements armés, (2) les attroupements qui s'accompagnent de crimes et de délits contre les personnes ou les biens ou d'infractions à la loi du 29 juillet 1934 « interdisant les milices privées », (3) les attroupements dont il apparaît qu'ils sont constitués ou se constituent en vue de porter la dévastation, le massacre ou le pillage ou d'attenter à l'intégrité physique ou à la vie des personnes et (4) les attroupements faisant obstacle à l'exécution de la loi, d'une ordonnance de police, d'une mesure de police, d'une décision de justice ou d'une contrainte.

Les informations de police administrative visées à l'article 44/5, § 1er, alinéa 1er, 2° et 3°, portent sur (1) les données relatives aux personnes impliquées dans les domaines relevant des problèmes portant atteinte à l'ordre public et nécessitant des mesures appropriées de police administrative parce qu'ils sont de même nature et répétitifs, qu'ils sont commis par les mêmes personnes ou qu'ils visent les mêmes catégories de victimes ou de lieux et (2) les données relatives aux membres d'un groupement national ou international susceptible de porter atteinte à l'ordre public tel qu'il est visé par l'article 14. La collecte d'informations concernant ces données est en outre limitée aux personnes mentionnées expressément dans l'article 46/4, 2°, qui, de manière univoque, peuvent être liées au terrorisme.

La disposition attaquée décrit donc de manière précise les circonstances particulières dans lesquelles l'utilisation de caméras de police non visibles est autorisée.

Par son arrêt n° 108/2016 du 14 juillet 2016, la Cour a du reste constaté que les catégories définies dans l'article 44/5, § 1er, alinéa 1er, 2° et 3°, de la loi du 5 août 1992 sont suffisamment précises (B.20-B.32).

B.13.2. L'accès des services de police aux données conservées sur la base de la loi attaquée est également réglé de manière précise dans les dispositions mentionnées en B.9.6 ci-dessus.

Les services de renseignement et de sécurité ont accès aux données conservées sur la base de la loi attaquée, pour autant que cet accès soit motivé sur le plan opérationnel, qu'il soit nécessaire pour l'exercice d'une mission précise et qu'il soit décidé par un officier de renseignement. Après le premier mois de conservation, l'accord du dirigeant du service ou de son délégué est requis (article 16/4, § 2, alinéas 1er et 2, de la loi du 30 novembre 1998, inséré par l'article 84 de la loi du 21 mars 2018). L'accès doit par ailleurs avoir lieu « de manière ponctuelle », ce qui n'est pas le cas « si la région et la durée ne sont pas proportionnellement limitées. Est par exemple ciblée la demande qui porte sur un box de garage déterminé pour une période de deux mois, afin d'y suivre les passages de membres d'un réseau terroriste. Ou encore, la consultation de la banque de données pour savoir si le numéro de plaque X est enregistré à l'endroit Y au moment Z » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-2855/001, p. 104).

La décision du dirigeant du service ou de son délégué et la motivation de celle-ci sont transmises sans délai au Comité permanent de contrôle des services de renseignement et de sécurité (Comité permanent R). La décision peut porter sur un ensemble de données relatives à une enquête de renseignements spécifiques. Dans ce cas, une liste des accès ponctuels est communiquée une fois par mois au Comité permanent R. Ce Comité interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans des conditions qui ne respectent pas les conditions légales (article 16/4, § 2, alinéa 3, de la loi du 30 novembre 1998, inséré par l'article 84 de la loi du 21 mars 2018).

Par ailleurs, le Comité permanent R exerce son pouvoir de contrôle général :

« Le Comité permanent R assure d'ailleurs un contrôle effectif. Ce sera spécifiquement rendu possible par le fait que chaque décision du dirigeant du service lui est notifiée. Cet organe de contrôle possède de larges compétences si une irrégularité est constatée. Il peut notamment ordonner la cessation de la méthode ainsi que l'interdiction de l'exploitation des données collectées et en même leur destruction. Une destruction s'étend également à toutes les mentions de ces données, par exemple dans des notes internes, de sorte que ces données ne peuvent plus être utilisées comme base de la mise en œuvre d'une nouvelle méthode de collecte. Pour ces raisons, les auteurs du projet de loi ne sont pas d'accord avec la remarque du Comité R selon laquelle la destruction n'aurait qu'une valeur symbolique.

Il existe aussi des règles internes qui contrent les abus. Ainsi, chaque collaborateur des services de renseignement et de sécurité fait l'objet d'une enquête de sécurité tous les 5 ans. En outre, tous les traitements sur des banques de données des services-mêmes ou d'autres services sont loggés; ceux-ci font l'objet d'un contrôle exercé par le bureau de sécurité de la VSSE et du SGRS et par le Comité permanent R. En plus, un collaborateur n'a accès qu'aux données qui sont en lien avec sa propre fonction, donc sur une base du principe du ' *need to know* ' (besoin d'en connaître), et seulement aux données qui peuvent être en relation avec des menaces bien déterminées pour lesquelles les services de renseignement et de sécurité sont compétents. Par ailleurs, les données que les services de renseignement obtiennent des caméras sont enregistrées dans un système sécurisé, voire classifié dès qu'elles sont traitées. Ceci renforce les prescriptions de sécurité avec lesquelles les données doivent être traitées. Enfin, un citoyen peut introduire une plainte à tout moment auprès de la Commission de la protection de la vie privée ou auprès du Comité permanent R, après quoi ces institutions peuvent procéder à une enquête. Le Comité permanent R peut aussi d'office et d'initiative procéder à une enquête. La VSSE et le SGRS sont tenus de prêter leur entière collaboration » (*ibid.*, pp. 106-107).

L'accès aux informations et aux données à caractère personnel est protégé, tous les accès sont journalisés et les raisons concrètes des accès sont enregistrées (article 16/4, § 2, alinéa 4, de la loi du 30 novembre 1998, inséré par l'article 84 de la loi du 21 mars 2018).

B.13.3. L'habilitation conférée aux services de police afin qu'ils puissent mettre les données conservées en corrélation avec d'autres données définies dans la loi est réglée en détail par l'article 44/11/3*decies*, § 4, mentionné en B.9.6, de la loi du 5 août 1992, inséré par l'article 35 de la loi du 21 mars 2018.

De manière analogue, le législateur a habilité les services de renseignement et de sécurité à mettre les données des banques de données techniques en corrélation avec d'autres banques de données qu'ils gèrent eux-mêmes ou qui sont directement disponibles ou accessibles dans le cadre de leurs missions ou des listes de personnes élaborées par les services de renseignement et de sécurité dans le cadre de leurs missions ou des critères d'évaluation préétablis (article 16/4, § 3, de la loi du 30 novembre 1998, inséré par l'article 84 de la loi du 21 mars 2018).

B.13.4. Enfin, la loi attaquée habilite les services de renseignement et de sécurité à procéder, à l'aide de moyens techniques, à une observation via l'accès aux données concernées et, le cas échéant, via la corrélation de ces données avec les autres données mentionnées (articles 18/4 et 18/11 de la loi du 30 novembre 1998, insérés par les articles 85 et 86 de la loi du 21 mars 2018).

B.14.1. Les autorisations et habilitations attaquées sont donc clairement délimitées dans les dispositions précitées. Elles tendent à contribuer à garantir la sécurité publique, à protéger l'ordre public, à prévenir les infractions et à protéger les droits et libertés d'autrui. Les mesures répondent donc à un besoin social impérieux dans une société démocratique.

B.14.2. Les autorisations et habilitations attaquées sont en outre soumises à des restrictions.

B.14.3. L'utilisation de caméras de police non visibles ne peut être autorisée qu'à des fins spécifiques et seulement si les circonstances ne permettent pas aux agents de police de s'identifier ou sont de nature à rendre inopérante l'utilisation de caméras visibles. L'utilisation est autorisée au cas par cas, toujours pour une durée limitée, par le commissaire général de la police fédérale ou par le chef de corps de la police locale, dans certains cas après l'avis préalable contraignant du procureur du Roi et de la Sûreté de l'État (article 46/5 de la loi du 5 août 1992, inséré par l'article 49 de la loi du 21 mars 2018). L'utilisation non visible est en règle générale soumise au contrôle spécial de l'Organe de contrôle ou se trouve placée sous l'autorité d'un magistrat.

B.14.4. L'accès des services de police aux données conservées sur la base de la loi attaquée est limité dans le temps et est soumis, dans certains cas, à l'autorisation d'un magistrat, à un enregistrement strict et à une analyse de l'impact et des risques en matière de protection de la vie privée. Des restrictions analogues s'appliquent à l'accès des services de renseignement et de sécurité. En tout état de cause, l'exigence de proportionnalité doit chaque fois être respectée.

B.14.5. L'habilitation conférée aux services de police pour mettre les données conservées en corrélation avec d'autres données définies dans la loi ne vaut que pour les données provenant des banques de données techniques, qui contiennent des informations provenant de la reconnaissance automatique des plaques d'immatriculation et qui peuvent être liées à d'autres données précises, pour une durée limitée et après les accords et contrôles prescrits. Des restrictions analogues s'appliquent à l'accès des services de renseignement et de sécurité. Dans ce cas aussi, l'exigence de proportionnalité doit chaque fois être respectée.

B.14.6. L'habilitation conférée aux services de renseignement et de sécurité pour procéder à une observation en utilisant des moyens techniques via l'accès aux données concernées et, le cas échéant, via leur corrélation avec les autres données mentionnées est uniquement autorisée aux mêmes conditions que celles applicables aux autres méthodes de collecte de données visées dans la loi du 30 novembre 1998.

Le Comité permanent R statue sur la légalité des décisions relatives à ces méthodes, ainsi que sur le respect des principes de proportionnalité et de subsidiarité (article 43/2, alinéa 2, de la loi du 30 novembre 1998).

B.14.7. Il découle de ces restrictions qui tendent à contrôler l'accès aux données conservées et leur utilisation que le législateur a ménagé un juste équilibre entre le droit au respect de la vie privée et les objectifs poursuivis en matière de maintien de l'ordre et de prévention des infractions.

Le simple constat que les autorisations et les habilitations attaquées ne sont pas limitées aux cas de criminalité grave ou aux raisons graves d'ordre public ou de sécurité nationale et qu'elles ne sont pas soumises à un contrôle préalable d'une juridiction ou d'une autorité administrative indépendante ne saurait y porter atteinte.

B.15. Le second moyen, en ses première et deuxième branches, n'est pas fondé.

Quant au principe de légalité

B.16. Dans la troisième branche du second moyen, la partie requérante invoque la violation du principe de légalité, contenu dans l'article 22 de la Constitution, par l'habilitation étendue conférée aux ministres de l'Intérieur et de la Justice pour prendre des mesures en ce qui concerne l'interconnexion et la corrélation avec les banques de données techniques (article 28 de la loi du 21 mars 2018) et par l'habilitation étendue conférée au Roi pour régler l'accès direct des services de renseignement et de sécurité aux données recueillies par les services de police à l'aide de caméras (article 84 de la même loi).

B.17. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout justiciable qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

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

B.18.1. L'article 44/4, § 4, de la loi du 5 août 1992, inséré par l'article 28 de la loi du 21 mars 2018, dispose :

« Les ministres de l'Intérieur et de la Justice déterminent par directives communes 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.

Ces directives communes tiennent 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.18.2. L'article 44/4 de la loi du 5 août 1992 a, dans l'intervalle, été remplacé, avec effet au 29 juin 2019, par l'article 7 de la loi du 22 mai 2019 « modifiant diverses dispositions en ce qui concerne la gestion de l'information policière ».

B.18.3. Étant donné qu'il n'est pas établi que l'article 44/4 de la loi du 5 août 1992, tel qu'il a été modifié par l'article 28 de la loi du 21 mars 2018, ait été appliqué avant le 29 juin 2019, le second moyen, en sa troisième branche, est sans objet en ce qu'il porte sur cette disposition.

B.19.1. L'article 16/4, § 1er, alinéa 1er, de la loi du 30 novembre 1998, tel qu'il a été inséré par l'article 84 de la loi du 21 mars 2018, dispose :

« Selon les modalités déterminées par le Roi, après avis de l'autorité compétente de contrôle des traitements de données à caractère personnel, un accès direct est autorisé pour les services de renseignement et de sécurité aux informations et données à caractère personnel qui sont collectées au moyen de caméras dont l'utilisation par les services de police est autorisée conformément au chapitre IV, section 1re, et au chapitre IV/1, section 2, de la loi sur la fonction de police et qui sont notamment traitées dans les banques de données visées à l'article 44/2 de ladite loi ».

B.19.2. Les travaux préparatoires précisent que le Roi détermine les modalités de l'accès sur la base de cette disposition :

« Il faudra notamment déterminer des règles générales quant à l'enregistrement des accès effectués par les membres des services de renseignement et de sécurité » (*Doc. parl.*, Chambre, 2017-2018, DOC 54-2855/001, p. 102).

B.19.3. Étant donné que les conditions d'accès ont été réglées de manière précise par le législateur lui-même, ainsi qu'il ressort du B.13.2, le second moyen, en sa troisième branche, n'est pas fondé.

Quant au principe d'égalité

B.20. Dans la quatrième branche du second moyen, la partie requérante invoque la violation du principe d'égalité et de non-discrimination en ce que la mise en corrélation de données, autorisée par l'article 44/11/3*decies*, § 4, de la loi du 5 août 1992, inséré par l'article 35 de la loi du 21 mars 2018, n'est pas soumise aux mêmes garanties que celles prévues par l'article 47*sexies* du Code d'instruction criminelle. Il en résulte que le principe de légalité en matière pénale serait également violé. Étant donné que la loi du 21 mars 2018 ne prévoit pas davantage un contrôle juridictionnel effectif de la corrélation de données et de l'accès à celles-ci, elle violerait également le droit à un procès équitable et le droit de défense.

B.21.1. Moyennant le respect de conditions strictes, mentionnées en B.9.6, l'article 44/11/3*decies*, § 4, de la loi du 5 août 1992 autorise les services de police à mettre les informations provenant de la reconnaissance automatique des plaques d'immatriculation, enregistrées dans les banques de données techniques, en corrélation avec (1) les listes auxquelles les services de police ont légalement accès ou les extraits de banques de données policières nationales ou internationales auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique; et (2) les critères d'évaluation préétablis.

Cette corrélation a pour but « de générer des alarmes (hits) et peut avoir lieu en temps réel ou *a posteriori*, après enregistrement des données par les caméras ANPR ou le système de reconnaissance ANPR » (*ibid.*, p. 43).

B.21.2. L'article 47*sexies*, § 1er, du Code d'instruction criminelle prévoit l'observation en tant que méthode particulière de recherche. L'observation au sens du Code d'instruction criminelle est l'observation systématique, par un fonctionnaire de police, d'une ou de plusieurs personnes, de leur présence ou de leur comportement ou de choses, de lieux ou d'événements déterminés. Une observation systématique est une observation de plus de cinq jours consécutifs ou de plus de cinq jours non consécutifs répartis sur une période d'un mois, une observation dans le cadre de laquelle des moyens techniques sont utilisés, une observation revêtant un caractère international ou une observation exécutée par des unités spécialisées de la police fédérale.

Le procureur du Roi peut, dans le cadre de l'information, autoriser une observation si les nécessités de l'enquête l'exigent et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité (article 47*sexies*, § 2, alinéa 1er). L'autorisation de procéder à l'observation est écrite et motivée (article 47*sexies*, § 3).

B.21.3. À la différence de l'observation, la mise en corrélation de certaines données n'est pas une méthode particulière de recherche. En règle générale, l'observation tend à recueillir de nouvelles données, alors que la mise en corrélation porte sur des données existantes, qui sont recueillies d'une manière qui, ainsi qu'il ressort de l'examen du premier moyen, est entourée de garanties suffisantes.

Il est dès lors raisonnablement justifié que les deux techniques ne soient pas soumises aux mêmes garanties.

Comme il est dit en B.9.7, tout accès aux données concernées doit en outre être expressément motivé, dans le respect du principe de proportionnalité.

B.21.4. En vertu de l'article 71 de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », il est créé auprès de la Chambre des représentants une autorité de contrôle indépendante de l'information policière, dénommée Organe de contrôle de l'information policière, qui est chargée de contrôler le traitement des informations et des données à caractère personnel visées à l'article 44/1 de la loi du 5 août 1992, en ce compris celles incluses dans les banques de données visées à l'article 44/2.

Il ressort de cette disposition que le pouvoir de contrôle qui a été conféré à l'Organe de contrôle de l'information policière est de nature générale, en ce sens que toutes les informations et données à caractère personnel qui sont traitées par les services de police peuvent être contrôlées par l'Organe de contrôle (article 44/1) et que toutes les banques de données policières relèvent du pouvoir de contrôle de cet organe (article 44/2).

L'Organe de contrôle veille, au moyen d'enquêtes de fonctionnement, à ce que le contenu de la Banque de données nationale générale, des banques de données de base, des banques de données particulières et des banques de données techniques, ainsi que la procédure de traitement des données et informations qui y sont conservées, soient conformes à ce qui est prescrit par les articles 44/1 à 44/11/13 de la loi du 5 août 1992 et à leurs mesures d'exécution (article 239 de la loi précitée du 30 juillet 2018). L'Organe de contrôle agit d'initiative ou à la demande de certaines autorités (article 237 de la même loi).

B.21.5. Étant donné que la mise en corrélation de données n'est pas une méthode particulière de recherche, cette technique ne relève pas du contrôle de la chambre des mises en accusation lors de la clôture d'une information.

Comme toute intervention d'une autorité publique, la mise en corrélation de certaines données par les services de police peut être soumise à un contrôle juridictionnel. Dans le cadre de son contrôle de légalité de la mesure, le juge compétent doit y associer le respect du principe de proportionnalité.

B.21.6. Enfin, la partie requérante n'expose pas en quoi la disposition attaquée violerait le principe de légalité en matière pénale.

B.22. Le second moyen, en sa quatrième branche, n'est pas fondé.

Par ces motifs,

la Cour

rejette le recours.

Ainsi rendu en langue néerlandaise, en langue française et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 20 février 2020.

Le greffier, Le président,

F. Meersschaut A. Alen