



Cour constitutionnelle

**Arrêt n° 30/2026
du 12 mars 2026
Numéro du rôle : 8349**

En cause : le recours en annulation de la loi du 29 mars 2024 « portant création de la banque de données commune ‘ Terrorisme, Extrémisme, processus de Radicalisation ’ (‘ T.E.R. ’) et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police », introduit par l’ASBL « Ligue des droits humains » et l’ASBL « Défense des Enfants - International - Belgique ».

La Cour constitutionnelle,

composée des présidents Pierre Nihoul et Luc Lavrysen, et des juges Thierry Giet, Joséphine Moerman, Michel Pâques, Yasmine Kherbache, Sabine de Bethune, Emmanuelle Bribosia, Willem Verrijdt et Magali Plovie, assistée du greffier Nicolas Dupont, présidée par le président Pierre Nihoul,

après en avoir délibéré, rend l’arrêt suivant :

I. Objet du recours et procédure

Par requête adressée à la Cour par lettre recommandée à la poste le 16 octobre 2024 et parvenue au greffe le 18 octobre 2024, un recours en annulation de la loi du 29 mars 2024 « portant création de la banque de données commune ‘ Terrorisme, Extrémisme, processus de Radicalisation ’ (‘ T.E.R. ’) et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police » (publiée au *Moniteur belge* du 16 avril 2024) a été introduit par l’ASBL « Ligue des droits humains » et l’ASBL « Défense des Enfants - International - Belgique », assistées et représentées par Me Catherine Forget, avocate au barreau de Bruxelles.

Le Conseil des ministres, assisté et représenté par Me Nicolas Bonbled et Me Lise-Marie Hennau, avocats au barreau de Bruxelles, a introduit un mémoire, les parties requérantes ont introduit un mémoire en réponse et le Conseil des ministres a également introduit un mémoire en réplique.

Par ordonnance du 17 décembre 2025, la Cour, après avoir entendu les juges-rapporteurs Magali Plovie et Willem Verrijdt, 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 à l'expiration de ce délai et l'affaire serait mise en délibéré.

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

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

II. *En droit*

- A -

Quant au premier moyen

A.1. Le premier moyen est pris de la violation, par la loi du 29 mars 2024 « portant création de la banque de données commune ' Terrorisme, Extrémisme, processus de Radicalisation ' (' T.E.R. ') et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police » (ci-après : la loi attaquée), des articles 10, 11 et 22 de la Constitution, lus en combinaison ou non avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 8, 10, 13 à 15 et 54 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil » (ci-après : la directive « police ») et avec les articles 7, 8, 47 et 52 de la Charte des droits fondamentaux de l'Union européenne (ci-après : la Charte). Ce moyen est subdivisé en douze griefs.

A.2. Les six premiers griefs sont pris de la violation du principe de légalité.

A.3.1. Dans le premier grief, les parties requérantes soutiennent que la notion de « propagandiste de haine » visée à l'article 2, 11°, de la loi attaquée n'est pas définie de manière suffisamment précise. Premièrement, les termes définissant l'objectif du propagandiste de haine, à savoir « porter atteinte aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit », sont tellement vagues et larges que cette notion est susceptible de s'appliquer à des discours protégés par la liberté d'expression. Certaines critiques du fonctionnement du pouvoir judiciaire ou du système électoral pourraient ainsi être considérées comme poursuivant un tel objectif. Deuxièmement, l'exigence selon laquelle le propagandiste de haine doit justifier « l'usage de la violence ou de la contrainte comme moyen d'action » introduit une confusion entre la violence et la contrainte non violente, de sorte que pourraient être visées des personnes qui plaident de manière non violente en faveur de changements sociétaux en appelant par exemple à la désobéissance civile. Les parties requérantes se réfèrent sur ce point au rapport de la rapporteuse spéciale des Nations Unies du 1er mars 2019 sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, intitulé « Effet des mesures de lutte contre le terrorisme et l'extrémisme

violent sur l'espace civique et sur les droits des acteurs de la société civile et des défenseurs des droits de l'homme » (A/HRC/40/52). Elles se réfèrent également à l'arrêt de la Cour européenne des droits de l'homme du 15 octobre 2015 en cause de *Perinçek c. Suisse* (grande chambre, ECLI:CE:ECHR:2015:1015JUD002751008), selon lequel un discours qui justifie l'usage de la contrainte pour parvenir à certains objectifs est protégé par la liberté d'expression tant qu'il ne constitue pas un appel direct ou indirect à la violence ou justifiant la violence, la haine ou l'intolérance. Troisièmement, la notion de « propagandiste de haine » peut engendrer une confusion avec les infractions pénales d'« incitation à la haine » et de « diffusion d'idée sur la supériorité ou la haine raciale » visées aux articles 20 et 21 de la loi du 30 juillet 1981 « tendant à réprimer certains actes inspirés par le racisme ou la xénophobie ». Quatrièmement, la notion d'« influence radicalisante » manque de précision. Lue en combinaison avec la notion de « processus de radicalisation » visée à l'article 3, 15°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, elle introduit un élément intentionnel, qui demeure toutefois encore loin d'une volonté d'inciter à commettre un acte terroriste. La référence à « toute action » se prête par ailleurs à des applications larges et difficilement prévisibles. Les parties requérantes se demandent, par exemple, si la publication d'une information d'intérêt public qui susciterait la colère d'une partie de la population pourrait être qualifiée d'« influence radicalisante ».

Les parties requérantes soutiennent qu'elles ne découpent pas artificiellement la notion de « propagandiste de haine » : elles constatent que les termes utilisés sont sujets à confusion et qu'ils manquent de clarté. Elles ajoutent qu'une information, telle une information critique relative au droit de propriété, peut avoir pour effet de porter atteinte aux droits humains.

Les parties requérantes soutiennent que des critiques analogues peuvent être formulées en ce qui concerne la notion d'« extrémiste potentiellement violent » visée à l'article 2, 9°, de la loi attaquée.

A.3.2. Le Conseil des ministres soutient que le premier moyen, en son premier grief, n'est pas fondé. Premièrement, les critères énumérés à l'article 2, 11°, de la loi attaquée doivent être appliqués de manière cumulative, de sorte qu'il n'est pas pertinent d'analyser séparément la compatibilité de chaque critère avec le principe de légalité. Le degré de précision requis de la loi attaquée doit par ailleurs tenir compte du domaine lié à la sécurité nationale dans lequel elle s'inscrit. Deuxièmement, l'exigence selon laquelle le propagandiste de haine doit justifier « l'usage de la violence ou de la contrainte comme moyen d'action » (article 2, 11°, b)) n'entraîne pas de confusion entre la violence et la contrainte non violente, dès lors que la qualification de propagandiste de haine requiert en outre la volonté, d'une part, de porter atteinte aux principes de la démocratie ou des droits de l'homme (article 2, 11°, a)) et, d'autre part, d'exercer une influence radicalisante (article 2, 11°, c)). Cette dernière disposition inclut un élément moral, à savoir la volonté d'exercer une influence ayant pour but d'initier, de soutenir ou de contribuer à un processus de radicalisation. Les travaux préparatoires confirment que la notion de « contrainte » désigne uniquement la contrainte violente. Troisièmement, la critique selon laquelle la notion de « propagandiste de haine » pourrait se confondre avec les notions d'« incitation à la haine » et de « diffusion d'idée sur la supériorité ou la haine raciale » est irrecevable, à défaut d'être démontrée par les parties requérantes. Quatrièmement, la référence faite à l'article 2, 11°, c), à « toute action » ne se prête pas à des applications larges ou difficilement prévisibles si l'on combine ces termes avec les exigences visées aux points a), b) et c) de l'article 2, 11°. La publication d'une information d'intérêt public suscitant la colère d'une partie de la population ne pourrait pas être qualifiée d'« influence radicalisante », puisque, cette publication, dès lors qu'elle est d'intérêt public, n'aurait pas pour but de porter atteinte aux principes de la démocratie ou des droits de l'homme. De même, une information critique du droit de propriété qui donnerait lieu à des manifestations violentes ne pourrait pas être assimilée à une influence radicalisante, dès lors que la simple critique du droit de propriété ne peut pas être considérée comme un acte justifiant l'usage de la violence ou de la contrainte comme moyen d'action.

A.4.1. Dans le deuxième grief, les parties requérantes font valoir que l'article 9 de la loi attaquée délègue au Roi la détermination d'éléments essentiels du traitement, en ce qu'il habilite Celui-ci à réglementer les finalités de l'interconnexion entre les banques de données.

A.4.2. Le Conseil des ministres soutient que le premier moyen, en son deuxième grief, n'est pas fondé. Il constate que la critique formulée par les parties requérantes est dirigée contre l'article 9 de l'avant-projet de loi qui est à l'origine de la loi attaquée. Cette disposition a toutefois été adaptée à la suite de l'avis de la section de législation du Conseil d'État sur l'avant-projet de loi, de l'avis de l'Autorité de protection des données (ci-après :

l'APD) n° 97/2023 du 16 juin 2023 et de l'avis du Comité permanent de contrôle des services de renseignement et de sécurité (ci-après : le Comité permanent R) n° 004/CPR/2023 du 13 juillet 2023. Selon le Conseil des ministres, les finalités de l'interconnexion figurent bien dans l'article 9, § 1er, alinéa 2, de la loi attaquée.

A.5.1. Dans le troisième grief, les parties requérantes soutiennent que les habilitations du Roi contenues dans l'article 16 de la loi attaquée sont formulées en des termes trop larges. Selon les parties requérantes, le fait que le Conseil des ministres soutienne que d'autres services pourraient obtenir par la suite un droit d'accès à la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (ci-après : T.E.R.) renforce ce grief.

A.5.2. Selon le Conseil des ministres, le premier moyen, en son troisième grief, n'est pas fondé. Il observe que, dans son avis du 20 juin 2023, l'Organe de contrôle de l'information policière a formulé une critique similaire à celle des parties requérantes et que le législateur y a répondu dans les travaux préparatoires. Ces derniers mentionnent les services partenaires que le législateur a pu identifier anticipativement. Il se peut toutefois que d'autres services doivent obtenir un droit d'accès à l'avenir. Le Conseil des ministres estime que l'habilitation visée à l'article 16 est définie de façon suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur. Selon le Conseil des ministres, la loi attaquée énumère en des termes clairs et précis les catégories de données à caractère personnel traitées dans la banque de données commune T.E.R. Les services partenaires disposent d'un droit de lecture et d'écriture ou d'interrogation dans cette banque de données, de sorte qu'ils peuvent avoir accès aux données relevant des catégories énumérées à l'article 6, § 2, de la loi attaquée. En ce qui concerne les catégories de personnes concernées, l'article 2, 4°, a) et b), de la loi attaquée définit avec précision le terme « entité » visé à l'article 6, § 2, de la même loi. L'article 16 de la loi attaquée précise la finalité du traitement effectué par les services partenaires. En ce qui concerne les catégories de personnes ayant accès aux données traitées, l'article 2, 3°, de la loi attaquée énumère de façon précise l'ensemble des services dits « partenaires ». Le délai maximal de conservation des données n'est pas une question pertinente pour ce qui est du droit de lecture et d'écriture ou d'interrogation des services partenaires. Enfin, la section de législation du Conseil d'État n'a pas émis de critique à propos de l'article 17 de l'avant-projet de loi qui est à l'origine de l'article 16 de la loi attaquée.

A.6.1. Dans le quatrième grief, les parties requérantes soutiennent que l'article 33, § 2, 7° et 8°, de la loi attaquée, qui prévoit la possibilité pour l'Office national de l'emploi (ONEm), l'Office wallon de la formation professionnelle et de l'emploi (FORem), l'Office régional bruxellois de l'emploi (Actiris), Bruxelles formation, l'Office flamand de l'emploi et de la formation professionnelle (« Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding » ou VDAB) ou le Bureau de l'emploi de la Communauté germanophone de Belgique (« Arbeitsamt der Deutschsprachigen Gemeinschaft Belgiens » ou ADG) et l'Office des étrangers de prendre des « mesures spécifiques » contre la personne inscrite dans la banque de données commune T.E.R., n'est pas suffisamment précis, à défaut d'identifier les mesures concernées et les dispositions légales correspondantes. Les parties requérantes estiment que la loi attaquée génère une confusion des rôles qui est incompatible avec le principe de légalité et avec le principe de finalité. Il n'est pas envisageable que les participants à la « Task Force locale » se concertent à propos de mesures à prendre par l'ONEm et par l'Office des étrangers alors que ces services poursuivent des finalités différentes.

A.6.2. Selon le Conseil des ministres, le quatrième grief du premier moyen repose sur une lecture erronée de l'article 33, § 2, 7° et 8°, de la loi attaquée. Cette disposition concerne uniquement la concertation de la « Task Force » locale sur l'opportunité de prendre ou non une ou plusieurs mesures visées au paragraphe 2. Le résultat de cette concertation est ensuite transmis aux autorités compétentes, qui, elles, prendront les éventuelles mesures à l'égard d'une entité visée dans la banque de données commune T.E.R. La « Task Force » locale n'est donc pas compétente pour prendre elle-même les mesures énumérées au paragraphe 2. Le Conseil des ministres relève que ni la section de législation du Conseil d'État, ni le Comité permanent R, ni l'APD n'ont émis de critiques à propos de l'article 33, § 2, 7° et 8°. C'est précisément parce que les mesures examinées poursuivent des finalités différentes que la « Task Force » locale doit les appréhender dans leur ensemble, afin d'évaluer si elles permettent de réduire au maximum le danger représenté par la personne concernée. Si la « Task Force » locale constate, dans le cadre du suivi d'une personne enregistrée dans la banque de données commune T.E.R., qu'une mesure de l'Office des étrangers va à l'encontre d'une mesure de l'ONEm pour la réintégration de cette personne dans la vie en société, elle partagera avec l'Office des étrangers le résultat de sa concertation et lui suggérera d'adapter sa mesure. L'Office des étrangers restera toutefois seul compétent pour apprécier la mesure à adopter au regard des finalités qu'il poursuit.

A.7.1. Dans le cinquième grief, les parties requérantes reprochent à l'article 32, § 1er, alinéa 4, de la loi attaquée de ne pas permettre la détermination des services susceptibles d'être invités par le président de la « Task

force » locale, de sorte qu'une personne concernée ne peut pas s'assurer que le traitement de ses données par les services invités est nécessaire et proportionné à la finalité poursuivie. D'après elles, le fait que le Conseil des ministres soutienne que d'autres services pourraient obtenir par la suite un droit d'accès à la banque de données commune T.E.R. renforce ce grief.

A.7.2. Le Conseil des ministres soutient que le premier moyen, en son cinquième grief, n'est pas fondé. Selon lui, il ressort des travaux préparatoires que le législateur a tenu compte des remarques formulées par la section de législation du Conseil d'État, par l'APD et par le Comité permanent R. Il n'est par ailleurs pas nécessaire que les services susceptibles d'être invités soient déterminables, puisque les services invités ne se voient pas communiquer des données ou informations détenues par les autres membres de la « Task Force » locale.

A.8.1. Dans le sixième grief, les parties requérantes font grief aux articles 23 et 26 de la loi attaquée de ne pas contenir une liste exhaustive des destinataires potentiels de la « carte d'information ». Elles se réfèrent aux arrêts de la Cour n^{os} 29/2018 (ECLI:BE:GHCC:2018:ARR.029) et 44/2015 (ECLI:BE:GHCC:2015:ARR.044), à l'arrêt de la Cour de justice du 12 janvier 2023 en cause de *RW c. Österreichische Post AG* (C-154/21, ECLI:EU:C:2023:3) et à l'avis de l'APD n^o 97/2023, précité.

A.8.2. Le Conseil des ministres soutient que le premier moyen, en son sixième grief, n'est pas fondé. Premièrement, le législateur a identifié les services qui, à sa connaissance, sont susceptibles d'avoir accès aux données de la base de données commune T.E.R. Il lui aurait toutefois été impossible de déterminer à l'avance l'ensemble de ces services. Deuxièmement, la carte d'information ne contient qu'un nombre limité d'informations, sans donner accès à la banque de données. Troisièmement, il est nécessaire que la carte d'information permette de communiquer certaines informations à des services autres que ceux qui sont visés par la loi attaquée. Il serait inconcevable que la transmission d'informations cruciales dans le cadre de la lutte contre le terrorisme et l'extrémisme soit entravée en cas d'urgence parce qu'un dispositif législatif trop fermé doit être révisé. Quatrièmement, il ressort de l'article 156, § 1er, 1^o, c), de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » (ci-après : la loi du 30 juillet 2018) que les catégories de destinataires des cartes d'information seront identifiées dans le registre des traitements des données, de sorte que les organes de contrôle compétents pourront opérer les vérifications nécessaires. Cinquièmement, le Conseil des ministres estime que les parties requérantes n'expliquent pas en quoi les extraits de l'avis de l'APD auxquels elles se réfèrent démontrent que l'absence d'une liste exhaustive des destinataires potentiels de la carte d'information porte atteinte au principe de légalité. Il souligne que le législateur s'est conformé aux recommandations de l'APD.

A.9. Les septième et huitième griefs sont pris de la violation des exigences de nécessité et d'efficacité.

A.10.1. Dans le septième grief, les parties requérantes soutiennent que le législateur n'a pas tenu compte des observations de l'APD relatives aux services qui ont accès à la banque de données commune T.E.R. Selon les parties requérantes, l'obligation de prévoir un rapport d'évaluation périodique découle bien de l'article 52, paragraphe 1, de la Charte et de l'article 8 de la Convention européenne des droits de l'homme.

A.10.2. Selon le Conseil des ministres, le premier moyen, en son septième grief, n'est pas fondé. Il indique que la banque de données commune « Terrorist Fighters » (combattants terroristes) et la banque de données commune « Propagandistes de haine » ont été créées en 2016 et en 2018, à la suite des attentats du 22 mars 2016, afin d'assurer un partage d'informations plus efficace entre les services compétents en matière de lutte contre les menaces terroristes et extrémistes. La loi attaquée tient compte des rapports annuels du Comité permanent R et de l'Organe de contrôle de l'information policière relatifs à ces banques de données. Dans ces rapports, le bien-fondé des accès fournis aux partenaires des banques de données communes n'est jamais remis en cause. Ces rapports ne soulèvent pas non plus de difficulté quant au respect du principe de proportionnalité. Au contraire, ils déplorent une sous-alimentation des banques de données par certains services. Le Conseil des ministres soutient par ailleurs que la recommandation de l'APD relative à la réalisation de statistiques aux fins de la publication d'un rapport d'évaluation périodique portant sur l'efficacité des moyens de traitement mis en œuvre et des autorités impliquées par la loi attaquée s'apparente à une critique d'opportunité qui ne relève pas de la compétence de la Cour. L'article 52, § 1er, de la Charte et l'article 8 de la Convention européenne des droits de l'homme n'imposent pas

une telle obligation, selon le Conseil des ministres. Enfin, les organes parlementaires chargés de contrôler la banque de données commune T.E.R. peuvent exiger, le cas échéant, la production de statistiques.

A.11.1. Dans le huitième grief, les parties requérantes soutiennent que le législateur n'a pas tenu compte des observations faites par l'APD dans son avis n° 97/2023, précité, en ce qui concerne la participation, prévue à l'article 32 de la loi attaquée, de l'Office des étrangers et des autres services aux « Task Forces locales ». Le fait que la loi du 15 décembre 1980 « sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers » confie aux autorités compétentes le soin de limiter ou d'interdire le séjour sur le territoire belge à des fins de sécurité nationale ne permet pas de déduire que ces autorités agissent à des fins de sécurité nationale.

A.11.2. Selon le Conseil des ministres, le premier moyen, en son huitième grief, n'est pas fondé. Il observe, premièrement, que les parties requérantes ne développent pas les motifs pour lesquels la loi attaquée dans son ensemble devrait être annulée sur la base de ce grief, et non uniquement l'article 32 de celle-ci. Elles n'expliquent pas davantage en quoi cette dernière disposition ne serait pas conforme au principe de légalité. Deuxièmement, contrairement à ce que soutient l'APD dans son avis, la référence faite par le législateur à l'affaire *Jürgen Conings* sert à illustrer la problématique à laquelle la loi attaquée entend répondre et non à justifier la participation de l'Office des étrangers et des autres services aux « Task Forces locales ». Cette participation fait suite aux recommandations de la Commission d'enquête parlementaire sur les attentats de 2016. La présence de l'Office des étrangers et des autres services au sein des « Task Forces locales » se justifie par leurs compétences dans des matières liées à l'ordre public et à la sécurité nationale. L'Office des étrangers assure en outre la coordination entre les mesures prises à l'égard d'un étranger par les différents intervenants à la « Task Force » locale. Troisièmement, le Conseil des ministres renvoie aux arguments consacrés à la réfutation du cinquième grief en ce qui concerne la critique de l'APD selon laquelle les services susceptibles d'être invités à la « Task Force » locale doivent être déterminables. Quatrièmement, la notion d'échange de données au sens de l'article 31 de la loi attaquée ne constitue pas un traitement. Il s'agit d'un échange oral ne relevant pas de la compétence de l'APD. Les échanges écrits entre partenaires de la banque de données commune T.E.R. s'effectuent dans le cadre de celle-ci. Les participants invités à la « Task Force » locale ne participent pas à un échange de données : ils apportent une contribution à sens unique à la « Task Force » locale afin de contextualiser la situation particulière d'une entité.

A.12. Les neuvième à douzième griefs sont pris de la violation de l'exigence de proportionnalité.

A.13.1. Dans le neuvième grief, les parties requérantes reprochent à l'article 5 de la loi attaquée de ne pas, d'une part, distinguer les finalités de la banque de données commune T.E.R. et les finalités des traitements des données à caractère personnel réalisés par chaque service et, d'autre part, intégrer les nécessités stratégiques, tactiques et opérationnelles dans des banques de données différentes.

A.13.2. Selon le Conseil des ministres, le premier moyen, en son neuvième grief, n'est pas fondé. Il constate que le législateur a répondu, à la suite de l'avis de l'APD n° 97/2023, précité, aux critiques des parties requérantes relatives aux finalités de la banque de données. La loi attaquée ne crée pas de nouveaux droits pour les services concernés. Lorsque ceux-ci peuvent déjà accéder aux données de la banque de données commune T.E.R. en vertu des finalités de traitement prévues par leurs lois organiques respectives, une simple référence à ces lois organiques suffit. Il n'est par ailleurs pas souhaitable de créer des banques de données distinctes pour les informations stratégiques, d'une part, et pour les informations tactiques et opérationnelles, d'autre part. La section de législation du Conseil d'État recommande d'ailleurs d'éviter de multiplier les banques de données liées à la lutte contre le terrorisme et l'extrémisme.

A.14.1. Dans le dixième grief, les parties requérantes soutiennent que la liste, visée à l'article 6, § 2, de la loi attaquée, des catégories de données pouvant être traitées dans la banque de données commune T.E.R. est longue et disproportionnée et qu'elle ne tient pas compte de l'avis de l'APD n° 97/2023, précité. Les parties requérantes précisent qu'il n'existe pas de lien de causalité entre la longueur de la liste et le caractère disproportionné de celle-ci. Elles font valoir que le traitement des données relatives aux convictions philosophiques ou politiques est disproportionné dès lors qu'un tel traitement est sans lien avec l'objectif, poursuivi, de lutte contre le terrorisme.

A.14.2. Le Conseil des ministres soutient que le premier moyen, en son dixième grief, n'est pas fondé. Selon lui, la longueur d'un article n'implique pas, en soi, que son contenu soit disproportionné. Les parties requérantes, en se contentant de renvoyer à l'avis de l'APD, restent en défaut d'expliquer en quoi le principe de proportionnalité serait violé. Enfin, le législateur a répondu aux critiques de l'APD. Le Conseil des ministres précise que le traitement des données à caractère politique, idéologique, confessionnel ou philosophique est limité aux conceptions ou visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires qui seraient contraires aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit, en ce compris le processus de radicalisation.

A.15.1. Dans le onzième grief, les parties requérantes font valoir que la durée de conservation des données sous la forme d'un archivage d'au maximum 30 ans, prévue à l'article 7 de la loi attaquée, est disproportionnée. Elles se réfèrent, sur ce point, à l'avis précité de l'Organe de contrôle de l'information policière du 20 juin 2023 sur l'avant-projet de loi qui est à l'origine de la loi attaquée.

A.15.2. Le Conseil des ministres soutient que le premier moyen, en son onzième grief, n'est pas fondé. Selon le Conseil des ministres, le simple renvoi par les parties requérantes à l'avis de l'Organe de contrôle de l'information policière ne permet pas de comprendre en quoi cette disposition violerait le principe de proportionnalité. Le législateur a précisé que l'archivage des données visé à l'article 7 de la loi attaquée ne fait pas double emploi avec ce que prévoit la loi sur la fonction de police. Plusieurs mécanismes existants permettent de contrôler le respect des délais prévus par cette disposition. Enfin, la section de législation du Conseil d'État a estimé que l'article 7 ne violait pas le principe de proportionnalité.

A.16.1. Dans le douzième grief, les parties requérantes soutiennent que les droits des personnes concernées par un traitement de leurs données à caractère personnel dans la banque de données commune T.E.R., prévus à l'article 4 de la loi attaquée, ne sont pas suffisamment garantis. Premièrement, les limitations de ces droits ne sont pas prévisibles, à défaut pour la loi attaquée de déterminer clairement le ou les responsables de chaque traitement. Elles ajoutent qu'en ce qui concerne les traitements des données policières, le législateur aurait dû se conformer à l'arrêt de la Cour de justice de l'Union européenne du 16 novembre 2023 en cause de *Ligue des droits humains ASBL et BA c. Organe de contrôle de l'information policière* (C-333/22, ECLI:EU:C:2023:874). Elles demandent, le cas échéant, que la Cour pose une question préjudicielle à la Cour de justice. Deuxièmement, aucune obligation de notification active n'est prévue à l'égard des personnes surveillées permettant de les informer, à l'issue d'une mesure de surveillance, du fait qu'elles ont fait l'objet d'une telle mesure. Cette lacune est contraire à la jurisprudence de la Cour européenne des droits de l'homme, de la Cour de justice de l'Union européenne (CJUE, grande chambre, 4 juin 2013, C-300/11, ZZ. c. *Secretary of State for the Home Department*, ECLI:EU:C:2013:363, points 57-58) et de la Cour constitutionnelle (arrêts n^{os} 41/2019, ECLI:BE:GHCC:2019:ARR.041, et 145/2011, ECLI:BE:GHCC:2011:ARR.145). Elles demandent, le cas échéant, que la Cour pose une question préjudicielle à la Cour de justice. Selon les parties requérantes, les arguments du Conseil des ministres ne mènent pas à une autre conclusion, puisqu'il invoque le respect de l'obligation de notification active dès que celle-ci ne risque plus de compromettre la sécurité nationale. Elles font valoir qu'en l'absence d'une obligation de notification active, des personnes ayant fait l'objet d'une enquête pour des faits de terrorisme ne sont jamais informées du traitement de leurs données à caractère personnel si cette enquête n'aboutit pas à des poursuites pénales en raison, par exemple, d'un classement sans suite. Troisièmement, le droit d'accès aux données et le droit à un recours juridictionnel effectif ne sont pas suffisamment garantis en ce que la seule possibilité de contrôle dont disposent les personnes concernées consiste à saisir l'Organe de contrôle de l'information policière et le Comité permanent R, lesquels peuvent uniquement répondre que toutes les vérifications nécessaires ont été effectuées. Elles se réfèrent au rapport du 8 mai 2019 de la rapporteuse spéciale des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, intitulé « Visite en Belgique » (A/HRC/40/52/Add.5), ainsi qu'à l'arrêt de la Cour de justice de l'Union européenne du 16 novembre 2023, précité, en cause de *Ligue des droits humains ASBL et BA c. Organe de contrôle de l'information policière*.

A.16.2. Le Conseil des ministres soutient que le premier moyen, en son douzième grief, n'est pas fondé. Il indique que l'article 4 de la loi attaquée énonce clairement que les droits des personnes concernées par un traitement de leurs données à caractère personnel dans la banque de données commune T.E.R. sont régis au sous-titre 4 du titre 3 de la loi du 30 juillet 2018. Selon le Conseil des ministres, le législateur a ainsi défini un régime commun pour les traitements de données à caractère personnel réalisés au sein de la banque de données commune T.E.R. et pour les traitements de données à caractère personnel réalisés par l'OCAM. Dans les deux cas, une mutualisation des données à caractère personnel et des informations provenant de responsables du traitement, qui

ne sont pas tous soumis aux mêmes obligations en matière de protection des données, est effectuée. En ce qu'il vise l'arrêt de la Cour de justice de l'Union européenne du 16 novembre 2023 en cause de *Ligue des droits humains ASBL et BA c. Organe de contrôle de l'information policière*, précité, le Conseil des ministres estime que le douzième grief est irrecevable. Il n'aperçoit pas le lien entre cet arrêt et le titre 2 de la loi du 30 juillet 2018.

En ce qui concerne l'absence d'une obligation de notification active, le Conseil des ministres fait valoir, premièrement, que cette absence est justifiée par l'efficacité des mesures de lutte contre le terrorisme concernées et par la marge d'appréciation dont le législateur dispose en la matière. Il est impossible, selon le Conseil des ministres, dans le cadre de mesures de lutte contre le terrorisme ou de la propagande de haine pouvant mener au terrorisme, de s'assurer à un moment donné qu'une entité inscrite dans la banque de données commune T.E.R. ne constitue plus une menace pour la sûreté de l'État et qu'une notification puisse être donnée à cette entité « sans compromettre le but de la restriction ». Selon le Conseil des ministres, face à l'ampleur du phénomène des attaques terroristes et au nombre de victimes de ces attaques, la prudence doit guider le législateur dans la détermination des informations qui peuvent être fournies aux personnes inscrites dans la banque de données commune T.E.R. Il estime que l'absence d'une obligation de notification active ne viole pas le principe de proportionnalité eu égard aux enjeux de la lutte contre le terrorisme et au type d'informations concernées, aux habilitations de sécurité requises pour accéder aux données reprises dans la banque de données commune T.E.R., ainsi qu'au faible nombre d'individus concernés par les mesures. Deuxièmement, des lois telles que la loi du 5 août 1992 « sur la fonction de police » et la loi du 10 juillet 2006 « relative à l'analyse de la menace » ne prévoient pas non plus d'obligation de notification active. Troisièmement, la loi attaquée ne soumet pas les individus inscrits dans la banque de données commune T.E.R. à une mesure de surveillance à proprement parler. Elle organise uniquement un partage d'informations et de données, qui permet à chaque service de base et partenaire de mieux exécuter ses missions légales. À la suite de ce partage d'informations, une notification de la personne concernée est faite, le cas échéant, par le service dans la mesure où celui-ci y est tenu lorsqu'il recourt à une mesure de surveillance. Quatrièmement, pour satisfaire à l'exigence d'un recours effectif devant un organe indépendant doté de ses propres règles de procédure, il suffit que soit mis en place un organe qui a accès à l'ensemble de l'information, ce qui est le cas du Comité permanent R et de l'Organe de contrôle de l'information policière.

Quant au deuxième moyen

A.17. Le deuxième moyen est pris de la violation des articles 10, 11 et 22 de la Constitution, lus en combinaison ou non avec l'article 10 de la Convention européenne des droits de l'homme et avec les articles 11 et 52 de la Charte. Les parties requérantes font valoir que la loi attaquée viole ces dispositions en ce qu'elle ne prévoit pas de garanties suffisantes pour protéger la liberté d'expression. Selon les parties requérantes, les mesures qui pourraient être prises sur la base d'une inscription dans la banque de données commune T.E.R. en raison d'un discours ou de propos protégés par la liberté d'expression constituent une restriction à cette liberté. En outre, le fait qu'il soit possible d'être inscrit dans la banque de données commune T.E.R. sur la seule base de propos qui n'incitent pas à la violence est susceptible d'avoir un effet dissuasif sur la liberté d'expression. Cela est d'autant plus important que le taux d'erreur des enquêtes préventives est élevé. La fragmentation des politiques belges de prévention du terrorisme entraîne par ailleurs de multiples interprétations des comportements indicateurs d'un risque et des propos considérés comme portant atteinte aux principes démocratiques et exerçant une influence radicalisante. Selon les parties requérantes, une violation, par la loi attaquée, de la liberté d'expression découle également des développements consacrés dans le premier moyen à la violation du principe de légalité. Elles se réfèrent à cet égard aux arrêts de la Cour n^{os} 145/2012 (ECLI:BE:GHCC:2012:ARR.145), 72/2016 (ECLI:BE:GHCC:2016:ARR.072) et 113/2023 (ECLI:BE:GHCC:2023:ARR.113).

A.18. Selon le Conseil des ministres, le deuxième moyen est irrecevable ou, à tout le moins, non fondé, dès lors que les parties requérantes ne démontrent pas en quoi la loi attaquée porterait une atteinte disproportionnée à la liberté d'expression. Le Conseil des ministres indique que les observations de la rapporteuse spéciale des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, auxquelles les parties requérantes se réfèrent, concernent le cadre législatif tel qu'il était applicable en Belgique en 2018. Ce cadre législatif a considérablement évolué depuis lors.

Quant au troisième moyen

A.19. Le troisième moyen est pris de la violation des articles 10, 11, 22 et 22bis de la Constitution, lus en combinaison ou non avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 24 et 52 de la Charte et avec les articles 3, 9, 12 et 40, paragraphe 1, de la Convention relative aux droits de l'enfant. Les parties requérantes soulèvent deux griefs.

A.20.1. Dans le premier grief, les parties requérantes soutiennent que l'âge minimal de douze ans auquel les mineurs peuvent être inscrits dans la banque de données commune T.E.R., en vertu de l'article 5 de la loi attaquée, n'est pas raisonnablement justifié. Premièrement, le législateur s'est référé à tort à l'observation générale n° 10 du Comité des droits de l'enfant dès lors que cette observation a été remplacée en 2020 par l'observation générale n° 24. Dans cette dernière, le Comité des droits de l'enfant recommande de fixer à quatorze ans au moins l'âge de la responsabilité pénale des mineurs. Deuxièmement, l'inscription dans la banque de données n'est pas directement comparable à la responsabilité pénale en termes de restrictions des droits humains, de sorte que le seuil d'âge applicable à l'un ne s'applique pas nécessairement à l'autre. Par ailleurs, l'âge de la responsabilité pénale en Belgique est de dix-huit ans et non de douze ou quatorze ans. Troisièmement, l'inscription d'un mineur dans la banque de données commune T.E.R. est susceptible de restreindre les droits fondamentaux de celui-ci pour une longue période avec des conséquences irrémédiables, compte tenu de l'absence de voies de recours pour obtenir la rectification des données contenues dans la banque de données ou la désinscription du mineur de celle-ci. Quatrièmement, la circonstance que la collecte, le traitement et la conservation des données personnelles d'enfants sont réalisés dans une perspective sécuritaire par des autorités non spécialisées dans la protection de la jeunesse est contraire aux droits de l'enfant. Cinquièmement, un seuil d'âge plus élevé serait plus conforme aux dispositions générales applicables en matière de protection des données, selon lesquelles un enfant de moins de treize ans ne peut pas consentir, en raison de son immaturité, au traitement de ses données personnelles.

A.20.2. Le Conseil des ministres soutient que le troisième moyen, en son premier grief, n'est pas fondé. Selon lui, il ressort des travaux préparatoires que les mesures relatives aux mineurs visent à protéger l'intérêt de ceux-ci et que les autorités chargées de la collecte, du traitement et de la conservation des données à caractère personnel relatives à des enfants adoptent à leur égard une attitude préventive. Il ajoute que selon la section de législation du Conseil d'État, il est aussi constitutionnel qu'une personne physique puisse être enregistrée dans la banque de données commune T.E.R. à partir de l'âge de douze ans.

A.21.1. Dans le second grief, les parties requérantes soutiennent que les articles 5 et 6 de la loi attaquée violent les normes de référence, en ce qu'ils prévoient l'enregistrement des enfants de « foreign terrorist fighters » (combattants terroristes étrangers) dans la base de données commune. Premièrement, les garanties prévues pour protéger les droits de ces enfants ne sont pas suffisantes. Deuxièmement, la détention d'informations relatives à ces enfants par d'autres organes que les services sociaux communautaires n'est pas nécessaire. Cela crée une différence de traitement non raisonnablement justifiée dès lors que seuls ces enfants sont enregistrés dans une banque de données policière en raison des infractions commises par leurs parents. Les parties requérantes se réfèrent à cet égard à l'avis du Comité permanent R n° 004/CPR/2023, précité, et aux avis des délégués généraux aux droits de l'enfant du 14 juin 2023 et du 21 juin 2023 rendus sur l'avant-projet de loi à l'origine de la loi attaquée. Troisièmement, le partage de l'identité de ces enfants avec l'ensemble des services disposant d'un droit de lecture dans la banque de données commune T.E.R. est disproportionné dès lors qu'il concerne des enfants qui sont particulièrement vulnérables. Il conduit par ailleurs à une confusion des rôles en matière de prévention et de contrôle du terrorisme, d'une part, et de protection de l'enfance, d'autre part. Quatrièmement, l'ajout d'une finalité protectionnelle à la banque de données commune T.E.R. porte atteinte au principe de finalité. Cinquièmement, les principes de minimisation et de pseudonymisation imposent que l'identité des mineurs concernés soit uniquement accessible aux services compétents pour assurer un suivi des enfants qui séjournent ou ont séjourné dans une zone de combat djihadiste. Une base de données spécifique pourrait être créée à cette fin. Les parties requérantes soutiennent que, contrairement à ce qu'allègue le Conseil des ministres, cette critique n'est pas d'opportunité mais qu'elle a trait au respect du principe de finalité qui est au cœur de la réglementation relative à la protection des données. Sixièmement, la durée de conservation des données relatives aux enfants est disproportionnée.

A.21.2. Le Conseil des ministres soutient que le troisième moyen, en son second grief, n'est pas fondé. Premièrement, la critique selon laquelle il aurait été plus judicieux de créer une base de données spécifique à laquelle seuls les services sociaux communautaires pourraient avoir accès est de pure opportunité et échappe dès

lors à la compétence de la Cour. Deuxièmement, les mineurs qui deviennent des entités dans la banque de données commune T.E.R. (article 5, 5°, *a*), de la loi attaquée) doivent être distinguées des enfants de « foreign terrorist fighters » nés « sur zone » (article 5, 5°, *b*), de la même loi). Les mineurs relevant de la première catégorie sont inscrits dans la base de données commune T.E.R. sous un statut spécifique si les finalités de celle-ci sont rencontrées. Il est toutefois prévu que le traitement de données à caractère personnel de ces mineurs vise l'aide à la protection, à l'accompagnement et au suivi de ceux-ci. Selon le Conseil des ministres, il ressort par ailleurs des travaux préparatoires que la présence des mineurs relevant de la seconde catégorie dans la banque de données commune T.E.R. est proportionnée. Troisièmement, le Conseil des ministres indique ne pas pouvoir déterminer si la critique des parties requérantes relative à la durée de conservation des données des mineurs est dirigée contre les articles 5 et 6 de la loi attaquée ou contre son article 7. Il soutient que les parties requérantes n'exposent pas en quoi la durée prévue par cette dernière disposition serait inconstitutionnelle.

- B -

Quant à la loi attaquée et à son contexte

B.1. Les parties requérantes demandent l'annulation totale ou partielle de la loi du 29 mars 2024 « portant création de la banque de données commune ' Terrorisme, Extrémisme, processus de Radicalisation ' (' T.E.R. ') et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police » (ci-après : la loi attaquée).

B.2.1. La loi attaquée crée une banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (ci-après : T.E.R.), qui « permet le traitement commun, par tout ou partie des services de base et des services partenaires, des données à caractère personnel et des informations relatives aux missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme, au sens de l'article 8, 1°, [alinéa 2,] *b*) et *c*), de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, de ces services, chacun dans le cadre de ses compétences légales » (article 3, alinéa 1er, de la loi attaquée).

Elle entend ainsi transposer dans une loi autonome les dispositions de la loi du 5 août 1992 « sur la fonction de police » (ci-après : la loi sur la fonction de police) relatives aux banques de données communes ainsi que la plupart des dispositions des arrêtés royaux relatifs, d'une part, à la banque de données commune « Terrorist fighters » (combattants terroristes) (anciennement

désignée : la banque de données commune « Foreign Terrorist Fighters » (combattants terroristes étrangers)) et, d'autre part, à la banque de données commune « Propagandistes de haine » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 5 et 7). Il s'agit, respectivement, (1) des articles 44/2 et suivants de la loi sur la fonction de police, tels qu'ils ont été modifiés par les articles 7 à 13 de la loi du 27 avril 2016 « relative à des mesures complémentaires en matière de lutte contre le terrorisme » (ci-après : la loi du 27 avril 2016), (2) de l'arrêté royal du 21 juillet 2016 « relatif à la banque de données commune Terrorist Fighters » (ci-après : l'arrêté royal du 21 juillet 2016), tel qu'il a été modifié par l'arrêté royal du 23 avril 2018 « modifiant l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters [et] portant exécution de certaines dispositions de la section 1^{er} *bis* ' de la gestion des informations ' du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters » et par l'arrêté royal du 20 décembre 2019 « modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters et l'arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1^{er} *bis* ' de la gestion des informations ' du chapitre IV de la loi sur la fonction de police » et (3) de l'arrêté royal du 23 avril 2018 « relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1^{er} *bis* ' de la gestion des informations ' du chapitre IV de la loi sur la fonction de police » (ci-après : l'arrêté royal du 23 avril 2018 « Propagandistes de haine »), tel qu'il a été modifié par l'arrêté royal du 20 décembre 2019 précité.

L'objectif de la banque de données commune T.E.R. est aussi de « renforcer la stratégie T.E.R relative à la banque de données commune et aux Task Forces locales » et de « mettre l'accent sur la nécessaire concertation entre professionnels de la sécurité à propos des données contenues dans la banque de données commune T.E.R. lesquels doivent notamment s'entendre sur l'opportunité de la prise de mesures lorsqu'une entité est enregistrée dans la banque de données commune » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 7).

B.2.2. La loi attaquée reprend « un maximum d'éléments » contenus dans les arrêtés royaux, précités, du 21 juillet 2016 et du 23 avril 2018 « Propagandistes de haine » pour

« donner une assise juridique plus forte à certaines dispositions, notamment en matière de protection des personnes à l'égard de traitements de données à caractère personnel et au niveau des catégories de données traitées » (*ibid.*). La majorité des dispositions de la loi sur la fonction de police relatives aux banques de données communes ou des arrêtés royaux précités ont été reprises dans la loi attaquée sans modification de fond (*ibid.*).

Sont traitées dans la banque de données commune T.E.R. les données à caractère personnel relatives à cinq catégories d'« entités » : les « foreign terrorist fighters », les « homegrown terrorist fighters », les extrémistes potentiellement violents, les personnes condamnées pour terrorisme et les propagandistes de haine (article 2, 4°, *juncto* l'article 6, § 2, 1°, de la loi attaquée). L'« entité » désigne la personne physique, la personne morale ou l'association de fait qui remplit les critères d'une des catégories précitées (« entité validée ») ou dont il existe des indices sérieux qu'elle peut remplir ces critères (« entité pré-enquête »), mais aussi l'ensemble des moyens utilisés par celle-ci, tels que « les moyens de transport, ou les numéros de téléphones/comptes utilisés » (article 2, 4°, de la loi attaquée et *Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 22).

Les données à caractère personnel traitées dans la banque de données commune T.E.R. sont les données non classifiées au sens de la loi du 11 décembre 1998 « relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé » (ci-après : la loi du 11 décembre 1998) (article 6, § 2, de la loi attaquée).

L'enregistrement d'une entité dans la banque de données T.E.R. a pour conséquence « d'une part, que l'échange de données et informations au sujet d'une entité se fait au sein d'une plateforme de concertation nommée [la « Task Force » locale] [...] et d'autre part, que la [« Task Force » locale], se concerte, dès la validation d'une entité dans la banque de données commune T.E.R. au sujet d'éventuelles mesures qui peuvent être prises suite à l'enregistrement d'une entité dans la banque de données commune T.E.R. Le résultat de cette concertation est transmis à l'autorité compétente pour décider de la mesure en question » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 132-133; voy. les articles 31 à 33 de la loi attaquée). Les mesures concernées sont, notamment, « le signalement policier, le signalement de renseignement, le signalement par l'Office des étrangers, conformément aux réglementations respectives en vigueur, ou encore le signalement dans le cadre de la réglementation belge

relative au traitement des données des passagers », la suspension ou le retrait « [d]es autorisations accordées aux entreprises de gardiennage, entreprises de consultance en sécurité, services internes de gardiennage et de détectives privés, [d]es agréments pour les entreprises de sécurité et les chargés de cours dans les organismes de formation ainsi que [d]es autorisations pour le personnel de travailler dans ce secteur » et des « permis d'armes octroyés aux agents de gardiennage », la mise en place d'une enquête sociale et fiscale, la mise en place d'une enquête financière, la prise de mesures spécifiques par les services de l'Office national de l'emploi (ONEm), l'Office wallon de la formation professionnelle et de l'emploi (FOREm), l'Office régional bruxellois de l'emploi (Actiris), Bruxelles formation, l'Office flamand de l'emploi et de la formation professionnelle (Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding ou VDAB) ou le Bureau de l'emploi de la Communauté germanophone de Belgique (Arbeitsamt der Deutschsprachigen Gemeinschaft Belgiens ou ADG), la prise de mesures spécifiques par l'Office des Étrangers, le refus, le retrait ou l'invalidation de passeport et de documents d'identité belge, l'inscription d'office ou la radiation d'office des registres de la population, le gel des avoirs, le suivi par les services de police, le suivi par les services de renseignement, le suivi des médias sociaux et les mesures prévues dans le règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 « relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne » et le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 « relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 142-146; article 33, § 2, de la loi attaquée).

B.2.3. Les ministres de l'Intérieur et de la Justice sont conjointement responsables du traitement de la banque de données commune T.E.R. (article 5, alinéa 1er, de la loi attaquée).

La police fédérale en est le gestionnaire (article 2 de l'arrêté royal du 14 juillet 2024 « relatif à la banque de données commune 'Terrorisme, Extrémisme, processus de Radicalisation' ('T.E.R.') », ci-après : l'arrêté royal du 14 juillet 2024, pris en exécution de l'habilitation contenue dans l'article 11, alinéa 1er, de la loi attaquée). À ce titre, il lui incombe notamment de créer, de mettre à disposition, de gérer et d'assurer la maintenance de la banque

de données commune, d'organiser les droits et les accès nécessaires aux traitements à effectuer dans celle-ci et de veiller à la journalisation de ces traitements (article 11, alinéa 2, de la loi attaquée).

L'Organe de coordination pour l'analyse de la menace (ci-après : l'OCAM) est le responsable opérationnel de la banque de données commune T.E.R. (article 3 de l'arrêté royal du 14 juillet 2024, pris en exécution de l'habilitation contenue dans l'article 12, alinéa 1er, de la loi attaquée). À ce titre, l'OCAM valide notamment l'enregistrement d'une entité dans la banque de données commune, contrôle la qualité des données qui y sont traitées et veille à ce que les données soient utilisées conformément aux finalités prévues (article 12, alinéa 2, de la loi attaquée; *Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/002, p. 14).

L'Organe de contrôle de l'information policière et le Comité permanent de contrôle des services de renseignement et de sécurité (ci-après : le Comité permanent R) sont les autorités de protection des données chargées conjointement du contrôle des traitements réalisés dans la banque de données commune T.E.R. (ci-après : les autorités de contrôle) (article 29 *juncto* l'article 2, 22°, de la loi attaquée; article 161, alinéa 2, de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », tel qu'il a été inséré par l'article 46 de la loi attaquée).

B.2.4. La création de la banque de données commune T.E.R. vise principalement à donner suite à la recommandation faite par la commission d'enquête parlementaire « chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste » (ci-après : la commission d'enquête parlementaire « Attentats terroristes ») et l'Autorité de protection des données de conférer une base juridique *ad hoc* aux banques de données communes existantes « Terrorist fighters » et « Propagandistes de haine ». Ces dernières ont été créées par les arrêtés royaux précités, en exécution de l'habilitation conférée par l'article 44/11/3*bis* de la loi sur la fonction de police, tel qu'il a été introduit par l'article 13 de la loi du 27 avril 2016, aux ministres de l'Intérieur et de la Justice pour créer conjointement des banques de données

communes en vue de l'exercice conjoint des missions de prévention et de suivi du terrorisme ou de l'extrémisme pouvant mener au terrorisme. Ces banques de données constituent techniquement une seule banque de données commune, « qui comme son nom l'indique, est commune à différents services et qui n'[a] donc pas de raison spécifique d'être rattachée à la loi sur la fonction de police » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 5; voy. aussi, DOC 55-3692/002, p. 3).

La création de la banque de données commune T.E.R. tend également, à la suite de « l'affaire Conings », à prévoir « l'obligation pour la Task Force Locale, lorsqu'une entité est reprise dans la banque de données commune T.E.R. de parcourir une liste de mesures qui peuvent être prises à l'égard d'une entité » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 6), par exemple « le retrait d'une autorisation de détention d'arme, d'une habilitation, d'un titre de séjour, etc. » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/002, p. 5).

Enfin, la création de la banque de données commune T.E.R. vise, suite « au décès tragique d'un policier poignardé par une personne [qui était] enregistrée dans la banque de données T.E.R. et qui avait été conduite dans un hôpital suite à la suspicion de troubles psychiatriques mais qui est repartie avant d'avoir été examinée par un professionnel de la santé » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 6), à permettre, d'une part, « aux services de base de communiquer des données relatives à la santé mentale et physique et à la dangerosité des personnes enregistrées dans la banque de données T.E.R. aux professionnels des soins de santé » et, d'autre part, « à l'ensemble des policiers qui sont sur le terrain de [...] prendre connaissance de l'évaluation de la menace d'une personne qui est enregistrée dans la banque de données T.E.R. et avec laquelle ils sont en contact sans devoir disposer d'une habilitation de sécurité » (*ibid.*).

B.3. La loi attaquée modifie trois autres lois et un code, à savoir la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » (ci-après : la loi sur la protection des données), la loi du 30 juillet 2018 « portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme », la loi sur la fonction de police et le Code consulaire.

Les modifications qui sont apportées à ces lois et à ce Code figurent dans le chapitre 4 de la loi attaquée (articles 34 à 54).

B.4. La loi attaquée est entrée en vigueur le 1er octobre 2024 (article 11, 1°, de l'arrêté royal du 14 juillet 2024, pris en exécution de l'habilitation contenue dans l'article 60, alinéa 2, de la loi attaquée). Ont été abrogés, à cette même date, l'article 44/11/3bis, précité, de la loi sur la fonction de police (article 55, 3°, de la loi attaquée), ainsi que les arrêtés royaux du 21 juillet 2016 et du 23 avril 2018 précités (articles 10 et 11, 2°, de l'arrêté royal du 14 juillet 2024; articles 56 et 57 de la loi attaquée *juncto* l'article 11, 1°, de l'arrêté royal du 14 juillet 2024).

Quant à la recevabilité des moyens

B.5.1. Pour satisfaire aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, les moyens de la requête doivent faire connaître, parmi les règles dont la Cour garantit le respect, celles qui seraient violées ainsi que les dispositions qui violeraient ces règles et exposer en quoi ces règles auraient été transgressées par ces dispositions.

Pour satisfaire aux exigences précitées, il incombe en particulier à toute partie requérante d'axer ses critiques sur les dispositions attaquées telles que le législateur les a finalement adoptées, au lieu de se fonder sur les versions qui étaient reprises dans le projet (ou l'avant-projet) de loi et auxquelles le législateur a encore apporté ou a pu apporter des modifications substantielles, par exemple à la suite des remarques d'une instance consultative.

B.5.2. La Cour n'examine le recours en annulation qu'en tant qu'il satisfait aux exigences précitées.

Quant au premier moyen (droit au respect de la vie privée, droit à la protection des données à caractère personnel et droit à un recours effectif)

B.6.1. Le premier moyen est pris de la violation des articles 10, 11 et 22 de la Constitution, lus en combinaison ou non avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 8, 10, 13 à 15 et 54 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil » (ci-après : la directive « police ») et avec les articles 7, 8, 47 et 52 de la Charte des droits fondamentaux de l'Union européenne (ci-après : la Charte). Il est subdivisé en douze griefs.

Selon les parties requérantes, la loi attaquée porterait atteinte au droit au respect de la vie privée, au droit à la protection des données à caractère personnel et au droit à un recours effectif, qui sont garantis par ces dispositions.

Les premier à sixième griefs sont pris de la violation du principe de légalité, dans ses dimensions formelle et matérielle.

Les septième et huitième griefs sont pris de la violation des exigences de nécessité et d'efficacité.

Les neuvième à douzième griefs sont pris de la violation du principe de proportionnalité.

B.6.2. Le droit au respect de la vie privée, tel qu'il est garanti par l'article 22 de la Constitution et par l'article 8 de la Convention européenne des droits de l'homme, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée. La proposition qui a précédé l'adoption de l'article 22 de la Constitution insistait sur « la protection de la personne, la reconnaissance de son identité, l'importance de son épanouissement et celui de sa famille » et elle soulignait la nécessité de protéger la vie privée et familiale « des risques d'ingérence que peuvent constituer, notamment par le biais de la modernisation constante des

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

Le droit au respect de la vie privée a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles. De la protection de ce droit relèvent notamment les données et informations personnelles suivantes : le nom, l'adresse, les activités professionnelles, les relations personnelles, les empreintes digitales, les images filmées, les photographies, les communications, les données ADN, les données judiciaires (condamnations ou inculpations), les données financières, les informations concernant des biens et les données médicales (voy. notamment CEDH, 26 mars 1987, *Leander c. Suède*, ECLI:CE:ECHR:1987:0326JUD000924881, §§ 47-48; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, §§ 66-68; 13 octobre 2020, *Frâncu c. Roumanie*, ECLI:CE:ECHR:2020:1013JUD006935613, § 51).

B.6.3. Le droit au respect de la vie privée n'est toutefois pas absolu. L'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme n'excluent pas une ingérence d'une autorité publique dans l'exercice de ce droit, pourvu que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit.

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

B.6.4. Dans le champ d'application du droit de l'Union européenne, l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme et l'article 7 de la Charte garantissent des droits fondamentaux analogues (CJUE, grande chambre,

9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke GbR e.a.*, ECLI:EU:C:2010:662), alors que l'article 8 de cette Charte vise spécifiquement la protection des données à caractère personnel.

La compatibilité d'une disposition législative avec les articles 7 et 8 de la Charte, lus en combinaison avec l'article 22 de la Constitution, ne peut être examinée par la Cour qu'en ce que la disposition attaquée entre dans le champ d'application du droit de l'Union (CJUE, grande chambre, 26 février 2013, C-617/10, *Åklagaren*, ECLI:EU:C:2013:105, points 17 et suiv.).

B.6.5. Les droits consacrés aux articles 7 et 8 de la Charte n'apparaissent pas non plus comme étant des prérogatives absolues (CJUE, grande chambre, 16 juillet 2020, C-311/18, *Data Protection Commissioner*, ECLI:EU:C:2020:559, point 172).

Conformément à l'article 52, paragraphe 1, première phrase, de la Charte, toute limitation de l'exercice des droits et libertés reconnus par celle-ci, dont le droit au respect de la vie privée garanti par l'article 7 et le droit à la protection des données à caractère personnel consacré par l'article 8, doit être prévue par la loi, respecter le contenu essentiel de ces droits et, dans le respect du principe de proportionnalité, être nécessaire et répondre effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui (CJUE, grande chambre, 6 octobre 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, point 64).

B.6.6. L'article 47 de la Charte prévoit le droit à un recours effectif.

B.6.7. Les traitements de données à caractère personnel effectués dans la banque de données commune T.E.R. sont réglés au sous-titre 4 du titre 3 de la loi sur la protection des données (article 4 de la loi attaquée; article 139, alinéa 1er, de la loi sur la protection des données, tel qu'il a été modifié par l'article 37 de la loi attaquée). Les titres 1er, 2, 4, 5 et 7 de cette loi ne s'appliquent pas à ces traitements. Sous le titre 6, seuls les articles 226, 227 et 230 s'y appliquent (article 139, alinéa 2 de la loi sur la protection des données).

B.7. Les griefs des parties requérantes portent sur les aspects suivants :

1. les notions de « propagandistes de haine » et d'« extrémistes potentiellement violents » (B.8 à B.12);
2. les finalités de l'interconnexion entre les banques de données (B.13 à B.15);
3. les droits d'accès des services partenaires (B.16 à B.20);
4. les services susceptibles d'être invités par la « Task force » locale (B.21 à B.23);
5. les mesures visées à l'article 33, § 2, 7° et 8°, de la loi attaquée (B.24 à B.26);
6. les destinataires de la « carte d'information » (B.27 à B.30);
7. les services ayant accès à la banque de données (B.31 à B.33);
8. la participation de l'Office des étrangers et des autres services aux « Task Forces locales » (B.34 à B.36);
9. les finalités du traitement (B.37 à B.39);
10. les catégories de données (B.40 à B.43);
11. la durée de conservation des données (B.44. à B.48);
12. les droits des personnes concernées (B.49 à B.56).

1. En ce qui concerne les notions de « propagandistes de haine » et d'« extrémistes potentiellement violents » (article 2, 9° et 11°, de la loi attaquée)

B.8. Les parties requérantes font valoir que l'article 2, 11°, de la loi attaquée viole le principe de légalité en ce qu'il ne définit pas de manière suffisamment précise la notion de « propagandistes de haine ».

B.9.1. L'article 22 de la Constitution réserve au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée. Il garantit ainsi à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

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

Par conséquent, les éléments essentiels du traitement des données à caractère personnel doivent être fixés dans la loi, le décret ou l'ordonnance même. À cet égard, quelle que soit la matière concernée, les éléments suivants constituent, en principe, des éléments essentiels : (1) la catégorie de données traitées, (2) la catégorie de personnes concernées, (3) la finalité poursuivie par le traitement, (4) la catégorie de personnes ayant accès aux données traitées et (5) le délai maximal de conservation des données.

B.9.2. Outre l'exigence de légalité formelle, l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8 et 52 de la Charte, impose que l'ingérence dans l'exercice du droit au respect de la vie privée et du droit à la protection des données à caractère personnel soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

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

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

B.9.3. En matière de surveillance secrète, l'exigence de prévisibilité ne peut pas se comprendre de la même façon que dans la plupart des autres domaines. Les États ne sont notamment pas tenus d'édicter des dispositions juridiques énumérant dans le détail tous les comportements pouvant conduire à la décision de soumettre un individu à une surveillance secrète pour des motifs de sécurité nationale. Toutefois, compte tenu du risque d'arbitraire inhérent à l'exercice en secret d'une prérogative de la puissance publique, le droit interne doit être suffisamment clair pour que chacun puisse s'assurer de manière adéquate des circonstances et des conditions dans lesquelles la puissance publique est habilitée à recourir à pareilles mesures secrètes. En outre, la loi doit définir l'étendue et les modalités d'exercice du pouvoir d'appréciation accordé aux autorités compétentes avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire (CEDH, grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*, ECLI:CE:ECHR:2015:1204JUD004714306, §§ 229, 230 et 247; grande chambre, 25 mai 2021, *Big Brother Watch e.a. c. Royaume-Uni*, ECLI:CE:ECHR:2021:0525JUD005817013, § 333). Il convient également de tenir compte des modalités du contrôle de l'application de mesures de surveillance secrète, de l'existence éventuelle d'un mécanisme de notification et des recours prévus en droit interne (CEDH, grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*, précité, §§ 231 et 238; grande chambre, 25 mai 2021, *Big Brother Watch e.a. c. Royaume-Uni*, précité, § 335).

B.10.1. Selon l'article 2, 11°, de la loi attaquée, les « propagandistes de haine » sont :

« les personnes physiques ou morales, associations de fait, y compris l'ensemble des moyens utilisés par celles-ci, nonobstant leur nationalité, lieu de résidence ou siège, qui remplissent les critères cumulatifs suivants :

a) ont pour objectif de porter atteinte aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit;

b) justifient l'usage de la violence ou de la contrainte comme moyen d'action;

c) propagent leurs convictions aux autres en vue d'exercer une influence radicalisante; on entend par ' influence radicalisante ' : toute action exercée par une entité dans le but d'initier, de soutenir ou de contribuer à un processus de radicalisation au sens de l'article 3, 15°, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité;

d) ont un lien avec la Belgique; ».

En vertu de cette disposition, sont considérés comme des « propagandistes de haine » au sens de la loi attaquée les personnes physiques ou morales et les associations de fait, ainsi que l'ensemble des moyens utilisés par celles-ci (par exemple « un site web, des tracts, des messages radio ou télévision, des chaînes de radio ou de télévision, des centres de propagandes ou culturels, des locaux, etc. ») (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 34-35) - que ces personnes physiques ou morales et associations de fait aient ou non la nationalité belge et qu'elles aient ou non leur lieu de résidence ou leur siège en Belgique -, qui remplissent les quatre critères cumulatifs énumérés dans cette disposition.

Les « propagandistes de haine » sont l'une des catégories d'« entités » dont les données à caractère personnel sont traitées dans la banque de données T.E.R. (article 2, 4°, *juncto* l'article 6, § 2, 1°, de la loi attaquée).

B.10.2. La notion de « propagandistes de haine » n'était pas définie dans l'avant-projet qui est à l'origine de la loi attaquée (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 160-162).

Dans son avis n° 73.442/2 du 7 juin 2023 sur cet avant-projet de loi, la section de législation du Conseil d'État a recommandé au législateur de préciser lui-même les catégories d'entités dont les données sont susceptibles d'être traitées dans la banque de données

commune T.E.R., dès lors qu'il s'agit d'un élément essentiel relatif au traitement de ces données (*ibid.*, pp. 200-202).

À la suite de cet avis, une définition de la notion de « propagandistes de haine » a été introduite à l'article 2, 11°, du projet de loi (*ibid.*, p. 228), lequel est devenu l'article 2, 11°, précité, de la loi attaquée. Cette définition reprend (en la déclinant au pluriel et en y ajoutant une définition de la notion d'« influence radicalisante ») les termes de l'ancien article 1er, 11°, de l'arrêté royal du 23 avril 2018 « Propagandistes de haine », tel qu'il était applicable avant son abrogation par l'article 57, 1°, de la loi attaquée, selon lesquels le « propagandiste de haine » est « la personne physique ou morale, l'association de fait ainsi que l'ensemble des moyens utilisés par celles-ci visés à l'article 6, § 1er, 1°, du présent arrêté ». Ledit article 6, § 1er, 1°, du même arrêté royal, tel qu'il était applicable avant son abrogation par l'article 57, 6°, de la loi attaquée, disposait que les données à caractère personnel et les informations traitées dans la banque de données « Propagandistes de haine » étaient :

« les données d'identification relative[s] aux entités nonobstant leur nationalité, lieu de résidence ou siège, et qui remplissent les critères cumulatifs suivants :

- a) ont pour objectif de porter atteinte aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'Etat de droit;
- b) justifient l'usage de la violence ou de la contrainte comme moyen d'action;
- c) propagent [leurs] convictions aux autres en vue d'exercer une influence radicalisante;
- d) ont un lien avec la Belgique ».

B.10.3. Comme il est dit en B.10.1, il ressort des termes de la disposition attaquée que ces critères sont cumulatifs.

Le fait, pour une personne, une association de fait ou des moyens, de ne pas satisfaire à l'un de ces critères suffit pour qu'ils ne soient pas enregistrés comme « propagandistes de haine » dans la base de données commune T.E.R.

B.10.4. La nature cumulative des critères visés à l'article 2, 11°, de la loi attaquée garantit que l'exigence de porter atteinte aux principes et droits qui fondent la société démocratique et l'État de droit visée sous le *littera a)* de cette disposition ne puisse pas être interprétée de

manière extensive et ne met pas les personnes concernées dans l'impossibilité de prévoir le seuil à partir duquel elles sont considérées comme « propagandistes de haine ». En particulier, la circonstance que la personne concernée a « pour but » de porter l'atteinte visée ci-avant implique qu'elle ait conscience dans une certaine mesure des conséquences potentielles de ses actes pour les fondements et le fonctionnement de l'État de droit démocratique.

B.10.5. À propos de l'exigence de « justifi[cation de] l'usage de la violence ou de la contrainte comme moyen d'action » visée à l'article 2, 11°, *b*), de la loi attaquée, les travaux préparatoires précisent :

« Le propagandiste de haine justifie l'usage de la violence ou de la force (y compris [...] toutes [les] formes de violence ou de [la] force, comme la violence physique et psychique, la violence intra- et extrafamiliale, la violence homophobe, les cyber-attaques, ...) afin de réaliser [l']objectif [de] porter atteinte, en théorie ou en pratique, aux institutions démocratiques ou aux autres fondements de l'État de droit ainsi qu'aux droits de l'homme [...]. Le propagandiste de haine manifeste son intention de porter préjudice ainsi que la justification du recours à la violence ou la force envers une ou plusieurs entités, par le biais d'actions ou de canaux concrets. L'intention doit être extériorisée publiquement au travers par exemple d'une publication » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 33).

B.10.6. À propos de l'exigence de « propag[ation de] [ses] convictions aux autres en vue d'exercer une influence radicalisante » visée à l'article 2, 11°, *c*), de la loi attaquée, cette disposition précise que la notion d'« influence radicalisante » désigne « toute action exercée par une entité dans le but d'initier, de soutenir ou de contribuer à un processus de radicalisation au sens de l'article 3, 15°, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité ».

L'article 3, 15°, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après : la loi organique du 30 novembre 1998) définit le « processus de radicalisation » comme « un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes ».

L'article 8, 1°, alinéa 2, *b*), de la même loi définit le « terrorisme » comme « le recours à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou

politiques, dans le but d'atteindre ses objectifs par la terreur, l'intimidation ou les menaces en ce compris le processus de radicalisation ».

Par son arrêt n° 145/2011 du 22 septembre 2011 (ECLI:BE:GHCC:2011:ARR.145), la Cour a jugé que la définition du « processus de radicalisation » contenue dans l'article 3, 15°, précité, de la loi organique du 30 novembre 1998, lue en combinaison avec celle de « terrorisme » visée à l'article 8, 1°, alinéa 2, *b*), de la même loi satisfait au principe de légalité garanti par l'article 22 de la Constitution :

« B.96.3. L'emploi de la notion de ' processus de radicalisation ', combiné avec celle de ' terrorisme ', renvoie ainsi à la phase qui précède la commission d'actes terroristes. En particulier, le processus de radicalisation vise un processus préparatoire de manipulation ou d'influence faisant apparaître des risques sécuritaires. L'article 3, 15°, de la loi du 30 novembre 1998 indique clairement qu'il s'agit d'un processus consistant à influencer l'intéressé de telle manière qu'il soit préparé ou disposé à commettre des actes terroristes. L'habilitation à utiliser les méthodes exceptionnelles de renseignement dans le cadre d'une menace grave relative à une activité du processus de radicalisation s'inscrit donc dans l'action préventive contre le terrorisme.

B.97. Il découle de ce qui précède que la disposition attaquée ne porte pas atteinte au principe de légalité consacré par l'article 22 de la Constitution ».

La notion d'« influence radicalisante » définie dans la disposition attaquée et lue en combinaison avec les définitions légales, précitées, des termes « processus de radicalisation » et « terrorisme » est suffisamment claire, de sorte que la personne concernée peut prévoir les circonstances dans lesquelles un traitement des données à caractère personnel peut avoir lieu.

B.10.7. Il ressort des travaux préparatoires cités en B.10.5 et de la nature cumulative des critères visés à l'article 2, 11°, de la loi attaquée que les termes « justifie[r] l'usage de la violence ou de la contrainte comme moyen d'action » contenus dans l'article 2, 11°, *b*), de la loi attaquée doivent être lus en combinaison avec ceux d'« influence radicalisante » visés à l'article 2, 11°, *c*), de la même loi et avec ceux de « processus de radicalisation » et de « terrorisme » visés aux articles 3, 15°, et 8, 1°, alinéa 2, *b*), de la loi organique du 30 novembre 1998.

Le terme « contrainte » doit s'interpréter dans son sens usuel, ce qui suppose en l'espèce l'exercice d'un certain pouvoir sur un individu, lequel se trouve ainsi forcé d'agir contre son gré. La mention de ce terme en apposition à celui de « violence » ne dénie pas de sa clarté le

critère de « justifi[cation de] l'usage de la violence ou de la contrainte comme moyen d'action ». Contrairement à ce que prétendent les parties requérantes, ce critère n'a en outre pas pour conséquence que des personnes plaident simplement sans violence pour des changements sociétaux, quand bien même elles appelleraient ce faisant à la désobéissance civile, doivent être considérées comme des « propagandistes de haine ».

B.10.8. En vertu des articles 20 et 21 de la loi du 30 juillet 1981 « tendant à réprimer certains actes inspirés par le racisme ou la xénophobie », auxquels les parties requérantes se réfèrent, quiconque, dans l'une des circonstances indiquées à l'article 444 du Code pénal, incite à la discrimination, à la haine ou à la violence à l'égard d'une personne en raison de l'un des critères protégés mentionnés dans cette loi ou à la discrimination, à la ségrégation, à la haine ou à la violence à l'égard d'un groupe, d'une communauté ou de leurs membres en raison de l'un de ces critères, et quiconque diffuse des idées fondées sur la supériorité ou la haine raciale, sont punis d'un emprisonnement d'un mois à un an et d'une amende de 50 euros à 1 000 euros ou de l'une de ces peines seulement.

Alors que ces dispositions pénales assortissent d'une incrimination l'« incitation à la discrimination, à la ségrégation, à la haine ou à la violence » et la « diffusion d'idées fondées sur la supériorité ou la haine raciale », tel n'est pas le cas pour l'article 2, 11°, de la loi attaquée, qui n'assortit d'aucune incrimination la définition de « propagandistes de haine ». Il s'ensuit que, contrairement à ce que les parties requérantes soutiennent, la notion de « propagandistes de haine » et les infractions précitées d'« incitation à la discrimination, à la ségrégation, à la haine ou à la violence » et de « diffusion d'idées fondées sur la supériorité ou la haine raciale » ne sauraient être confondues.

B.11. En ce qu'il porte sur la notion de « propagandistes de haine » visée à l'article 2, 11°, de la loi attaquée, le grief n'est pas fondé.

B.12.1. Les parties requérantes font valoir que des critiques analogues à celles qu'elles dirigent contre la notion de « propagandistes de haine » peuvent être formulées à l'égard de la notion d'« extrémistes potentiellement violents » visée à l'article 2, 9°, de la loi attaquée.

B.12.2. Les parties requérantes n'exposent pas en quoi les critiques qu'elles développent à l'égard de la notion de « propagandistes de haine » sont susceptibles de s'appliquer à la notion, distincte, d'« extrémistes potentiellement violents ».

B.12.3. En ce qu'il porte sur la notion d'« extrémistes potentiellement violents » visée à l'article 2, 9°, de la loi attaquée, le grief est irrecevable.

2. En ce qui concerne les finalités de l'interconnexion entre les banques de données (article 9 de la loi attaquée)

B.13. Les parties requérantes font grief à l'article 9 de la loi attaquée de ne pas déterminer les finalités de l'interconnexion qu'il prévoit entre les banques de données.

B.14.1. L'article 9 de la loi attaquée dispose :

« § 1er. Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, une interconnexion des données visées à l'article 6, § 2, alinéa 1er, et des informations enregistrées dans la banque de données commune T.E.R. peut être établie entre la banque de données commune T.E.R. et d'autres banques de données gérées par les services de base ou les services partenaires dans le cadre de leurs missions légales ou les sources authentiques de données visées au paragraphe 2.

Le Roi détermine, après avis des responsables du traitement des banques de données visées à l'alinéa 1er et des autorités de contrôle compétentes, et pour les banques de données gérées par le partenaire visé à l'article 2, 3°, e), après accord du Collège du ministère public, les traitements visés par l'interconnexion, les catégories de données à caractère personnel interconnectées et les modalités d'interconnexion, lesquelles doivent respecter l'intégrité des données et des réseaux, en particulier pour ce qui concerne les banques de données qui contiennent des données classifiées au sens de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé.

§ 2. Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, pour les données visées à l'article 6, § 2, alinéa 1er, 1°, 1), a), i. à xii., une interconnexion peut être établie du registre national des personnes physiques visé à l'article 1er de la loi du 8 août 1983 organisant un registre national des personnes physique vers la banque de données commune T.E.R.

Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, pour les données visées à l'article 6, § 2, alinéa 1er, 1°, 2), a) à d), h) et i) et 3), a) à d), h) et i),

une interconnexion peut être établie de la Banque Carrefour des Entreprises visée à l'article III.15 du Code de droit économique vers la banque de données commune T.E.R.

Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, pour les données visées à l'article 6, § 2, alinéa 1er, 1°, 1), *h*), 2), *f*) et 3), *f*), une interconnexion peut être établie du répertoire-matricule des véhicules visée à l'article 6 de l'arrêté royal du 20 juillet 2001 relatif à l'immatriculation de véhicules vers la banque de données commune T.E.R.

Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, pour les personnes physiques et les personnes morales enregistrées dans la banque de données commune T.E.R., une interconnexion peut être établie du Casier judiciaire central visé à l'article 589 du Code d'instruction criminelle vers la banque de données commune T.E.R. ».

L'article 5, alinéa 2, de la loi attaquée dispose :

« Les finalités de la banque de données commune T.E.R. sont les suivantes :

- 1° la concertation coordonnée entre les services de base et les services partenaires;
- 2° la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des services de base et des services partenaires;
- 3° l'aide à la prise de décisions par les autorités administratives ou à la prise de décisions de police administrative ou judiciaire;
- 4° l'analyse, l'évaluation et le suivi, en ce compris la prise de mesures, des entités validées enregistrées dans la banque de données commune T.E.R., l'analyse, l'évaluation et le suivi des entités en pré-enquête enregistrées dans la banque de données commune T.E.R. et l'analyse, l'évaluation et le suivi du phénomène du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme;
- 5° l'aide à la protection, à l'accompagnement et au suivi des personnes suivantes :
 - a) les mineurs de douze ans ou plus qui sont considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine;
 - b) les enfants mineurs d'un *foreign terrorist fighter* qui répond aux critères visés à l'article 2, 7°, a) ou c), et qui ne sont pas ou ne peuvent pas être considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine ».

B.14.2. L'article 9 de la loi attaquée donne suite aux recommandations de la commission d'enquête parlementaire « Attentats terroristes », qui a « mis en évidence le besoin d'un

échange optimal des données collectées entre les services de sécurité et une gestion intégrée de l'information » (*Doc. parl., Chambre, 2023-2024, DOC 55-3692/001, pp. 93-94*). La possibilité d'établir une interconnexion entre la banque de données commune T.E.R. et d'autres banques de données gérées par les services de base ou par les services partenaires dans le cadre de leurs missions légales (article 9, § 1er) ainsi que les sources authentiques de données visées à l'article 9, § 2, (le Registre national des personnes physiques, la Banque-carrefour des entreprises, le Répertoire-matricule des véhicules et le Casier judiciaire central) vise notamment à « enrichir la banque de données commune T.E.R. avec les données d'autres bases de données existantes sans devoir réintroduire manuellement ces données dans la banque de données commune T.E.R. » et à permettre un accès aux données « les plus actuelles et [...] fiables possible[s] » provenant directement du service qui est à la source de celles-ci (*Doc. parl., Chambre, 2023-2024, DOC 55-3692/001, p. 92*). En ce qui concerne spécifiquement la possibilité d'établir une interconnexion entre la banque de données commune T.E.R. et les sources authentiques de données visées à l'article 9, § 2, l'objectif est d'« éviter que chaque service qui a un droit de lecture et d'écriture ne doive individuellement s'adresser au gestionnaire de ces bases de données pour obtenir l'accès aux données pertinentes de ces sources authentiques » (*ibid.*, p. 93).

B.14.3. Il ressort des termes de l'article 9 de la loi attaquée que cette disposition détermine les finalités de l'interconnexion qu'il prévoit entre les banques de données, en renvoyant aux finalités visées à l'article 5, alinéa 2, de la même loi.

B.15. Le grief n'est pas fondé.

3. *En ce qui concerne les droits d'accès des services partenaires (article 16 de la loi attaquée)*

B.16. Les parties requérantes font valoir que les habilitations du Roi contenues dans l'article 16 de la loi attaquée sont formulées en des termes trop larges.

B.17.1. L'article 16 de la loi attaquée dispose :

« Sur la base du respect des principes d'adéquation, de pertinence et du caractère non excessif, dans le cadre de l'exercice de leurs missions visées à l'article 3, et conformément aux finalités de l'article 5, alinéa 2, chacun dans le cadre de ses compétences respectives, les services partenaires peuvent disposer :

1° d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R.; ou

2° d'un droit d'interrogation dans la banque de données commune T.E.R.

Le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, pour chaque service partenaire, le type de droit et ses modalités d'exercice.

Pour le service partenaire visé à l'article 2, 3°, e), le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle et avis conforme du Collège des procureurs généraux, le type de droit et ses modalités d'exercice ».

B.17.2. La banque de données commune T.E.R. vise à rendre plus efficace le partage de données et d'informations entre les différents services qui interviennent dans la prévention et la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 4). Deux catégories de services ont accès à la banque de données commune T.E.R. : les « services de base », d'une part, et les « services partenaires », d'autre part (*ibid.*, pp. 9-10).

Les « services de base » sont identifiés à l'article 2, 2°, de la loi attaquée comme étant l'OCAM, la police intégrée et les services de renseignement et de sécurité, à savoir « [la] Sûreté de l'État (VSSE) et le Service Général du Renseignement et de [la] Sécurité (SGRS) » (*ibid.*, p. 9). Il s'agit de « services répressifs ou d'analyse qui travaillent directement en première ligne avec les entités et les finalités T.E.R. ou dont le travail d'analyse porte sur ces entités et, qui sont conséquemment susceptibles d'avoir le plus de données relatives à ces entités ou de détecter prioritairement une nouvelle entité T.E.R. » (*ibid.*).

Les « services partenaires » sont énumérés à l'article 2, 3°, de la loi attaquée :

« a) l'Unité d'information des passagers du Centre de Crise national du Service Public fédéral Intérieur;

b) la Direction générale Sécurité et Prévention du Service Public fédéral Intérieur;

c) la Direction générale des Etablissements Pénitentiaires du Service Public fédéral Justice;

d) la Direction générale Affaires Consulaires du Service Public fédéral Affaires étrangères;

e) le ministère public;

f) la Cellule de Traitement des Informations Financières;

g) la Direction générale de l'Office des Etrangers du Service Public fédéral Intérieur;

h) l'Administration générale des douanes et accises du Service Public fédéral Finances;

i) le Service des cultes et de la laïcité du Service Public fédéral Justice;

j) l'Autorité Nationale de Sécurité;

k) l'Administration générale de la Trésorerie du Service Public fédéral Finances;

l) dans le cadre de leurs missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions, l'Administration générale des Maisons de Justice de la Communauté Française, le département Maison de Justice du Ministère de la Communauté Germanophone, l'Agence flamande pour la Justice et le Maintien, l'Administration générale de l'Aide à la Jeunesse de la Communauté Française, le département Aide à la Jeunesse de la Communauté Germanophone et l'Agence flamande Opgroeien ».

Les services partenaires sont des « services fédéraux ou appartenant à des entités fédérées qui sont spécifiquement identifiés comme partenaires dans le cadre des finalités de la banque de données commune » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 10), à savoir :

« - soit un service de l'État qui exécute des missions de *law enforcement* en deuxième ligne qui touchent directement aux finalités et entités T.E.R. (comme par exemple, le Ministère public, la CTIF, la Direction Générale des Etablissements Pénitentiaires du Service public fédéral Justice);

- soit un service de l'État qui vu l'exercice de ses missions est susceptible de rentrer en contact avec une personne T.E.R., et qui s'il ne connaît pas sa qualité T.E.R. peut lui délivrer des 'prérogatives' au nom de l'État, notamment sous forme de documents administratifs lui permettant de s'établir en Belgique [et] d'exercer une profession rémunérée (comme par

exemple, l'Office des étrangers, les Affaires consulaires, la DG sécurité et prévention, le service [des] cultes et de la laïcité du SPF Justice) » (*ibid.*, pp. 10-11).

B.17.3. Les articles 14 et 16 de la loi attaquée définissent les types de droits d'accès à la banque de données commune T.E.R. dont disposent les services de base et les services partenaires.

Alors que les services de base disposent d'un « droit de création », d'un « droit de lecture » et d'un « droit d'écriture » dans la banque de données (article 14; voy. aussi article 17), les services partenaires disposent soit d'un « droit de lecture et d'un droit d'écriture » soit d'un « droit d'interrogation » (article 16, alinéa 1er).

Le droit de « création » concerne « l'enregistrement d'une nouvelle entité dans la banque de données commune T.E.R. » (article 2, 18°, de la loi attaquée). Le « droit de lecture » concerne « la consultation de l'ensemble des données à caractère personnel et des informations de la banque de données commune T.E.R. » (article 2, 19°). Le « droit d'écriture » concerne « l'introduction, modification ou effacement des données à caractère personnel et des informations dans la banque de données commune T.E.R. » (article 2, 20°). Le « droit d'interrogation » concerne « [la] prise de connaissance de l'existence d'une entité dans la banque de données commune T.E.R. et en cas de confirmation de l'existence d'une entité dans la banque de données commune T.E.R., la prise de connaissance de l'évaluation de la menace » visée à l'article 22 de la loi attaquée (article 2, 21°, *juncto* l'article 22).

Un droit de lecture, qui suppose l'accès à toutes les données de la banque de données commune, va de pair avec un droit d'écriture. « Le droit d'écriture ne peut en effet être utilement rempli que [...] si le service qui doit compléter la banque de données commune T.E.R. [...] avec les données visées à l'article 6 qu'il détient [...] connaît bien le contexte lié à l'entité et dispose donc d'un droit de lecture » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 44-45). L'article 18 de la loi attaquée précise que les services partenaires qui bénéficient d'un droit de lecture et d'un droit d'écriture « sont tenus respectivement de consulter la banque de données commune T.E.R. et d'y introduire d'office leurs propres données à caractère personnel et les informations pertinentes. Ces données à caractère personnel et informations sont enregistrées dans la banque de données commune T.E.R., sous leur responsabilité et suivant leurs procédures internes de validation ».

B.17.4. L'article 16, alinéa 2, de la loi attaquée habilite le Roi à déterminer, « par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle », pour chaque service partenaire autre que le ministère public, « le type de droit et ses modalités d'exercice ». L'article 16, alinéa 3, de la loi attaquée habilite le Roi à déterminer, « par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle et avis conforme du Collège des procureurs généraux », « le type de droit et ses modalités d'exercice » dont bénéficie le ministère public.

B.17.5. Compte tenu de cette nouvelle réglementation en matière de droits d'accès à la banque de données commune T.E.R. des services partenaires, le législateur a abrogé, par l'article 55, 3°, de la loi attaquée, l'article 44/11/3^{ter}, § 2, de la loi sur la fonction de police, qui prévoyait des droits d'accès pour les services partenaires et une habilitation du Roi analogues (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 107-108).

B.18. Comme il est dit en B.9.1, l'article 22 de la Constitution garantit à tout citoyen qu'il ne peut y avoir ingérence dans l'exercice du droit au respect de la vie privée qu'en vertu de règles adoptées par une assemblée délibérante démocratiquement élue, même si une délégation octroyée à un autre pouvoir reste possible, pour autant que l'habilitation soit définie en des termes suffisamment précis et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été préalablement fixés par le législateur.

La Cour européenne des droits de l'homme n'a pas jugé que le traitement des données à caractère personnel et l'accès aux données traitées doivent être réglés par le pouvoir législatif. Elle a seulement souligné que ce traitement et cet accès doivent trouver une base claire, accessible et prévisible en droit interne (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, précité, §§ 47-63).

La Cour de justice exige elle aussi seulement que « la base légale qui permet l'ingérence dans [le droit au respect de la vie privée définit] elle-même la portée de la limitation de l'exercice du droit concerné » (CJUE, grande chambre, 6 octobre 2020, C-623/17, *Privacy*

International, précité, point 65). Elle n'exige pas que tous les aspects de cette limitation soient réglés par une loi formelle.

B.19.1. Il ressort des termes de l'article 16, alinéa 1er, de la loi attaquée que l'habilitation conférée au Roi par les alinéas 2 et 3 de la même disposition pour déterminer « le type de droit » des services partenaires implique uniquement qu'Il doit établir si le service partenaire concerné dispose soit d'un « droit de lecture et d'un droit d'écriture » soit d'un « droit d'interrogation ».

Le choix de déléguer au Roi le pouvoir de déterminer le type de droit d'accès à la banque de données commune T.E.R. dont bénéficie chaque service partenaire parmi les deux types de droits d'accès visés à l'article 16, alinéa 1er, de la loi attaquée a été justifié par la nécessité de conserver une flexibilité « dans l'octroi, le retrait ou la modification de l'accès en fonction de l'évolution des compétences, des missions et des besoins des différents services partenaires » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 108). À propos du droit d'interrogation, les travaux préparatoires précisent par ailleurs que ce droit est donné « aux services de l'État qui sont susceptibles de rentrer en contact avec une personne T.E.R., et qui en l'absence de la qualité T.E.R. de la personne, peuvent lui délivrer des documents administratifs lui permettant de s'établir en Belgique, d'exercer une profession rémunérée. Mais ceux-ci ne gèrent pas d'informations visées à l'article 6 du projet de loi et ne doivent donc pas alimenter la banque de données commune T.E.R. » (*ibid.*, p. 45).

B.19.2. Le législateur a déterminé lui-même les types de droits d'accès susceptibles d'être accordés aux services partenaires (article 16, alinéa 1er, *juncto* l'article 2, 19° à 21°), les catégories de données auxquelles les services partenaires ont accès (article 6, § 2), les catégories de personnes dont les données sont traitées (article 6, § 2, 1° et 2°, *juncto* l'article 2, 4°, 7° à 11°), les catégories de personnes ayant accès aux données traitées (articles 2, 3°, 6, § 2, 3°, et 16, alinéa 1er) et les finalités du traitement (article 5, alinéa 2). L'article 16, alinéa 1er, de la loi attaquée précise à cet égard que les services partenaires disposent d'un ou l'autre types de droit d'accès visés en B.19.1 « sur la base du respect des principes d'adéquation, de pertinence et du caractère non excessif, dans le cadre de l'exercice de leurs missions visées à l'article 3, et

conformément aux finalités de l'article 5, alinéa 2 » et « chacun dans le cadre de ses compétences respectives ».

En outre, le législateur a assorti l'exercice des droits d'accès accordés aux services partenaires de mesures de contrôle. Premièrement, les traitements effectués dans la banque de données commune, tels que l'enregistrement et la consultation des données, font l'objet d'une « journalisation ». Les fichiers de journalisation permettent d'établir, entre autres, « le motif, la date et l'heure de ces traitements » et « les catégories de personnes qui ont consulté les données à caractère personnel, ainsi que l'identification ou le code d'identification de la personne ou du service qui a consulté ces données » (article 8). Deuxièmement, la police fédérale a pour mission, en tant que gestionnaire de la banque de données commune, de tenir la liste des personnes ou codes d'identification des personnes ou des services ayant accès à la banque de données et de veiller à la journalisation des traitements réalisés dans celle-ci (article 11, alinéa 2, 7° et 8°). Troisièmement, l'OCAM veille, en tant que responsable opérationnel de la banque de données commune, à la qualité et à la pertinence des données traitées au regard des finalités du traitement et à organiser une collaboration adéquate entre le gestionnaire, les services de base et les services partenaires (article 12, 1°, 3° et 6°). Quatrièmement, le service partenaire qui dispose d'un droit d'interrogation de la banque de données commune est tenu de prendre directement contact avec l'un des services de base en vue de contextualiser l'information disponible relative à l'évaluation de la menace d'une entité validée (article 22, alinéa 2). Cinquièmement, le responsable du traitement du service partenaire est responsable de la qualité des données à caractère personnel et informations transmises par ce service et de la légalité de ces transmissions (article 30, § 1er, 1°, et § 2). Sixièmement, les traitements effectués dans la banque de données commune sont soumis au contrôle de l'Organe de contrôle de l'information policière et du Comité permanent R (article 29 *juncto* l'article 2, 22°; article 161, alinéa 2, de la loi sur la protection des données, tel qu'il a été inséré par l'article 46 de la loi attaquée). Ces autorités de contrôle disposent d'un droit de lecture de la banque de données commune dans le cadre de l'exercice de leurs missions (article 15).

B.19.3. Le législateur a ainsi habilité le Roi en des termes suffisamment précis et il a fixé les éléments essentiels des droits d'accès des services partenaires à la banque de données commune T.E.R.

Étant donné la diversité des compétences, missions et besoins des services partenaires visés à l'article 2, 3°, de la loi attaquée et leur caractère technique et évolutif, il n'est pas dénué de justification raisonnable que le Roi soit habilité à déterminer la nature du droit d'accès à la banque de données commune T.E.R. dont chaque service partenaire bénéficie, dans le respect des éléments essentiels contenus dans les dispositions de la loi attaquée mentionnées en B.19.2.

Le cas échéant, il appartient au juge compétent d'examiner si l'utilisation, faite par le Roi, des habilitations visées à l'article 16 de la loi attaquée est conforme à cette dernière disposition et aux dispositions constitutionnelles et conventionnelles invoquées au premier moyen.

B.20. Le grief n'est pas fondé.

4. En ce qui concerne les services susceptibles d'être invités par la « Task force locale » (article 32, § 1er, alinéa 4, de la loi attaquée)

B.21. Les parties requérantes allèguent que les services susceptibles d'être invités par le président de la « Task force locale » en vertu de l'article 32, § 1er, alinéa 4, de la loi attaquée ne sont pas identifiables.

B.22.1. L'article 31 de la loi attaquée dispose :

« En vue d'assurer l'enrichissement des données à caractère personnel et informations relatives aux entités validées et aux entités en pré-enquêtes enregistrées dans la banque de données commune T.E.R. ainsi que le suivi et la prise de mesures à l'égard des entités validées dans la banque de données commune T.E.R., des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. ainsi que d'autres données à caractère personnel et informations pertinentes, y compris les informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé, sont échangées au sein d'une ou plusieurs plateformes de concertation créées auprès de chaque arrondissement judiciaire, appelée Task force locale, dénommée ci-après ' TFL ', sauf si cet échange peut compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes.

La TFL est une structure de concertation au sens de l'article 458^{ter} du Code pénal ».

L'article 32 dispose :

« 1er. La TFL est présidée par le directeur coordinateur administratif de la police fédérale ou son représentant.

Outre le président, la TFL se compose de représentants:

- 1° des services de renseignements et de sécurité;
- 2° de l'Organe de coordination pour l'analyse de la menace;
- 3° de la police fédérale et de la police locale;
- 4° de la Direction générale de l'Office des Étrangers du Service public fédéral Intérieur;
- 5° du ministère public.

Le président et les participants à la TFL visés à l'alinéa 2, 1° à 4°, sont titulaires d'une habilitation de sécurité au moins du niveau 'secret' en vertu des articles 4, alinéa 3, et 8 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé.

Le président, en concertation avec les participants à la TFL visés à l'alinéa 2, 1° à 5°, peut inviter d'autres services, organes ou instances en raison de la contribution qu'ils peuvent apporter par leur fonction ou leurs compétences à un suivi ciblé et individualisé de l'entité.

Les services partenaires visés à l'article 2, 3°, 1), seront représentés par un membre de l'administration centrale titulaire d'une habilitation de sécurité.

La coordination administrative, le secrétariat et le suivi de la TFL sont assurés par le directeur coordinateur ou les personnes qu'il désigne.

§ 2. Sans préjudice des compétences des services de base et des services partenaires, la [TFL] assure au moins les missions suivantes :

1° l'échange des données à caractère personnel et des informations visé [...] à l'article 31 dans le cadre des missions visées à l'article 3;

2° le suivi des entités de la banque de données commune T.E.R. présentes sur son territoire;

3° la détermination de mesures appropriées pour chacune des entités validées ».

B.22.2. L'article 31, alinéa 1er, de la loi attaquée dispose qu'une ou plusieurs « Task forces locales » sont créées auprès de chaque arrondissement judiciaire. Il détermine les finalités de l'échange de données et d'informations qui intervient au sein des « Task forces locales » (« assurer l'enrichissement des données à caractère personnel et informations relatives aux entités validées et aux entités en pré-enquêtes enregistrées dans la banque de données commune T.E.R. ainsi que le suivi et la prise de mesures à l'égard des entités validées dans la banque de données commune T.E.R. ») ainsi que les catégories de données visées par cet échange (les « données à caractère personnel et [l]es informations enregistrées dans la banque de données commune T.E.R. ainsi que [les] autres données à caractère personnel et informations pertinentes, y compris les informations classifiées »). L'article 31, alinéa 2, dispose que la « Task force locale » est une structure de concertation au sens de l'article 458^{ter} du Code pénal.

L'article 32, § 1er, de la loi attaquée prévoit que la « Task force locale » est composée du directeur coordinateur administratif de la police fédérale ou son représentant - qui en est le président - ainsi que de représentants des services de renseignement et de sécurité, de l'OCAM, de la police fédérale et de la police locale, de la direction générale de l'Office des étrangers du Service public fédéral Intérieur et du ministère public. L'alinéa 4 du même paragraphe dispose que le président, en concertation avec les autres membres précités de la « Task force locale », peut inviter « d'autres services, organes ou instances en raison de la contribution qu'ils peuvent apporter par leur fonction ou leurs compétences à un suivi ciblé et individualisé de l'entité ».

B.22.3. Les « Task forces locales » sont « des plateformes de concertation qui rassemblent l'ensemble des acteurs associés à la stratégie T.E.R. » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/002, p. 5). Contrairement aux cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme (CSIL-R) créées par la loi du 30 juillet 2018 « portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme » qui travaillent « au niveau de la prévention sociale », les « Task forces locales » constituent un « réseau permanent établi dans une optique sécuritaire » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 133, 134 et 137).

Les « Task forces locales » ont pour objectif « d'avoir une mise en commun d'informations et d'en discuter. Ensuite, chaque service, sur base de ses propres règles, prend les mesures qu'il

estime nécessaire[s] » (*ibid.*, p. 134). Il s'agit, d'une part, de « contextualiser » des données relatives à une entité et, d'autre part, de « mettre à jour des données et des informations déjà enregistrées dans la banque de données commune T.E.R. et/ou d'apporter des nouveaux éléments » :

« La contextualisation des données et informations est importante dans la mesure où la banque de données commune T.E.R. ne contient pas toutes les informations disponibles des services de base ou des services partenaires sur les entités (la banque de données commune T.E.R. ne reprend pas, par exemple, le contenu *in extenso* des procès-verbaux). Elle permet donc de donner tout le contexte relatif à la donnée enregistrée dans la banque de données commune T.E.R. (personne, véhicule,...). Par ailleurs, lors de la TFL, et de la discussion avec les différents services présents, il peut ressortir qu'il y ait des nouvelles données ou informations à enregistrer dans la banque de données commune T.E.R. et qu'il faille donc l'« enrichir » ou qu'il soit nécessaire de mettre des données ou de l'information déjà enregistrées à jour » (*ibid.*).

Au sein des « Task forces locales », sont échangées « non seulement les données à caractère personnel et les informations non classifiées contenues dans la banque de données commune T.E.R. mais également d'autres données à caractère personnel ou informations considérées comme pertinentes, y compris les classifiées et celles qui proviennent de services qui ne sont pas tenus d'alimenter la banque de données commune T.E.R. » :

« Il ne serait en effet pas concevable que pour ce phénomène particulièrement sérieux ce type d'informations ne soient pas échangées loyalement entre les services concernés. Toutefois, tant que ces informations sont classifiées ou confidentielles, elles ne pourront être mentionnées dans le rapportage des task force[s] locales. Maintenant, lorsqu'une donnée ou information classifiée ou confidentielle est intéressante à enregistrer dans la banque de données commune T.E.R., rien n'empêche le service propriétaire de la donnée ou information concernée de réévaluer la nécessité de maintenir la protection et de procéder, le cas échéant, à une déclassification.

Comme souligné par le Conseil d'État dans son avis n° 73.442/2 du 7 juin 2023, cet article ne peut pas être interprété « comme permettant l'enregistrement dans la banque de données commune T.E.R. de données ou d'informations classifiées, celles-ci pouvant tout au plus faire l'objet d'échanges lors des réunions de la Task force locale. ».

Les services sont tenus de n'échanger que les données à caractère personnel et les informations qu'ils ont le droit de traiter dans le cadre de leurs missions » (*ibid.*, pp. 134-135).

La majorité des traitements qui ont lieu lors de la concertation au sein de la « Task Force locale » sont régis par les règles applicables à la banque de données commune T.E.R. Les

traitements de données relatives à des entités non encore enregistrées dans cette banque de données se font sous la responsabilité des services qui sont en possession de ces données. « Ainsi par exemple, le président de la TFL, à savoir le directeur coordinateur administratif de la police fédérale, lorsqu'il prépare sa réunion doit gérer les données qu'il va traiter durant cette préparation selon les règles de la loi sur la fonction de police. Il en va de même pour les autres organisations qui devront respecter leurs propres législations » (*ibid.*, p. 133).

Le fait que la « Task force locale » constitue une structure de concertation au sens de l'article 458^{ter} du Code pénal a pour conséquence que le dépositaire du secret professionnel qui participe à la « Task force locale » peut, dans le cadre de celle-ci, révéler des informations couvertes par le secret sans risquer d'être poursuivi pour violation du secret professionnel.

B.22.4. À propos de la possibilité d'inviter d'« autres services, organes ou instances », prévue à l'article 32, § 1er, alinéa 4, de la loi attaquée, l'Autorité de protection des données a demandé au législateur de détailler les critères permettant de garantir à une personne concernée que le traitement de ses données est nécessaire et proportionné à sa finalité (avis n° 97/2023 du 16 juin 2023, § 91). Le Comité permanent R a recommandé de mieux définir les catégories de « services, organes ou instances » concernés (avis n° 004/CPR/2023 du 13 juillet 2023, § 31).

À la suite de ces avis, les travaux préparatoires précisent :

« Afin que la TFL puisse travailler de manière optimale et lorsque cela s'avère nécessaire pour le suivi ciblé d'une entité, le président peut inviter d'autres services, organes ou instances en raison de leurs compétences ou fonctions à participer à la TFL et ce, le temps strictement nécessaire à la contribution qu'ils peuvent apporter à la TFL. Ces services, organes ou instances sont invités pour fournir des données, éclairer un point précis de leur expertise. Ainsi, comme précisé par le Conseil d'État dans son avis 73.442/2 du 7 juin 2023, et en réponse aux remarques de l'Autorité de protection des données dans son avis 97/2023 du 16 juin 2023 (§§ 45-46 et 91) et du Comité R dans son avis du 13 juillet 2023 (§ 31), ' l'article 32, § 1er, alinéa 4, en projet doit être interprété comme permettant aux " autres services, organes ou instances " invités à participer aux réunions de la Task force locale de communiquer des données ou des informations dont ils seraient détenteurs en raison de leur mission en vue d'enrichir les données ou informations contenues dans la banque de données. Ils ne pourraient en revanche se voir communiquer des données ou informations dont les autres membres de la Task force locale seraient détenteurs '. Très concrètement, un expert sera présent uniquement durant ' son point ' »

et quittera ensuite la réunion après son exposé. En outre, une concertation entre le président et les participants à la TFL permettra de n'inviter que des services, organes ou instances fiables. La concertation devrait aussi évaluer si lors de l'échange, il est nécessaire de communiquer des informations sensibles ou classifiées auquel cas une habilitation sera nécessaire. À noter que pour les services partenaires visés à l'article 2, 3°, 1), une habilitation de sécurité sera toujours nécessaire. Dans son avis du 13 juillet 2023, le Comité R demande de mieux définir quelles catégories de 'services, organes ou instances' peuvent être invitées à une T.F.L. (§ 31). Comme cela est indiqué dans le dispositif, il s'agit d'invite[r] ceux qui peuvent apporter leur expertise dans le cadre du suivi d'une entité déterminée. Le but est d'être le plus large possible. Le critère déterminant est l'apport que peut avoir une personne ou un service pour le cas examiné en T.F.L. » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 138-139).

B.22.5. Il ressort des termes des articles 31 et 32, § 1er, alinéa 4, de la loi attaquée et des travaux préparatoires précités que les « services, organes ou instances » susceptibles d'être invités à participer à la « Task force locale » « le temps strictement nécessaire à la contribution qu'ils peuvent apporter » sont tous les services, organes ou instances qui disposent d'une expertise pertinente « par leur fonction ou leurs compétences », en vue d'enrichir les données et informations contenues dans la banque de données commune T.E.R. et de permettre le suivi « ciblé et individualisé » et la prise de mesures à l'égard de l'entité concernée. Ces derniers objectifs sont les finalités de la communication des données et informations détenues par les services invités à la « Task force locale ».

La compétence, confiée au président de la « Task force locale », de déterminer, en concertation avec les autres participants de celle-ci, les services, organes ou instances qu'il invite à la « Task force locale », est raisonnablement justifiée, eu égard à la nécessité de tenir compte de la diversité des situations locales.

Les travaux préparatoires précités confirment par ailleurs que l'article 32, § 1er, alinéa 4, de la loi attaquée doit être compris dans l'interprétation, précitée, que lui donne la section de législation du Conseil d'État, selon laquelle « les autres services, organes ou instances » invités à participer à la « Task force locale » en vertu de cette disposition peuvent communiquer des données ou des informations dont ils sont détenteurs en raison de leur mission en vue d'enrichir les données ou informations contenues dans la banque de données, mais ne peuvent en revanche se voir communiquer des données ou informations dont les autres membres de la « Task force locale » sont détenteurs (*ibid.*, p. 221).

B.23. Compte tenu de ce qui est dit en B.22.5, le grief n'est pas fondé.

5. En ce qui concerne les mesures visées à l'article 33, § 2, 7° et 8°, de la loi attaquée

B.24. Les parties requérantes font valoir que l'article 33, § 2, 7° et 8°, de la loi attaquée n'est pas suffisamment précis.

B.25.1. L'article 33 de la loi attaquée dispose :

« § 1er. Dès la validation d'une entité dans la banque de données commune T.E.R., sur la base des données à caractère personnel et des informations visées à l'article 31, la TFL, afin d'assurer le suivi de l'entité validée, se concerte systématiquement sur l'opportunité de prendre ou non une ou plusieurs mesures visées au paragraphe 2 à l'égard de l'entité validée, sans préjudice des prérogatives des autorités compétentes pour prendre ces mesures.

Dans le cadre du suivi d'une entité validée, lorsque des nouvelles données à caractère personnel et informations visées à l'article 31 peuvent entraîner un changement de mesures à son égard, la TFL procède à la concertation visée à l'alinéa premier.

En vue de l'élaboration de l'approche proactive, le résultat de la concertation visée aux alinéas 1 et 2 est transmis aux autorités compétentes pour prendre les éventuelles mesures à l'égard d'une entité validée dans la banque de données commune T.E.R. Le résultat de la concertation visée aux alinéas 1 et 2 relative à une entité validée est également enregistré dans la banque de données commune T.E.R. sauf si la mesure peut compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes ou qu'elle est classifiée au sens de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé.

Sans préjudice de leurs prérogatives, les autorités compétentes pour prendre les mesures à l'égard d'une entité validée dans la banque de données commune prennent en considération le résultat de la concertation visée aux alinéas 1 et 2 lors de leur prise de décision.

§ 2. La TFL se concerte notamment sur les mesures suivantes, sauf si elles peuvent compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes :

[...]

7° la prise de mesures spécifiques dans les limites des compétences légales des services de l'Office National de l'Emploi (ONEm), l'Office wallon de la formation professionnelle et de l'emploi (FOREm), l'Office régional bruxellois de l'Emploi (Actiris), Bruxelles formation, le *Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (VDAB)* et l'*Arbeitsamt der Deutschsprachigen Gemeinschaft Belgiens (ADG)*;

8° la prise de mesures spécifiques par l'Office des Étrangers en matière d'accès au territoire, de séjour, d'établissement et d'éloignement;

[...] ».

B.25.2. L'article 33, § 1er, de la loi attaquée prévoit que la « Task force locale » se concerta à deux moments afin d'assurer le suivi d'une entité validée : d'une part, « dès la validation d'une entité dans la banque de données commune et sur base des données à caractère personnel et des informations visées à l'article 31 » (alinéa 1er) et, d'autre part, « dans le cadre du suivi d'une entité validée, lorsque de nouvelles données à caractère personnel et informations visées à l'article 31 peuvent entraîner un changement de mesures » (alinéa 2) (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 141).

La concertation porte sur « l'opportunité de prendre ou non une ou plusieurs mesures visées au paragraphe 2 » à l'égard de l'entité validée, « sans préjudice des prérogatives des autorités compétentes pour prendre ces mesures » (alinéa 1er).

Le résultat de la concertation est transmis aux autorités compétentes pour qu'elles prennent les éventuelles mesures en question. Il est également enregistré dans la banque de données commune T.E.R., sauf si la mesure peut compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes ou qu'elle est classifiée au sens de la loi du 11 décembre 1998 (alinéa 3; *Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 133 et 141). Enfin, les autorités compétentes en tiennent compte lorsqu'elles prennent les mesures concernées « sans préjudice de leurs prérogatives » (alinéa 4).

L'article 33, § 2, de la loi attaquée énonce une liste « non exhaustive » des mesures qui doivent faire l'objet d'une concertation au sein de la « Task force locale » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 142). Parmi ces mesures, figurent « 7° la prise de mesures spécifiques dans les limites des compétences légales des services de l'Office National de

l'Emploi (ONEm), l'Office wallon de la formation professionnelle et de l'emploi (FOREm), l'Office régional bruxellois de l'Emploi (Actiris), Bruxelles formation, le « Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (VDAB) » et l'« Arbeitsamt der Deutschsprachigen Gemeinschaft Belgiens (ADG) » et « 8° la prise de mesures spécifiques par l'Office des Étrangers en matière d'accès au territoire, de séjour, d'établissement et d'éloignement ».

À propos des mesures susceptibles d'être prises par l'Office des étrangers, les travaux préparatoires mentionnent que « pour chaque entité enregistrée dans la banque de données commune T.E.R., l'Office des étrangers procède à une analyse afin de prendre les mesures adéquates. Par exemple, en ce qui concerne l'accès au territoire, la demande de visa peut être examinée. En ce qui concerne le séjour, c'est le dossier individuel qui peut être examiné » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 144).

B.25.3. À la suite de l'avis n° 97/2023, précité, de l'Autorité de protection des données (§ 90) et de l'avis n° 004/CPR/2023 du Comité permanent R (§§ 32-33), le législateur a précisé dans les travaux préparatoires que la concertation organisée à l'article 33 ne constitue pas une procédure d'avis préalable obligatoire qui conditionnerait l'exercice, par les autorités compétentes concernées, de leurs compétences. Celles-ci les conservent « à tout moment » et ne sont pas tenues d'attendre « qu'une [« Task force locale »] se soit réunie pour prendre une mesure qu'[elles] estime[nt] nécessaire ». Le résultat de la concertation est uniquement un élément « non contraignant » parmi d'autres qui est mis à la disposition de ces autorités (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 141-142).

B.25.4. Il s'ensuit que la disposition attaquée porte uniquement sur la concertation menée au sein de la « Task force locale » quant à l'opportunité de prendre ou non des mesures qui relèvent des compétences des autorités visées au paragraphe 2. Si ces autorités sont tenues de prendre en considération le résultat de cette concertation lors de leur prise de décision (article 33, § 1er, alinéa 4, de la loi attaquée), elles sont libres de s'écarter du résultat de la concertation, comme elles sont libres de prendre des mesures qui n'ont pas fait l'objet d'une concertation préalable au sein de la « Task force locale ».

B.25.5. Pour le reste, l'article 33, § 2, 7° et 8°, de la loi attaquée n'a pas pour conséquence que les autorités visées puissent prendre des mesures pour lesquelles elles ne sont pas compétentes conformément à la réglementation qui leur est applicable, ainsi qu'en attestent également les précisions selon lesquelles la concertation au sein de la « Task force locale » porte sur des mesures spécifiques « dans les limites des compétences légales » des services concernés (7°) ou, en ce qui concerne l'Office des étrangers, « en matière d'accès au territoire, de séjour, d'établissement et d'éloignement » (8°). Contrairement à ce que soutiennent les parties requérantes, l'absence d'une définition plus précise de ces mesures et/ou d'un renvoi explicite à la réglementation fixant les compétences des services concernés ne permet pas de conclure que cette disposition n'est pas suffisamment claire.

Le cas échéant, il appartient au juge compétent d'examiner si les décisions prises par ces autorités à l'égard d'une entité à la suite de la concertation prévue à l'article 33 de la loi attaquée sont conformes aux dispositions légales qui fondent ces décisions et aux dispositions constitutionnelles et conventionnelles invoquées au premier moyen.

B.26. Le grief n'est pas fondé.

6. En ce qui concerne les destinataires de la « carte d'information » (articles 23 et 26 de la loi attaquée)

B.27. Les parties requérantes font grief aux articles 23 et 26 de la loi attaquée de ne pas contenir une liste exhaustive des destinataires de la « carte d'information ».

B.28.1. L'article 2, 17°, de la loi attaquée définit la « carte d'information » comme étant la « fiche d'une entité qui consiste en un extrait de la fiche de renseignements, contenant les données à caractère personnel et informations adéquates, pertinentes et non excessives au destinataire, pour le suivi des entités validées ».

L'article 2, 16°, de la loi attaquée définit la « fiche de renseignement » comme étant la « fiche qui contient l'ensemble des données à caractère personnel et des informations relatives à une entité de la banque de données commune T.E.R. provenant de l'ensemble des services qui l'alimentent ».

L'article 23 de la loi attaquée dispose :

« Aux fins de renforcer la prévention et la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme, dans les limites visées à l'alinéa 2 et à l'article 24, une carte d'information peut être communiquée à une autorité ou une institution tierce dans le respect des principes d'adéquation, de pertinence et du caractère non excessif, et après évaluation par le gestionnaire, le responsable opérationnel et les services de base, sauf décision contraire du ministère public compétent lorsque la communication des données à [caractère] personnel et des informations judiciaires peut compromettre l'exercice de l'action publique ou la sécurité de personnes.

L'évaluation visée à l'alinéa 1er porte au minimum sur :

1° la contribution de l'autorité ou de l'institution tierce à la prévention et à la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme;

2° le traitement ultérieur qui sera réalisé par l'autorité ou l'institution tierce eu égard à l'exercice de ses compétences et les risques éventuels pour les libertés et droits fondamentaux de la personne concernée;

3° la situation de vulnérabilité de la personne concernée, en ce compris la minorité de la personne;

4° le caractère adéquat, pertinent et non excessif des catégories de données communiquées tenant compte du traitement ultérieur.

Le responsable opérationnel tient à la disposition des autorités de contrôle une liste actuelle des communications visées à l'alinéa 1er et l'évaluation visée à l'alinéa 2 ».

L'article 24 dispose :

« § 1er. La communication visée à l'article 23 s'effectue par la transmission, par quelque moyen sécurisé que ce soit, de la carte d'information relative aux entités validées.

Seuls les services de base sont autorisés à transmettre la carte d'information, sans préjudice des règles et procédures applicables pour leurs propres données à caractère personnel et informations.

§ 2. Les informations émanant de la carte d'information sont utilisées par le destinataire dans le cadre de ses propres compétences légales, sans que la carte d'information ne soit ni versée au dossier de l'entité validée ni communiquée à celle-ci ».

L'article 25 dispose :

« Seuls les services qui ont un droit de lecture et un droit d'écriture dans la banque de données commune T.E.R. sont autorisés à en extraire des listes de données à caractère personnel et d'informations de la carte d'information relative aux entités validées et ce, exclusivement pour un traitement interne. Cette extraction est effectuée par un membre du personnel titulaire d'une habilitation de sécurité ' secret '.

La communication par un service de base, sous forme de listes, de données à caractère personnel ou d'informations extraites des cartes d'information à d'autres services ou institutions n'est pas autorisée, sauf dans les cas visés à l'article 23. Les listes ne peuvent être communiquées qu'aux autorités publiques et services publics. La finalité de la liste s'inscrit dans les missions légales du destinataire et est précisée et communiquée au destinataire de celle-ci. L'utilisation de la liste n'est autorisée que dans le cadre de la finalité précisée. Les listes ne peuvent pas être conservées pour une durée excédant celle nécessaire à la réalisation de la finalité pour laquelle elles sont obtenues ».

L'article 26 dispose :

« § 1er. Le bourgmestre est destinataire de la carte d'information relative aux entités validées suivantes :

1° les *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents et les personnes condamnées pour terrorisme, qui ont établi leur résidence ou domicile dans sa commune, la fréquentent régulièrement ou y organisent régulièrement des activités;

2° les propagandistes de haine dont les effets sont perceptibles dans sa commune ou qui ont établi leur résidence ou leur domicile dans sa commune, la fréquentent régulièrement, y organisent ou y planifient d'organiser une ou plusieurs activités.

§ 2. Sans mettre en péril les impératifs opérationnels, le bourgmestre utilise, après un contact avec le chef de corps de la zone de police qui lui a transmis la carte d'information, les données à caractère personnel et informations émanant de celle-ci dans le cadre de ses compétences légales et sous sa propre responsabilité ».

B.28.2. L'article 20 de la loi attaquée dispose que la « fiche de renseignements » qui contient l'ensemble des données à caractère personnel et des informations relatives à une entité de la banque de données commune T.E.R (article 2, 16°, de la même loi) est uniquement accessible aux services qui ont un droit de lecture et un droit d'écriture dans la banque de données commune T.E.R. et qu'elle ne peut pas être communiquée à d'autres services ou institutions, à l'exception des autorités de contrôle dans le cadre de leurs missions. En vertu de l'article 21, la création d'une nouvelle entité dans la banque de données commune T.E.R. est immédiatement communiquée au président de la « Task force locale » et au chef de corps de chaque zone de police concernée, lequel informe lui-même « les autorités de police

administrative compétentes », notamment le bourgmestre (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 125). En vertu de l'article 22, les services partenaires qui disposent d'un droit d'interrogation de la banque de données T.E.R. reçoivent une évaluation de la menace en cas de confirmation de l'existence d'une entité validée dans la banque de données.

B.28.3. L'article 23, alinéa 1er, de la loi attaquée prévoit qu'un extrait de la fiche de renseignements contenant les données à caractère personnel et informations adéquates, pertinentes et non excessives pour le suivi des entités validées, dit « carte d'information » (voy. article 2, 17°, de la même loi), peut être communiqué, sauf décision contraire du ministère public, à des destinataires autres que ceux visés aux articles 20 à 22 de la loi attaquée (« une autorité ou une institution tierce »), moyennant le respect de deux conditions : (1) d'une part, cette communication doit respecter les principes d'adéquation, de pertinence et du caractère non excessif et (2) d'autre part, elle doit avoir fait l'objet d'une évaluation préalable par le gestionnaire, le responsable opérationnel et les services de base (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 118-119). L'article 23, alinéa 2, précise l'objet de cette évaluation (*ibid.*, p. 120). L'article 23, alinéa 3, dispose que le responsable opérationnel tient à la disposition des autorités de contrôle une liste actuelle des communications de la carte d'information et de l'évaluation précitées. L'article 24 prévoit que la communication de la carte d'information se fait par un moyen sécurisé (§ 1er, alinéa 1er), que seuls les services de base peuvent transmettre la carte d'information (§ 1er, alinéa 2) et que le destinataire de la carte d'information utilise les informations contenues dans celle-ci « dans le cadre de ses propres compétences légales » et « sans que la carte d'information ne soit ni versée au dossier de l'entité validée ni communiquée à celle-ci » (§ 2).

La carte d'information est destinée « aux autorités susceptibles de prendre des mesures à l'égard des entités validées de la banque de données commune T.E.R., dans le but d'éviter la prise de mesures incohérentes entre elles » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 121). Elle a pour but « d'éviter que l'autorité administrative ne prenne des mesures contradictoires par rapport à celles qui ont été discutée[s] en [Task force locale] » (*ibid.*).

Les travaux préparatoires, pour illustrer l'application de l'article 23 de la loi attaquée, donnent l'exemple suivant :

« [II] se peut qu'un des services qui bénéficie d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R. estime qu'il est nécessaire de fournir tout ou partie des données à caractère personnel à une ASBL ou à une école afin de prévenir un départ d'un jeune en décrochage social vers la Syrie. Dans ce cas, les services qui sont à la base des informations doivent évaluer préalablement à cette communication si celle-ci est bénéfique à tout le monde ainsi que les conditions relatives à cette communication, sur la base des modalités déterminées à l'article 24 » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 119).

Les travaux préparatoires précisent que « chaque destinataire [de la carte d'information] agit dans le cadre de ses compétences et de ses finalités et traite les données selon ses objectifs sans pour autant devenir [un] acteu[r] en matière de terrorisme, extrémisme et processus de radicalisation » (*ibid.*).

En outre, l'article 24, § 2, de la loi attaquée rappelle « le principe général selon lequel aucun destinataire d'une carte d'information ne peut verser celle-ci dans un dossier sur base duquel une décision administrative est prise concernant la personne visée. En effet, il faut éviter que les données et informations de ce document ne [soient] divulguées à des personnes ou organismes au sens large ayant accès au dossier et qui ne sont pas directement liés à la lutte contre le terrorisme et que le mécanisme de protection des données gérées au sein de la banque de données commune T.E.R. ne puisse être contourné par une procédure administrative » (*ibid.*, p. 122). « La carte d'information contient les mesures de suivi qui ne doivent pas être connues de l'entité validée concernée (ex. enquête judiciaire ou de renseignement, surveillance discrète) au risque d'entraver une enquête. Outre les mesures de suivi, la carte d'information peut également contenir des informations qu'il n'est pas pertinent de communiquer à l'entité validée concernée. Exemples: les services intéressés dans le suivi de la personne (ex. la PJF d'Anvers), la date du début du suivi » (*ibid.*, p. 121). « Ce qui sert à la motivation de la décision de l'autorité administrative, c'est l'évaluation de la menace qui, elle, peut être versée au dossier de l'entité (art. 27) » (*ibid.*).

B.28.4. L'article 25, alinéa 2, première phrase, de la loi attaquée prévoit que « la communication par un service de base, sous forme de listes, de données à caractère personnel ou d'informations à d'autres services ou institutions n'est pas autorisée, sauf dans les cas prévus à l'article 23 ».

Il ressort de cette disposition, ainsi que le confirment d'ailleurs les travaux préparatoires précités, que l'interdiction de communiquer des données à caractère personnel et des informations extraites des cartes d'information à des services qui n'ont pas de droit de lecture ni de droit d'écriture ne souffre qu'une exception, lorsque « le gestionnaire, le responsable opérationnel et les services de base estiment que la communication est nécessaire pour une finalité précise dont est chargé le destinataire en question. En effet, la communication ne peut être effectuée qu'avec une finalité déterminée qui s'inscrit dans le cadre des missions légales du destinataire en question (par exemple, pour la mise à jour de la banque de données que gère le Ministère public une liste des nouvelles entités et des entités supprimées est adressée aux magistrats spécialisés) » (*ibid.*, p. 123). Seuls les services qui ont un droit de lecture et un droit d'écriture dans la banque de données commune T.E.R. sont autorisés à en extraire des listes de données à caractère personnel et d'informations depuis la carte d'information, et ce, exclusivement à des fins de traitement interne. Cette extraction est effectuée par un membre du personnel titulaire d'une habilitation de sécurité du niveau « secret » (article 25, alinéa 1er). Les listes ne peuvent être communiquées qu'aux autorités et services publics. La finalité de la liste doit s'inscrire dans les missions légales du destinataire et doit être précisée et communiquée à celui-ci. L'utilisation de la liste n'est autorisée que dans le cadre de la finalité précisée et les listes ne peuvent pas être conservées pour une durée excédant celle qui est nécessaire à la réalisation de la finalité pour laquelle elles sont obtenues (article 25, alinéa 2, deuxième à quatrième phrases).

B.28.5. Enfin, l'article 26, § 1er, de la loi attaquée prévoit que les cartes d'information relatives aux entités validées mentionnées dans cette disposition sont communiquées au bourgmestre. En vertu de l'article 26, § 2, le bourgmestre utilise les données à caractère personnel et informations émanant de la carte d'information, après avoir pris contact avec le chef de corps de la zone de police qui la lui a transmise, « dans le cadre de ses compétences légales », « sous sa propre responsabilité » et « sans mettre en péril les impératifs opérationnels ».

Les travaux préparatoires indiquent :

« Vu les compétences du bourgmestre en matière de sécurité telles que légalement définies dans la nouvelle loi communale, celui-ci doit disposer des informations nécessaires afin d'exercer son rôle dans le domaine de la prévention en matière de terrorisme. En tant qu'autorité

en matière de police administrative, il doit également être tenu au courant du suivi concret de certaines entités validées liées à sa commune.

Le bourgmestre devra donc être informé lorsqu'une entité validée, dont les activités ont des effets perceptibles dans sa commune ou qui a établi sa résidence ou son domicile dans sa commune, la fréquente régulièrement, y organise ou planifie d'y organiser une ou plusieurs activités, est suivie dans la banque de données commune T.E.R.

Cette information au bourgmestre est transmise au moyen de la carte d'information.

Sous sa responsabilité, le bourgmestre pourra partager ces données et informations avec les différents acteurs locaux qui ont la nécessité de prendre connaissance de celles-ci pour l'exercice de leurs missions légales, et donc dans le respect des principes d'adéquation, de pertinence et du caractère non excessif.

Ce partage d'informations ne peut bien entendu pas mettre en péril les missions opérationnelles qui découlent de l'exploitation des données et informations gérées dans la banque de données commune T.E.R.

S'il existe un doute quant au fait de mettre en péril une mission opérationnelle, le bourgmestre prendra toujours contact avec le chef de corps du service de police qui lui a transmis la carte d'information » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 124-125).

Le bourgmestre, en sa qualité d'autorité en matière de police administrative, est ainsi informé à deux moments : (1) lors de la création d'une entité, par le biais du chef de corps, en vertu de l'article 21, précité, de la loi attaquée et (2) lors du suivi de l'entité validée, par le biais de la carte d'information communiquée en vertu de l'article 26 de la même loi :

« Le premier moment a pour objectif d'informer le plus rapidement possible le bourgmestre même si les informations disponibles ne sont pas encore complètes. Le second moment donne au bourgmestre des informations dont le contenu est plus développé pour qu'il puisse prendre les mesures qui relèvent de ses compétences » (*ibid.*, p. 125).

B.29. Il s'ensuit que l'article 26 de la loi attaquée désigne de manière claire et précise le bourgmestre comme destinataire de la carte d'information.

Compte tenu, d'une part, de la difficulté d'identifier à l'avance de manière exhaustive les autorités ou institutions autres que celles visées aux articles 20 à 22 de la loi attaquée et les autorités ou institutions autres que le bourgmestre qui sont susceptibles de prendre des mesures à l'égard des entités validées de la banque de données commune T.E.R. et, d'autre part, des garanties contre les abus contenues dans les articles 23 à 25 de la loi attaquée, les termes « une

autorité ou une institution tierce » figurant à l'article 23, alinéa 1er, de la loi attaquée, lus en combinaison avec les articles 20 à 22 de cette même loi, permettent de définir de manière suffisamment précise la catégorie des destinataires de la carte d'information autres que le bourgmestre, les circonstances dans lesquelles une communication de la carte d'information à cette catégorie de destinataires est autorisée ainsi que les précautions à prendre pour cette communication.

En particulier, l'Organe de contrôle de l'information policière et le Comité permanent R peuvent vérifier que la carte d'information est communiquée à des destinataires autorisés, dès lors qu'une liste actuelle des communications de la carte d'information et des évaluations ayant précédé celles-ci est tenue à leur disposition (article 23, alinéa 3, de la loi attaquée).

B.30. Le grief n'est pas fondé.

7. En ce qui concerne les services ayant accès à la banque de données

B.31. Les parties requérantes citent dans la requête diverses remarques tirées de l'avis de l'Autorité de protection des données concernant l'avant-projet qui a mené à la loi attaquée, par lesquelles cette Autorité estime qu'il convient de démontrer, dans les travaux préparatoires, le caractère nécessaire et proportionné, d'une part, de la participation à la base de données commune T.E.R. des services existants et des nouveaux services et, d'autre part, de la centralisation systématique et exclusive des données dans la banque de données commune T.E.R. Toujours selon ces remarques, il s'indique de réaliser des statistiques en vue de la publication d'un rapport d'évaluation. Les parties requérantes précisent encore dans leur requête que « le législateur n'a pas tenu compte de ces remarques, de sorte que la loi attaquée viole les dispositions visées au moyen et doit être annulée ».

B.32. Un tel grief ne satisfait pas aux exigences, précitées, de l'article 6 de la loi spéciale du 6 janvier 1989 lorsque, comme en l'espèce, le législateur a formulé dans les travaux préparatoires une réponse circonstanciée sur cet aspect de l'avis (*Doc. parl.*, Chambre, 2023-

2024, DOC 55-3692/001, pp. 10-21) et que, par conséquent, ce dernier a bien été pris en compte, contrairement à ce qu'allèguent les parties requérantes.

B.33. Le grief est irrecevable.

8. En ce qui concerne la participation de l'Office des étrangers et des autres services aux « Task Forces locales »

B.34. Les parties requérantes se contentent de reproduire des extraits de l'avis de l'Autorité de protection des données n° 97/2023, précité, dans lesquels cette dernière estime, entre autres, que le caractère nécessaire et proportionné de la participation de l'Office des étrangers et des autres services aux « Task forces locales » n'est pas démontré.

B.35. Pour les mêmes motifs que ceux qui sont énoncés en B.32, un tel exposé ne satisfait pas aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989.

B.36. Le grief n'est pas recevable.

9. En ce qui concerne les finalités (article 5 de la loi attaquée)

B.37. Les parties requérantes font grief à l'article 5 de loi attaquée de ne pas distinguer, d'une part, les finalités poursuivies par la banque de données commune T.E.R. et les finalités des traitements des données à caractère personnel réalisés par chaque service et, d'autre part, les nécessités stratégiques, tactiques et opérationnelles.

B.38.1. L'article 5, alinéa 2, de la loi attaquée, cité en B.14.1, définit les finalités de la banque de données commune T.E.R.

B.38.2. Dans son avis n° 97/2023, précité, l'Autorité de protection des données a observé :

« 30. Tout d’abord, l’Autorité répète la demande formulée dès 2015 par la CPVP, à savoir que les nécessités stratégiques, tactiques et opérationnelles soient distinguées les unes des autres et décrites précisément dans la loi ou un arrêté d’exécution.

31. En outre, l’Autorité rappelle qu’elle est favorable à la détermination des finalités d’une banque de données (ou d’un registre), mais qu’il n’en demeure pas moins que le respect de l’article 5.1.b) du RGPD (de même que des art. 28, 2°, et 75 LTD) impose la détermination des finalités des traitements de données à caractère personnel (dont l’enregistrement dans une banque de données spécifique constitue un exemple parmi d’autres). Par conséquent, il y a lieu de distinguer les finalités liées à la création d’une banque de données, des finalités des différents traitements réalisés par chacun des services relativement à ces données (collecte, concertation en TFL, enregistrement dans la BDC, communication à d’autres services, transferts internationaux, etc...).

32. En ce qui concerne la collecte, il sera simplement renvoyé (dans le commentaire) aux législations organiques des services de base et des services partenaires. En revanche, il devra être démontré (dans le commentaire de l’art. 6), pour chacun des services disposant d’un droit d’écriture, en quoi la finalité de chacun des traitements ultérieurs de ces données est compatible avec la finalité pour laquelle elles ont été collectées.

33. En ce qui concerne les traitements ultérieurs réalisés par les services partenaires, l’art. 6, § 2, 2° du projet de loi permet le traitement des données opérationnelles policières, contenues dans la BDC, « qui sont adéquates, pertinentes et non excessives au regard des missions [de prévention et de suivi du terrorisme et de l’extrémisme, lorsqu’il peut mener au terrorisme (...)] de ces services, chacun dans le cadre de ses compétences légales] et des finalités [de la BDC] », par les services de base et les services partenaires disposant d’un droit de lecture.

34. L’Autorité précise que la détermination des catégories de données à caractère personnel relatives aux entités contenues dans la BDC qui sont accessibles de manière licite, c’est-à-dire communicables aux services partenaires (ou même la simple interrogation de la BDC) dépend à la fois de l’existence d’une base légale pour la communication ET des finalités propres de ces services partenaires. En d’autres termes, quelles que soient les limitations techniques du support d’enregistrement, l’enregistrement dans la BDC ne peut aboutir à ce qu’un service traite (ne fut-ce qu’en consultant) des données à caractère personnel qu’il ne serait pas autorisé à traiter en vertu de ses finalités propres.

35. Par conséquent, soit (1) les finalités de traitements auxquelles leurs lois organiques les soumettent leur permettent déjà d’avoir accès à ces données (dans ce cas, il convient de faire référence aux normes applicables et de préciser dans le commentaire de l’art. 6 que la disposition en projet se limite à prévoir une modalité technique de communication), soit (2) le projet entend prévoir une nouvelle finalité d’accès pour ces services (dans ce cas, il convient de le prévoir expressément, d’en justifier le caractère nécessaire et proportionné ET de prévoir une modification des lois organiques concernées en ce sens), soit enfin (3) le demandeur considère que la communication actuelle, par exemple sous forme de simple avis (favorable ou négatif), de rapport de police ou de demande de prise de mesures est trop limitée et entend l’étendre (et dans ce cas, outre l’adaptation des lois organiques respectives, il convient de dûment démontrer le caractère nécessaire et proportionné de l’augmentation de la quantité de données communiquées).

36. Le cas échéant et, pour autant que le caractère nécessaire et proportionné d'une telle communication et/ou de tels accès soient démontrés, le projet devra prévoir une adaptation (valable pour le futur) des normes organiques des services dont la finalité n'est actuellement pas libellée d'une manière à permettre un traitement ultérieur compatible ».

B.38.3. En ce qui concerne la nécessité de distinguer les finalités de la banque de données commune T.E.R. et les finalités des traitements des données à caractère personnel réalisés par chaque service, il ressort de l'article 3, alinéa 1er, *in fine*, de la loi attaquée et des travaux préparatoires que l'accès des services de base et des services partenaires aux données contenues dans la banque de données commune T.E.R. s'inscrit dans la réalisation des finalités propres de ces services (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 56-57 et pp. 86-87). Le législateur a dès lors pu estimer qu'il n'était pas nécessaire de modifier les lois organiques respectives de chacun de ces services.

B.38.4. En ce qui concerne la nécessité de distinguer les finalités stratégiques, tactiques et opérationnelles, il peut être admis que ces finalités sont indissociablement liées :

« Ainsi, ' au niveau stratégique, il faudra par exemple, sur la base des données à caractère personnel et informations disponibles dans la banque de données commune, décider de la politique à mener dans la lutte contre ces phénomènes ' (DOC 54 1727/001, p. 20). Cela se fera notamment dans le cadre du Conseil national de sécurité ou du Comité de coordination du renseignement et de la sécurité.

' Au niveau tactique, il sera question sur la base des données à caractère personnel et informations disponibles d'évaluer la façon dont les différents services vont mettre en œuvre les différentes actions à mener ' (DOC 54 1727/001, p. 20). Il s'agit par exemple des actions de la TFL ou de la National task force qui coordonne la stratégie T.E.R.

' Au niveau opérationnel, il s'agira de déterminer quelles actions doivent être prises conjointement ou par chaque service particulier sur la base des données à caractère personnel et des informations disponibles ainsi que les éventuelles mesures à prendre à l'égard de certaines personnes (arrestation, auditions, ...). [...] ' (DOC 54 1727/001, p. 20) » (*ibid.*, p. 51).

B.39. Le grief n'est pas fondé.

10. En ce qui concerne les catégories de données (article 6, § 2, de la loi attaquée)

B.40. Les parties requérantes font valoir que l'article 6, § 2, de la loi attaquée est disproportionné, notamment en ce que cette disposition permet le traitement de données à caractère personnel relatives aux opinions politiques et aux convictions religieuses ou philosophiques des entités concernées.

B.41. La Cour examine uniquement ce dernier grief, dès lors que c'est le seul à satisfaire aux exigences précitées de l'article 6 de la loi spéciale du 6 janvier 1989.

B.42.1. L'article 6, § 2, 1°, 1), c), ii. et iii., de la loi attaquée dispose :

« Les données à caractère personnel traitées dans la banque de données commune T.E.R. sont les données non classifiées au sens de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé suivantes :

1° les données des entités suivantes :

1) Si l'entité est une personne physique majeure ou mineure de douze ans ou plus :

[...]

c) les données relatives aux catégories particulières de données à caractère personnel suivantes :

[...]

ii. les opinions politiques;

iii. les convictions religieuses ou philosophiques; ».

B.42.2. Dans son avis n° 97/2023, précité (§ 101), l'Autorité de protection des données a observé que « le caractère nécessaire et proportionné du traitement des données relatives aux opinions politiques et aux convictions religieuses ou philosophiques, par chacun des services susceptible d'en prendre connaissance, devra [...] être démontré » et que cette démonstration « permettra [de] déterminer si les convictions philosophiques sont (erronément) mentionnées en raison du fait qu'elles sont énoncées conjointement dans de nombreuses dispositions (dont

l'art. 9.1 du RGPD) ou si certaines convictions philosophiques doivent effectivement laisser craindre une radicalisation violente ».

B.42.3. À cet égard, il a été répondu, lors des travaux préparatoires, que les opinions politiques et les convictions religieuses ou philosophiques font partie des catégories particulières de données à caractère personnel au sens de l'article 9, paragraphe 1, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) » (ci-après : le RGPD) dont le traitement dans la banque de données T.E.R. est « nécessaire et important pour comprendre le contexte lié à la personne concernée » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 67).

À propos, en particulier, des « opinions politiques », les travaux préparatoires précisent :

« Dans le cadre du suivi des extrémistes de gauche ou de droite, il est important de connaître leur idéologie (qui est fortement liée à leur opinion politique). Il est important de savoir si une propagandiste de haine propage une idéologie de droite ou de gauche et même de quel type de droite ou de quel type de gauche. Exemple: l'enregistrement de ces informations peut permettre d'identifier d'éventuelles cibles de la personne suivie dans la banque de données commune T.E.R. » (*ibid.*, p. 67)

En ce qui concerne les « convictions religieuses ou philosophiques », les travaux préparatoires précisent :

« Dans les cas d'extrémisme et de terrorisme religieux, il est important de connaître la conviction religieuse de l'intéressé notamment pour identifier d'éventuelles cibles de l'intéressé. Exemple: un chiite ne va pas avoir les mêmes cibles que des sunnites. Savoir qu'une personne est salafiste madkhalite ou jihadiste a aussi un impact important sur l'évaluation qui peut être faite de la menace.

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données s'interroge sur la nécessité de traiter également les convictions philosophiques (§ 101). Or, cette notion fait partie intégrante de la définition d'extrémisme visé à l'article 8, 1°, c), de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité: ' les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des

institutions démocratiques ou aux autres fondements de l'État de droit en ce compris le processus de radicalisation. '. Cette définition constitue la base de travail des services de base et des services partenaires comme le précise l'article 3 du projet » (*ibid.*, pp. 67-68).

Il ressort des travaux préparatoires précités que les notions d'« opinions politiques » et de « convictions religieuses » sont suffisamment claires. Il ressort des mêmes travaux préparatoires que les « convictions philosophiques » susceptibles d'être mentionnées dans la banque de données commune T.E.R. en vertu de l'article 6, § 2, 1°, 1), c), iii., de la loi attaquée désignent uniquement « les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, [...] à caractère [...] philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'Etat de droit en ce compris le processus de radicalisation » au sens de l'article 8, 1°, alinéa 2, c), de la loi organique du 30 novembre 1998.

Par conséquent, l'article 6, § 2, 1°, 1), c), iii., de la loi attaquée satisfait aux exigences mentionnées en B.6.2.

B.43. Le grief n'est pas fondé.

11. En ce qui concerne la durée de conservation des données (article 7 de la loi attaquée)

B.44. Les parties requérantes font valoir que l'article 7 de la loi attaquée est disproportionné. L'exposé développé dans la requête permet de déduire que le grief est notamment dirigé contre l'archivage des données à caractère personnel conservées dans la banque de données commune T.E.R. pour une durée de maximum trente ans, tel qu'il est prévu à l'article 7, § 3, de la loi attaquée. La Cour limite son examen à cet aspect de la disposition attaquée.

B.45.1. En ce qui concerne la durée de conservation des données de la banque de données commune T.E.R., l'article 143 de la loi sur la protection des données, tel qu'il a été modifié par l'article 39 de la loi attaquée, dispose :

« Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées dans [...] l'article 7 de la loi du 29 mars 2024 portant création de la banque de données commune ' Terrorisme, Extrémisme, processus de Radicalisation ' (' T.E.R. ') en ce qui concerne la banque de données commune T.E.R. ».

B.45.2. L'article 7 de la loi attaquée dispose :

« § 1er. Les données à caractère personnel conservées dans la banque de données commune T.E.R. sont archivées dès que les finalités visées à l'article 5, alinéa 2, ne sont plus rencontrées, et au maximum trente ans après le dernier enregistrement d'une donnée ou information dans la fiche de renseignement de l'entité validée, à l'exception des données à caractère personnel relatives à des mineurs qui sont conservées au maximum quinze ans après le dernier enregistrement d'une donnée ou information.

Après le dernier enregistrement d'une donnée ou information dans la fiche de renseignement de l'entité validée, le responsable opérationnel examine tous les cinq ans si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités de l'article 5, alinéa 2. Si tel n'est pas le cas, les données sont archivées.

Lorsque les données à caractère personnel sont relatives à des mineurs, l'examen visé à l'alinéa 2 a lieu tous les trois ans.

§ 2. Par dérogation au paragraphe 1er, les données à caractère personnel et les informations relatives à une entité en pré-enquête sont conservées pour une durée de maximum six mois après leur enregistrement.

A l'issue de ce délai, les données à caractère personnel et les informations sont supprimées de la banque de données commune T.E.R. conformément au paragraphe 3, alinéa 2, dès lors que l'entité en pré-enquête ne répond pas aux critères d'un *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou d'un propagandiste de haine.

§ 3. Les données à caractère personnel et les informations qui doivent être archivées le sont pour une durée de maximum trente ans.

À l'issue de ce délai, ces données et informations sont supprimées de la banque de données commune T.E.R., sans préjudice de la loi du 24 juin 1955 relative aux archives.

Lorsqu'une donnée ou information relative à une entité enregistrée se révèle être fausse ou erronée, elle est immédiatement supprimée.

La consultation des archives de la banque de données commune T.E.R. ne peut être réalisée que dans le cadre des finalités suivantes:

1° l'appui à la définition et à la réalisation de la politique de sécurité en matière de terrorisme et d'extrémisme pouvant mener au terrorisme;

2° le traitement des antécédents dans le cadre d'une enquête judiciaire ou de renseignement relative au terrorisme ou à l'extrémisme pouvant mener au terrorisme;

3° la défense en justice des autorités visées à l'article 5, alinéa 2, 3°;

4° l'exercice des missions des autorités de contrôle;

5° la réalisation de finalités historiques, scientifiques ou statistiques.

Le résultat de l'exploitation des archives de la banque de données commune T.E.R. pour la finalité prévue à l'alinéa 4, 1°, est anonymisé.

§ 4. Si dans le cadre de la consultation visée au paragraphe 3, alinéa 4, 2°, les données archivées répondent de nouveau à la finalité visée à l'article 5, alinéa 2, 2°, les données sont désarchivées ».

B.45.3. En vertu de l'article 7, § 1er, alinéas 2 et 3, de la loi attaquée, après le dernier enregistrement d'une donnée ou information dans la fiche de renseignement de l'entité validée, l'OCAM, en tant que responsable opérationnel de la banque de données commune T.E.R., examine tous les cinq ans (tous les trois ans lorsque les données à caractère personnel sont relatives à des mineurs) si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités de la banque de données commune. Sinon, et en tout cas trente ans (ou quinze ans pour les données relatives aux mineurs) après le dernier enregistrement, les données sont archivées pour une durée de maximum trente ans (article 7, § 1er, alinéas 1er et 2, *juncto* le § 3, alinéa 1er).

À l'issue du délai d'archivage de maximum trente ans, les données et informations archivées sont supprimées de la banque de données commune T.E.R. « sans préjudice de la loi du 24 juin 1955 relative aux archives » (article 7, § 3, alinéa 2).

Une donnée ou information relative à une entité enregistrée qui se révèle fausse ou erronée est immédiatement supprimée (article 7, § 3, alinéa 3).

Les données archivées peuvent être consultées dans le cadre de l'une des finalités mentionnées à l'article 7, § 3, alinéa 4. Le résultat de l'exploitation des archives de la banque de données commune T.E.R. pour la finalité prévue à l'article 7, § 3, alinéa 4, 1° (« l'appui à la définition et à la réalisation de la politique de sécurité en matière de terrorisme et d'extrémisme

pouvant mener au terrorisme ») est anonymisé (article 7, § 3, alinéa 5). Les données archivées qui, au terme de la consultation visée à l'article 7, § 3, alinéa 4, 2° (« le traitement des antécédents dans le cadre d'une enquête judiciaire ou de renseignement relative au terrorisme ou à l'extrémisme pouvant mener au terrorisme »), répondent de nouveau à la finalité visée à l'article 5, alinéa 2, 2° (« la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des services de base et des services partenaires ») sont désarchivées (article 7, § 4).

Pour les entités pré-enquête, il est prévu un délai de conservation réduit de six mois maximum, au terme duquel les données à caractère personnel et informations concernant ces entités sont supprimées (article 7, § 2).

B.46.1. Comme il est dit en B.6.2, une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement reposer sur une disposition législative suffisamment précise, mais aussi répondre à un besoin social impérieux dans une société démocratique et être proportionnée au but légitime poursuivi.

Dans le cadre de cet examen, il y a lieu de vérifier si l'ingérence ne va pas au-delà de ce qui est nécessaire à la réalisation des objectifs poursuivis, et en particulier s'il existe des mesures qui sont moins attentatoires aux droits concernés, tout en contribuant de manière efficace au but de la réglementation en cause (CJUE, 17 octobre 2013, C-291/12, *Schwarz c. Stadt Bochum*, ECLI:EU:C:2013:670, points 46-47). La protection du droit fondamental au respect de la vie privée au niveau de l'Union exige, conformément à la jurisprudence constante de la Cour de justice, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire (CJUE, grande chambre, 16 décembre 2008, C-73/07, *Satakunnan Markkinapörssi Oy e.a.*, ECLI:EU:C:2008:727, point 56; grande chambre, 6 octobre 2015, C-362/14, *Schrems*, ECLI:EU:C:2015:650, point 92; grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, ECLI:EU:C:2020:791, point 130).

Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient de tenir compte, notamment, de leur caractère automatisé, des

techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées et de la présence ou de l'absence de garanties visant à éviter l'usage inapproprié et abusif, par les services publics, des données à caractère personnel traitées (arrêt n° 108/2016, ECLI:BE:GHCC:2016:ARR.108, B.12.2; arrêt n° 29/2018, ECLI:BE:GHCC:2018:ARR.029, B.14.4; arrêt n° 27/2020, ECLI:BE:GHCC:2020:ARR.027, B.8.3; CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, précité, § 59; 12 janvier 2016, *Szabó et Vissy c. Hongrie*, ECLI:CE:ECHR:2015:1013JUD001132714, § 68; CJUE, grande chambre, 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland Ltd e.a.*, ECLI:EU:C:2014:238, points 56-66).

B.46.2. Le pouvoir de surveiller en secret les citoyens, caractéristique de l'État policier, n'est tolérable, d'après la Convention, que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques (CEDH, grande chambre, 6 septembre 1978, *Klass e.a. c. Allemagne*, ECLI:CE:ECHR:1978:0906JUD000502971, § 42; 12 janvier 2016, *Szabó et Vissy c. Hongrie*, précité, § 54).

Lorsqu'elles mettent en balance, d'une part, l'intérêt de l'État défendeur à protéger la sécurité nationale au moyen de méthodes de surveillance secrète et, d'autre part, la gravité de l'ingérence dans l'exercice du droit au respect de la vie privée, les autorités nationales disposent d'une certaine marge d'appréciation dans le choix des moyens permettant d'atteindre le but légitime que constitue la protection de la sécurité nationale. Cette marge d'appréciation va toutefois de pair avec un contrôle de l'existence de garanties adéquates et effectives contre les abus, car un système de surveillance secrète destiné à protéger la sécurité nationale risque de saper, voire de détruire, la démocratie au motif de la défendre. L'appréciation de cette question est fonction de toutes les circonstances de la cause, par exemple la nature, la portée et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour

les permettre, les exécuter et les contrôler, et le type de recours fourni par le droit interne (CEDH, grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*, précité, § 232; grande chambre, 25 mai 2021, *Big Brother Watch e.a. c. Royaume-Uni*, précité, §§ 338-339).

B.47.1. Le législateur a opté, à l'article 7 de la loi attaquée, pour un système dans lequel deux périodes doivent être distinguées : d'une part, la période de conservation initiale de cinq ans, renouvelable cinq fois jusqu'à maximum trente ans (ou de trois ans renouvelable quatre fois jusqu'à un maximum de quinze ans pour les données relatives aux mineurs), visée au paragraphe 1er de cette disposition et, d'autre part, la période d'archivage ultérieure de maximum trente ans visée au paragraphe 3, qui est consécutive à la période de conservation initiale. Les données à caractère personnel concernées sont donc susceptibles d'être conservées dans la banque de données commune T.E.R. pendant soixante ans au total (avis n° 97/2023 de l'Autorité de protection des données, § 113).

Ainsi, selon les termes de l'article 7 de la loi attaquée, l'OCAM examine tous les cinq ans (ou tous les trois ans) si les données à caractère personnel de la banque de données commune T.E.R. présentent toujours un lien direct avec l'une des finalités de cette banque de données. Si, à l'échéance du premier délai de cinq ans (ou de trois ans), les données à caractère personnel présentent toujours un tel lien, elles sont conservées dans la banque de données commune T.E.R. jusqu'à la prochaine évaluation de la pertinence de leur conservation, cinq ans (ou trois ans) plus tard. Les données conservées de manière « active » pendant maximum trente ans (ou quinze ans) dans la banque de données commune T.E.R. (période de conservation initiale) sont donc les données dont l'OCAM a considéré lors des contrôles successifs effectués à cinq ans (ou trois ans) d'intervalle qu'elles demeurent en lien direct avec l'une des finalités de la banque de données.

Si, à l'issue de l'une des évaluations réalisées tous les cinq ans (ou tous les trois ans), il s'avère que les données à caractère personnel ne présentent plus de lien direct avec l'une des finalités de la banque de données commune T.E.R. et en tout cas trente ans (ou quinze ans) après le dernier enregistrement des données concernées, ces données sont archivées dans cette banque de données pour une période de maximum trente ans (période d'archivage ultérieure). Les données concernées sont ainsi archivées dès qu'il s'avère qu'elles ne présentent plus de

lien direct avec l'une des finalités de la banque de données commune T.E.R., sans attendre l'expiration du délai de conservation initial de trente ans (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 80 et 83).

B.47.2. En ce qui concerne la période de conservation initiale, le contrôle régulier, tous les cinq ans (ou tous les trois ans) de l'actualité de la pertinence de conserver les données à caractère personnel de la banque de données commune T.E.R. est prévu « par parallélisme avec le délai prévu par la loi du 10 juillet 2006 relative à l'analyse de la menace » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 80) pour « renforcer les obligations en matière de conservation des données qui ne sont manifestement plus traitées depuis un certain temps » (*ibid.*, p. 81). Ce contrôle constitue « une garantie supplémentaire qui se rajoute à l'obligation de l'OCAM de réaliser des évaluations de la menace en continu (et actualiser cette évaluation au minimum deux fois par [an]) » visée à l'article 27, alinéa 2, de la loi attaquée (*ibid.*, p. 80).

B.47.3. En ce qui concerne la période d'archivage ultérieure, l'article 7, §§ 1er et 3, de la loi attaquée remplace l'article 44/11/3bis, §§ 5 et 7, de la loi sur la fonction de police, tel qu'il a été inséré par l'article 13 de la loi du 27 avril 2016 et tel qu'il était applicable avant son abrogation par l'article 55, 3°, de la loi attaquée. Cet article 44/11/3bis, §§ 5 et 7, de la loi sur la fonction de police disposait :

« § 5. Les données à caractère personnel conservées au sein des banques de données communes sont supprimées dès que les finalités visées au § 2 disparaissent, et au maximum 30 ans après le dernier traitement, sans préjudice de la loi du 24 juin 1955 relative aux archives.

Après le dernier traitement, il est examiné au minimum tous les trois ans si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités du § 2. Si tel n'est pas le cas, les données sont supprimées.

[...]

§ 7. Les données à caractère personnel et les informations qui doivent être supprimées peuvent être archivées pour une durée de maximum 30 ans.

A l'issue de ce délai, ces données et informations sont effacées, sans préjudice de la loi du 24 juin 1955 relative aux archives.

La consultation des archives d'une banque de données commun[e] ne peut être réalisée que dans le cadre des finalités suivantes :

1° l'appui à la définition et à la réalisation de la politique policière et de sécurité en matière de terrorisme et d'extrémisme pouvant mener au terrorisme;

2° le traitement des antécédents dans le cadre d'une enquête relative à un fait criminel de terrorisme;

3° la défense des autorités visées à l'article 44/11/3bis, § 2, 2° en justice.

Le résultat de l'exploitation des archives de la banque de données commune pour la finalité prévue à l'alinéa 1er, 1°, est anonymisé ».

Par rapport à l'article 44/11/3bis, § 7, précité, de la loi sur la fonction de police, l'article 7, § 3, de la loi attaquée « rend obligatoire, et non plus optionnel, l'archivage pour une durée de 30 ans des données à caractère personnel et des informations » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 84).

Il ressort des travaux préparatoires de la loi attaquée que l'accès aux archives consiste en une « simple consultation » des données à caractère personnel et informations qui y figurent, sans droit de création, un droit de lecture ou d'écriture dans celles-ci. En effet, « rien de nouveau n'est créé ou modifié dans les archives » (*ibid.*, p. 84). En ce qui concerne la finalité de « traitement des antécédents dans le cadre d'une enquête judiciaire ou de renseignement relative au terrorisme ou à l'extrémisme pouvant mener au terrorisme » (article 7, § 3, alinéa 4, 2°, de la loi attaquée), seuls le ministère public, les services de police et les services de renseignement pourront avoir accès aux archives dans le cadre d'enquêtes judiciaires et d'enquêtes de renseignement (*ibid.*, p. 85).

Les travaux préparatoires de la loi attaquée (*ibid.*, pp. 85-88) renvoient par ailleurs à ceux de la loi du 27 avril 2016, laquelle a introduit l'article 44/11/3bis, précité, de la loi sur la fonction de police.

Les travaux préparatoires de cette dernière loi précisent notamment :

« Les phénomènes de terrorisme et d'extrémisme pouvant conduire au terrorisme ne peuvent en effet pas être traités utilement sur des courtes périodes vu que les réponses opérationnelles à apporter sont tributaires d'une compréhension historique, anthropologique et sociétale de ceux-ci.

Il peut en effet s'avérer que des données recueillies prennent plus de sens ou un éclairage différent après de nombreuses années, à la lumière de nouvelles informations ou d'événements nouveaux.

De même, les premières phases d'identification, de recrutement et d'activation de personnes ou de cellules dormantes peuvent être espacées par de nombreuses années. Certaines organisations laissent leurs membres parvenir à des fonctions-clés avant de les solliciter à nouveau.

L'allongement de la durée de vie amène à devoir concevoir l'implication de personnes dans des organisations ou des mouvances qui font l'objet de l'attention légitime des services compétents et dont les données sont traitées dans les banques de données communes sur une durée plus longue correspondant à cette mutation démographique.

Il convient ainsi de relever que certaines personnes ayant quitté un groupement, ou n'ayant plus attiré l'attention des autorités au sein d'une mouvance pendant de nombreuses années, reprennent leurs activités passées. C'est ainsi que des personnes, bien qu'âgées, reprennent un activisme délaissé après être entré en sommeil durant une période de leur vie.

Il est également possible d'archiver les données et informations qui entrent dans les conditions pour être supprimées.

Cet archivage n'est pas rendu obligatoire du fait que les banques de données communes sont alimentées par différents services qui, comme par exemple la police en ce qui concerne la BNG et les banques de données de base, disposent déjà d'un système d'archivage pour leurs propres banques de données.

Toutefois, il arrive qu'une recherche sur l'historique soit nécessaire.

Comme ces données et informations archivées ne remplissent plus les conditions pour une utilisation opérationnelle, elles ne pourront être consultées que pour des finalités strictement limitées et qui répondent aux nécessités suivantes :

- établir une politique de sécurité en matière de terrorisme en comparant anciennes et nouvelles données et informations. Dans ce cas, le résultat de l'exploitation sera anonymisé;
- sur le plan opérationnel, certaines vieilles données peuvent s'avérer utiles dans le cadre d'une enquête sur un fait grave de terrorisme;
- lorsque la décision d'une autorité est attaquée en justice » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1727/001, pp. 24-25).

B.47.4. Il en découle qu'après leur archivage, conformément à l'article 7, § 3, de la loi attaquée, les données à caractère personnel conservées dans la banque de données commune T.E.R. ne sont plus visibles dans celle-ci pour les services de base et les services

partenaires concernés et que les données à caractère personnel archivées ne peuvent plus être consultées que dans des situations exceptionnelles, par un nombre limité de personnes ou d'instances. Compte tenu des finalités pour lesquelles une telle consultation est possible, il est question d'un archivage soit dans l'intérêt général (article 7, § 3, alinéa 4, 1° à 4°, de la loi attaquée), soit dans le cadre de finalités historiques, scientifiques ou statistiques (article 7, § 3, alinéa 4, 5°, de la loi attaquée).

Si la consultation s'inscrit en appui de la définition et de la réalisation de la politique de sécurité en matière de terrorisme et d'extrémisme pouvant mener au terrorisme, le résultat de celle-ci doit être anonymisé (article 7, § 3, alinéa 5, de la loi attaquée). Les articles 162 à 167 de la loi sur la protection des données prévoient également des garanties spécifiques qui s'appliquent à la consultation des données à caractère personnel archivées à des fins historiques, scientifiques ou statistiques, en particulier l'anonymisation ou la pseudonymisation de ces données. Plus généralement, il convient de se conformer, dans le cadre de l'archivage également, au principe de la minimisation des données. En vertu de ce principe, les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

B.47.5. Vu le caractère exceptionnel de la consultation et compte tenu du principe, susvisé, de minimisation des données, il y a lieu de considérer que, hors les cas précités où le résultat de la consultation est anonymisé ou pseudonymisé, la consultation des archives de la banque de données commune T.E.R. n'est possible que lorsque les finalités mentionnées précédemment ne peuvent pas être rencontrées d'une autre manière, comme c'est également le cas pour la consultation des archives de la Banque de données nationale générale (B.N.G.) effectuée en vertu de l'article 44/10 de la loi sur la fonction de police (voy. arrêt n° 108/2016 du 14 juillet 2016, précité, B.113.2).

Sous réserve de cette interprétation, vu la nature des finalités décrites à l'article 7, § 3, alinéa 4, de la loi attaquée et compte tenu, d'une part, des conditions strictes régissant la consultation des archives et, d'autre part, du contrôle qu'exercent sur cette consultation l'Organe de contrôle de l'information policière et le Comité permanent R, il est raisonnablement justifié que les données traitées dans la banque de données commune T.E.R. ne fassent pas l'objet d'une suppression immédiate et définitive lorsque les finalités de cette

banque de données ne sont plus rencontrées ou que les délais visés à l'article 7, § 1er, de la loi attaquée ont expiré, mais qu'elles soient archivées. À cet égard, les finalités liées à l'archivage justifient que les archives concernées soient conservées pendant une période substantielle, en l'espèce trente ans. C'est d'autant plus vrai dans le contexte du terrorisme et de l'extrémisme pouvant mener au terrorisme, où, comme il ressort des travaux préparatoires cités en B.47.3, les données à caractère personnel concernées peuvent de nouveau s'avérer pertinentes après un long laps de temps.

B.48. Sous réserve de l'interprétation mentionnée en B.47.5, le grief n'est pas fondé.

12. En ce qui concerne les droits des personnes concernées (article 4 de la loi attaquée)

a) Les règles régissant les droits des personnes concernées et les responsables du traitement

B.49. Les parties requérantes soutiennent que l'article 4 de la loi attaquée viole les normes de référence visées au premier moyen, en ce que les limitations des droits des personnes concernées ne sont pas suffisamment prévisibles à défaut d'une identification claire du ou des responsables de chaque traitement.

B.50.1. L'article 4 de la loi attaquée dispose :

« Sans préjudice des articles 11 et 45 de la loi relative à la protection des données, les règles relatives à la protection des données et aux droits de la personne concernée sont celles visées au titre 3, sous-titre 4, de la même loi ».

L'article 11, § 1er, de la loi sur la protection des données prévoit que les dispositions relatives aux droits des personnes concernées applicables aux traitements de données à caractère personnel qui relèvent du champ d'application du RGPD (les articles 12 à 22 et l'article 34 de ce règlement) ainsi que le principe de la transparence du traitement visé à l'article 5 de ce règlement ne s'appliquent pas aux traitements de données à caractère personnel émanant directement ou indirectement des autorités visées au titre 3 de la même loi à l'égard des autorités et personnes que désigne ce paragraphe. L'article 11, § 5, alinéa 3, de la même loi prévoit que

si l'Autorité de protection des données est saisie d'une requête ou d'une plainte qui ne porte que sur des données à caractère personnel émanant d'une autorité visée au titre 3, elle répond, après réception de la réponse du Comité permanent R, que « les vérifications nécessaires ont été effectuées ».

L'article 45, § 1er, de la même loi prévoit que les dispositions relatives aux droits des personnes concernées applicables aux traitements de données à caractère personnel qui relèvent du champ d'application de la directive « police » (les articles 36 à 44 et 62 de la même loi) ne s'appliquent pas aux traitements de données à caractère personnel émanant directement ou indirectement des autorités visées au titre 3 à l'égard des responsables du traitement et des autorités compétentes visées au titre 2 de cette loi, auxquelles ces données ont été transmises. L'article 45, § 6, alinéa 3, de la même loi, lu en combinaison avec l'article 71 de celle-ci, prévoit que, si l'Organe de contrôle de l'information policière est saisi d'une requête ou d'une plainte qui ne porte que sur des données à caractère personnel émanant d'une autorité visée au titre 3, il répond, après réception de la réponse du Comité permanent R, que « les vérifications nécessaires ont été effectuées ».

L'article 139, alinéa 1er, de la loi sur la protection des données, tel qu'il a été modifié par l'article 37 de la loi attaquée, dispose que le sous-titre 4 du titre 3 de cette loi s'applique « à tout traitement de données à caractère personnel par l'OCAM et ses sous-traitants effectué dans le cadre des missions visées par la loi du 10 juillet 2006, ainsi que par ou en vertu de lois particulières et à tout traitement de données à caractère personnel dans la banque de données commune T.E.R. ». L'article 139, alinéa 2, de la même loi précise que « les titres 1er, 2, 4, 5, et 7 de la présente loi ne s'appliquent pas [à ces traitements]. Dans le titre 6, seuls les articles 226, 227 et 230 s'appliquent ».

Il s'ensuit que, contrairement à ce que les parties requérantes allèguent, les traitements des données effectués dans la banque de données commune T.E.R. ne relèvent du champ d'application ni du titre 1 ni du titre 2 de la loi sur la protection des données, mais bien du champ d'application du titre 3 de cette loi, qui est intitulé « De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par d'autres autorités que celles visées aux titres 1er et 2 », et plus particulièrement du sous-titre 4 sous ledit titre, qui est

intitulé « De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par l'organe de coordination pour l'analyse de la menace et dans la banque de données commune ' Terrorisme, Extrémisme, processus de Radicalisation ' » et qui est composé des articles 138 à 167 de cette loi.

B.50.2. Les travaux préparatoires de la loi attaquée mentionnent :

« Le présent avant-projet de loi règle les questions en matière de protection des données qui sont propres aux traitements de données au sein de la banque de données commune T.E.R., à savoir quels types de données à caractère personnel y sont traitées, pour quelles finalités, pendant combien de temps, qui est responsable du traitement, quelles autorités doivent alimenter la banque de données, avec quelles catégories de données, quelles sont les catégories d'autorités qui peuvent recevoir accès ou communication de tout ou partie des données, l'obligation de journaliser les données, et quelles sont les autorités de protection des données compétentes.

Par ailleurs, dans une optique de cohérence, le législateur a choisi pour les autres règles en matière de protection des données (obligation des responsables du traitement, choix d'un sous-traitant, droits des personnes concernées,...) de se raccrocher par analogie au titre 3, sous-titre 4 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui est dédié aux traitements de données à caractère personnel réalisés par l'OCAM. Bien que le contexte qui entoure les traitements de données à caractère personnel par l'OCAM au moyen de ses propres systèmes d'informations est fort différent du contexte particulier qui entoure les traitements de données à caractère personnel réalisés au sein de la banque de données commune T.E.R., nous retrouvons dans les deux cas une mutualisation de données à caractère personnel et d'informations provenant de responsables du traitement qui ne sont pas tous soumis aux mêmes obligations en matière de protection des données à caractère personnel. Il est impératif, pour garantir la plus grande sécurité juridique possible, mais également en termes de lisibilité pour les personnes concernées – et par conséquent, faciliter l'exercice de leurs droits – de définir un régime commun à ces traitements » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 48-49).

Et :

« Toute proportion gardée, on retrouve [...] une similitude entre les traitements que l'OCAM effectue sur des données à caractère personnel et des informations provenant de ses différents services d'appui avec la banque de données commune T.E.R. qui mutualise les données à caractère personnel et les informations introduites par les services de bases et d'autres partenaires. Le traitement ' en commun ' des données dans la banque de données commune T.E.R. implique qu'un seul régime commun soit appliqué à ces données, en particulier concernant le droit des personnes concernées, ceci au bénéfice d'une plus grande sécurité juridique profitable à tous.

[...]

En définitive, le régime général en matière de traitement de données à caractère personnel pour la banque de données commune T.E.R. se trouve entièrement [intégré] dans la loi sur la protection des données. L'avant-projet ne contient plus que des aménagements, comme les délais de conservation des données et les brèches de sécurité ou des règles spécifiques à certains acteurs de la banque de données commune (notamment le gestionnaire et le responsable opérationnel) » (*ibid.*, pp. 146-147).

B.50.3. Comme l'a observé la section de législation du Conseil d'Etat (*ibid.*, p. 197), il résulte des travaux préparatoires précités que, d'une part, le régime autonome que prévoit la loi attaquée et, d'autre part, les articles 138 à 167 de la loi sur la protection des données, tels qu'ils sont modifiés par les articles 35 à 50 de la loi attaquée, s'appliquent complémentirement afin d'énoncer l'ensemble des règles en matière de droit au respect de la vie privée, de droit à la protection des données à caractère personnel et d'admissibilité des ingérences dans l'exercice de ces droits, qui s'appliquent aux traitements effectués dans la banque de données commune T.E.R.

Par ailleurs, il ressort des mêmes travaux préparatoires que, pour les règles relatives aux droits des personnes concernées par le traitement de données à caractère personnel dans la banque de données T.E.R., le législateur a choisi d'appliquer par analogie les règles relatives aux droits applicables aux traitements de données à caractère personnel effectués par l'OCAM. À cette fin, les articles 35 à 50 de la loi attaquée modifient les articles 138 à 167 de la loi sur la protection des données afin d'étendre l'application de ces dispositions, anciennement applicables uniquement aux traitements de données à caractère personnel effectués par l'OCAM, aux traitements effectués dans la banque de données commune T.E.R.

B.50.4. Les règles qui régissent les droits des personnes concernées par le traitement de données à caractère personnel dans la banque de données T.E.R., et les limitations éventuelles de ces droits, sont ainsi définies de manière claire.

B.51.1. En ce qui concerne la répartition des responsabilités en matière de protection des données, l'article 30 de la loi attaquée dispose que la responsabilité de la qualité des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. incombe, d'une part, au responsable du traitement propre à chaque service qui alimente la banque de données commune T.E.R. pour les données à caractère personnel et informations transmises par ces services (article 30, § 1er, 1°, de la loi attaquée) et, d'autre part, aux ministres

de l'Intérieur et de la Justice, en tant que responsables conjoints du traitement de la banque de données commune T.E.R., pour les données à caractère personnel et informations validées sur les fiches de renseignement (article 30, § 1er, 2°, lu en combinaison avec l'article 5, alinéa 1er). La responsabilité de la légalité de la transmission des données à caractère personnel et informations vers la banque de données commune T.E.R. incombe au responsable du traitement de chaque service qui alimente la banque de données commune T.E.R. (article 30, § 2). La responsabilité de la légalité de la transmission des données à caractère personnel et informations depuis la banque de données commune T.E.R. incombe aux ministres de l'Intérieur et de la Justice, qui sont les responsables conjoints du traitement de la banque de données commune T.E.R. (article 30, § 3, 1°). Ces derniers veillent également au bon fonctionnement technique et opérationnel de cette banque de données et à l'intégrité, à la disponibilité et à la confidentialité des données à caractère personnel et informations de la banque de données commune T.E.R., ainsi qu'à la sécurité des systèmes d'accès (article 30, § 3, 2° et 3°).

B.51.2. À ce propos, les travaux préparatoires mentionnent :

« En matière de qualité des données, il convient de distinguer la responsabilité du responsable du traitement du service qui transmet une donnée à la banque de données commune T.E.R. et celle du responsable du traitement de la banque de données commune T.E.R. même. [...]

Ainsi, le responsable du traitement du service fournisseur garde sa responsabilité quant à la licéité de sa donnée transmise aux termes de la loi vie privée, tandis que le responsable du traitement de la banque de données commune T.E.R. en assure la responsabilité dès lors que cette donnée transmise est exploitée dans sa banque de données.

Il serait en effet incohérent que le responsable du traitement de la banque de données commune T.E.R. puisse porter une quelconque responsabilité sur une donnée erronée dont le traitement aurait été effectué par un tiers.

De même, le responsable du traitement du fournisseur ne pourrait être tenu responsable d'une donnée qui a été transmise à la banque de données commune T.E.R. et qui, à la suite de son exploitation, ne serait plus correcte. Il convient de préciser que le terme 'service' doit être entendu de manière générale, on ne vise dès lors pas un individu spécifique mais bien l'institution.

En matière de transmission des données, là aussi, chaque responsable du traitement doit porter une responsabilité sur la légalité de cette transmission. Le responsable du traitement fournisseur doit s'assurer que la transmission de sa donnée soit effectuée dans le respect de la

loi, tandis que le responsable du traitement de la banque de données commune T.E.R. doit s'assurer de la légalité lorsque la donnée est transmise de cette banque de données.

À noter que ces règles en matière de responsabilité concernent également les données et informations d'un certain service qui seraient enregistrées dans la banque de données commune T.E.R. par un autre service. Ce serait éventuellement le cas lorsqu'un service de base estime, après prise de contact, qu'une donnée d'un service partenaire ayant reçu un HIT lors de l'utilisation du droit d'interrogation, pourrait enrichir la banque de données commune T.E.R. La qualité de l'information ainsi enregistrée par le service de base serait de la responsabilité du responsable du traitement du service source et non du service de base.

Les responsabilités du responsable du traitement sont décrites dans la loi relative à la protection des données, mais, dans un souci de clarté, le projet met l'accent sur certaines obligations que doit assurer le responsable du traitement de la banque de données commune T.E.R. Il est ainsi rappelé que le responsable du traitement de la banque de données commune T.E.R. doit veiller au bon fonctionnement technique et fonctionnel de sa banque de données afin, par exemple, de s'assurer qu'une donnée transmise ne soit pas altérée par un dysfonctionnement technique.

Le responsable de la banque de données commune T.E.R. s'assure également de l'intégrité, la disponibilité et la confidentialité des données et informations qui y sont enregistrées » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 129-131).

B.51.3. Les responsables de chaque traitement sont dès lors clairement déterminés.

B.52. Le grief des parties requérantes relatif aux règles régissant les droits des personnes concernées et des responsables du traitement n'est pas fondé.

b) L'absence d'une notification active

B.53. Les parties requérantes reprochent en outre à l'article 4 de la loi attaquée de ne pas prévoir une notification active aux personnes surveillées les informant, à l'issue d'une mesure de surveillance, du fait qu'elles ont fait l'objet d'une telle mesure. Le droit d'accès aux données et le droit à un recours juridictionnel effectif des personnes concernées ne seraient pas non plus suffisamment garantis en ce que la seule possibilité de contrôle dont disposeraient les personnes concernées serait de saisir l'Organe de contrôle de l'information policière et le Comité

permanent R, lesquels pourraient uniquement répondre que toutes les vérifications nécessaires ont été effectuées.

B.54.1. Ni la loi attaquée ni les articles 138 à 167 de la loi sur la protection des données, tels qu'ils ont été modifiés par les articles 35 à 50 de la loi attaquée, ne prévoient une obligation, pour les autorités, de notifier activement à la personne concernée le fait que des données à caractère personnel et informations la concernant ont été traitées dans la banque de données commune T.E.R. par les services de base et les services partenaires.

B.54.2. Les droits des personnes concernées sont fixés aux articles 144 à 148 de la loi sur la protection des données, qui forment le chapitre VI (« Droits de la personne concernée ») du sous-titre 4 du titre 3 de cette loi. Ces articles disposent :

« Art. 144. Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel.

Art. 145. La personne concernée a le droit de demander :

- 1° la rectification ou la suppression de ses données à caractère personnel inexactes;
- 2° la vérification auprès de l'autorité de contrôle compétente du respect des dispositions du présent sous-titre.

Art. 146. Les droits visés à l'article 145 s'exercent, sans frais, par l'intermédiaire de l'autorité de contrôle compétente, à l'initiative de la personne concernée justifiant de son identité.

L'autorité de contrôle compétente effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

Les modalités d'exercice de ces droits sont déterminées par la loi.

Art. 147. Les autorités de contrôle visées à l'article 161, les responsables conjoints du traitement de la banque de données commune T.E.R. et l'OCAM tiennent un journal des demandes d'exercice des droits par les personnes concernées.

Art. 148. Une décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

L'interdiction prévue à l'alinéa 1er ne s'applique pas lorsque la décision est fondée sur une disposition prévue par ou en vertu d'une loi ou lorsque la décision est nécessaire pour la sauvegarde d'un intérêt public important ».

En vertu de l'article 146 de la loi sur la protection des données, les droits de la personne concernée visés à l'article 145 de cette loi (à savoir le droit d'obtenir la rectification ou la suppression des données à caractère personnel la concernant qui seraient inexactes et le droit d'obtenir la vérification du respect des dispositions du sous-titre 3) peuvent être exercés, à l'initiative de cette personne, sans frais et moyennant la seule justification de son identité, par l'intermédiaire de l'Organe de contrôle de l'information policière et le Comité permanent R, en tant qu'autorités de contrôle des traitements réalisés dans la banque de données commune T.E.R. (alinéa 1er, *juncto* l'article 161, alinéa 2, de la même loi). Ces autorités « effectue[nt] les vérifications » et « communique[nt] uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires » (alinéa 2).

B.55.1. En ce qui concerne le grief relatif à l'absence d'une notification active, il ressort de la jurisprudence de la Cour européenne des droits de l'homme que l'examen et le contrôle des méthodes de surveillance secrète peuvent intervenir à trois stades : lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé (CEDH, grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*, précité, § 233; grande chambre, 29 avril 2022, *Centrum för rättvisa c. Suède*, ECLI:CE:ECHR:2021:0525JUD003525208, § 250; grande chambre, 25 mai 2021, *Big Brother Watch e.a. c. Royaume-Uni*, ECLI:CE:ECHR:2021:0525JUD005817013, § 336).

En ce qui concerne le troisième stade, c'est-à-dire lorsque la surveillance a cessé, la Cour européenne des droits de l'homme a jugé :

« [...] la question de la notification *a posteriori* de mesures de surveillance est indissolublement liée à celle de l'effectivité des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance. La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci (*Klass et autres*, précité, § 57, et *Weber et Saravia*, décision précitée, § 135) ou si – autre cas de figure –, soupçonnant que ses communications font ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de l'interception n'a pas été informé de cette mesure (*Kennedy*, précité, § 167) » (CEDH, grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*, précité, § 234. Voir aussi : CEDH, grande chambre, 25 mai 2021, *Big Brother Watch e.a. c. Royaume-Uni*, précité, § 337; grande chambre, 29 avril 2022, *Centrum för rättvisa c. Suède*, précité, § 251).

B.55.2. Lorsqu'elles mettent en balance, d'une part, l'intérêt à protéger la sécurité nationale au moyen de méthodes de surveillance secrète et, d'autre part, la gravité de l'ingérence dans l'exercice du droit au respect de la vie privée, les autorités nationales disposent d'une certaine marge d'appréciation dans le choix des moyens permettant d'atteindre le but légitime que constitue la protection de la sécurité nationale (CEDH, grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*, précité, § 232 ; grande chambre, 29 avril 2022, *Centrum för rättvisa c. Suède*, précité, § 252; grande chambre, 25 mai 2021, *Big Brother Watch e.a. c. Royaume-Uni*, précité, § 338. Voir aussi : CEDH, grande chambre, 6 septembre 1978, *Klass et autres c. Allemagne*, précité, §§ 49, 50 et 59 ; décision, 29 juin 2006, *Weber et Saravia c. Allemagne*, précité, § 106; 18 mai 2010, *Kennedy c. Royaume-Uni*, ECLI:CE:ECHR:2010:0518JUD002683905, §§ 153-154; 12 janvier 2016, *Szabó et Vissy c. Hongrie*, précité, § 57).

B.55.3. La loi attaquée ne soumet pas elle-même les personnes figurant dans la banque de données commune T.E.R. aux mesures visées en son article 33, § 2. Elle confère toutefois une base légale au traitement, dans cette banque de données commune, de nombreuses données à caractère personnel et informations relatives à ces personnes, à l'insu de celles-ci, à des fins de prévention et de suivi du terrorisme, ainsi qu'à la concertation des acteurs professionnels de la sécurité au sein de la « Task Force locale », sur la base de ces données et informations, en vue de la prise ultérieure éventuelle des mesures précitées à l'égard de ces personnes.

Toute personne figurant dans la banque de donnée commune T.E.R. est considérée comme faisant l'objet d'un suivi par l'OCAM, eu égard aux missions légales de l'OCAM, qui consistent notamment à effectuer une évaluation commune de la menace, conformément à l'article 8 de la loi du 10 juillet 2006 « relative à l'analyse de la menace », et à sa fonction de responsable opérationnel de la banque de données commune T.E.R.

B.55.4. Compte tenu de la marge d'appréciation dont il dispose lorsqu'il met en balance, d'une part, l'intérêt de l'État à protéger la sécurité nationale au moyen de mesures de surveillance secrète et, d'autre part, la gravité de l'ingérence dans l'exercice du droit au respect

de la vie privée, le législateur a pu estimer qu'il était nécessaire que les personnes dont les données à caractère personnel sont traitées dans la banque de données commune T.E.R. ne soient pas informées de ces traitements.

Les personnes qui soupçonnent que des données à caractère personnel ou des informations les concernant font ou ont fait l'objet d'un traitement dans la banque de données commune T.E.R. peuvent s'adresser aux autorités de contrôle, à l'Organe de contrôle de l'information policière et au Comité permanent R, afin de contester d'éventuels traitements illicites de leurs données.

B.55.5. L'arrêt n° 145/2011, précité, (B.86, B.88 et B.92) et l'arrêt de la Cour n° 41/2019 (ECLI:BE:GHCC:2019:ARR.041, B.9-B.16) portent exclusivement sur l'absence d'une notification active *a posteriori* à la personne concernée pour l'informer qu'elle a fait l'objet d'une méthode spécifique ou exceptionnelle de collecte des données au sens des articles 18/4 à 18/8 et 18/11 à 18/17 de la loi organique du 30 novembre 1998.

Il n'est certes pas exclu que les services de renseignement, en tant que services de base, enregistrent dans la banque de données commune T.E.R. des données à caractère personnel et informations relatives à une entité enregistrée dans cette banque de données qu'ils ont obtenues, le cas échéant, au moyen d'une méthode spécifique ou exceptionnelle de collecte de données au sens des articles 18/4 à 18/8 et 18/11 à 18/17 de la loi organique du 30 novembre 1998 (article 14 *juncto* l'article 2, 2°, de la loi attaquée; article 19, alinéa 1er, de la loi organique du 30 novembre 1998). L'absence persistante d'une disposition législative prévoyant une notification active à la personne concernée de ce qu'elle a fait l'objet d'une méthode spécifique ou exceptionnelle de collecte des données dont les résultats sont, le cas échéant, susceptibles d'être enregistrés dans la banque de données commune T.E.R., dès que cette notification peut être donnée sans que le but de la restriction soit compromis, est toutefois imputable à la loi organique du 30 novembre 1998, que le présent recours ne vise pas, et non à la loi attaquée.

B.55.6. Compte tenu des autres garanties contre les abus contenues dans la loi attaquée, et en particulier du contrôle permanent exercé par l'Organe de contrôle de l'information policière

et par le Comité permanent R, l'article 4 de la loi attaquée n'entraîne pas une limitation disproportionnée du droit au respect de la vie privée, du droit à la protection des données à caractère personnel et du droit à un recours effectif.

B.55.7. Le grief des parties requérantes relatif à l'absence d'une notification active n'est pas fondé.

c) L'exercice des droits de la personne concernée par l'intermédiaire des autorités de contrôle

B.56.1. En ce qui concerne le grief relatif à l'exercice des droits de la personne concernée par l'intermédiaire des autorités de contrôle et au droit à un recours effectif, comme il est dit en B.54.2, en vertu de l'article 146, alinéa 1er, précité, de la loi sur la protection des données, les personnes qui soupçonnent que des données à caractère personnel ou des informations les concernant fassent ou aient fait l'objet d'un traitement dans la banque de données commune T.E.R. peuvent s'adresser à l'Organe de contrôle de l'information policière et au Comité permanent R pour exercer les droits visés à l'article 145 de cette loi. Les personnes concernées peuvent dès lors exercer leur droit d'obtenir la rectification ou l'effacement des données inexactes, ainsi que leur droit d'obtenir la vérification du respect des dispositions du sous-titre 3 exclusivement par l'intermédiaire de l'Organe de contrôle de l'information policière et du Comité permanent R.

B.56.2. L'exercice des droits des personnes concernées par l'intermédiaire de la ou des autorités de contrôle compétentes vise à ménager un juste équilibre entre les droits de l'individu et les nécessités de la recherche et de la poursuite des infractions ainsi que de la prévention des atteintes à la sûreté de l'État (voy. *Doc. parl.*, Chambre, 1990-1991, n° 1610/1, p. 19; *Doc. parl.*, Chambre, 2017-2018, DOC 54-3126/001, p. 85). Pour répondre à la requête de la personne concernée, la ou les autorités de contrôle se tournent vers le responsable de traitement compétent en charge du traitement de l'information (*ibid.*, p. 86).

B.56.3. En espèce, l'Organe de contrôle de l'information policière et le Comité permanent R assurent conjointement le contrôle des traitements de données à caractère

personnel et informations réalisés dans la banque de données commune T.E.R. Dans le cadre de l'exercice de leurs missions, ils ont accès à la banque de données commune T.E.R. (droit de lecture) (article 15, alinéa 1er, de la loi attaquée), aux archives de cette banque de données (article 7, § 3, alinéa 4, 4°, de la même loi), aux fiches de renseignement relatives aux entités enregistrées dans la banque de données (article 20 de la même loi), aux listes des communications de cartes d'information à une autorité ou à une institution tierce et aux évaluations y relatives (article 23 de la même loi). Ils peuvent à tout moment émettre les recommandations qu'ils estiment nécessaires pour les traitements réalisés dans la banque de données commune T.E.R. (article 29 de la même loi).

B.56.4. Compte tenu des droits et intérêts fondamentaux en cause, le législateur a pu estimer qu'il était nécessaire que seul le droit de s'adresser sans frais à l'Organe de contrôle de l'information policière et au Comité permanent R afin d'exercer les droits de contrôle visés à l'article 145 de la loi sur la protection des données pouvait être accordé aux personnes dont les données sont traitées dans la banque de données commune T.E.R.

B.56.5. La circonstance que les autorités de contrôle communiquent uniquement à la personne concernée qu'« il a été procédé aux vérifications nécessaires », sans autre précision (article 146, alinéa 2, précité, de la même loi), engendre une limitation du droit de la personne concernée à un recours juridictionnel effectif (dans ce sens, à propos de l'obligation d'information analogue prévue à l'article 17, paragraphe 3, de la directive « police », voy. CJUE, 16 novembre 2023, C-333/22, *Ligue des droits humains ASBL et BA c. Organe de contrôle de l'information policière*, , ECLI:EU:C:2023:874, §§ 60 -61).

B.56.6. Lorsque, d'une part, la protection du droit de la personne concernée à un recours juridictionnel effectif contre la décision de clore le processus de vérification l'exige et que, d'autre part, les objectifs d'intérêt public visés en B.56.2 ne s'y opposent pas, le législateur doit prévoir que l'information de la personne concernée peut aller au-delà des informations prévues à l'article 146, alinéa 2, de la loi sur la protection des données, de manière à lui permettre de défendre ses droits et de décider en pleine connaissance de cause de l'utilité de saisir le juge compétent. De même, le législateur doit, dans la mesure du possible, laisser aux autorités de contrôle compétentes, une certaine marge d'appréciation pour déterminer si les circonstances ne s'opposent pas à ce qu'elles communiquent à cette personne, de manière à tout le moins

succincte, le résultat de leurs vérifications, ainsi que, le cas échéant, les mesures correctrices auxquelles elles ont procédé. Il appartient à ces autorités de contrôle d'engager un dialogue confidentiel avec les responsables du traitement de la banque de données commune T.E.R., ainsi que, le cas échéant, avec ceux des services concernés et, à l'issue de ce dialogue, de décider quelles sont les informations nécessaires à l'exercice, par la personne concernée, de son droit à un recours juridictionnel effectif qu'elle peut communiquer sans compromettre les objectifs d'intérêt public visés en B.56.2 (voy. *ibid.*, §§ 65-66).

Le législateur doit en outre garantir un contrôle juridictionnel effectif tant de l'existence et du bien-fondé des motifs ayant justifié la limitation de ces informations que de l'exécution correcte, par les autorités de contrôle, de leur mission de vérification de la licéité du traitement. Le juge compétent doit pouvoir prendre connaissance tant de l'ensemble des motifs que des éléments de preuve y afférents, sur lesquels les autorités de contrôle ont fondé la vérification de la licéité du traitement de données en cause ainsi que les conclusions qu'elles en ont tirées (voy. *ibid.*, §§ 67-69).

B.56.7. En l'espèce, l'article 146, alinéa 2, de la loi sur la protection des données prévoit que, dans tous les cas, l'Organe de contrôle de l'information policière et le Comité permanent R « communique[nt] uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires ». L'obligation d'information limitée prévue par cette disposition vaut dès lors en toutes circonstances.

Par ailleurs, cette disposition ne prévoit pas que la personne concernée puisse former un recours auprès d'un organe juridictionnel disposant d'une compétence de pleine juridiction contre la décision de ces autorités de contrôle. À cet égard, il découle de l'article 139 de la loi sur la protection des données que ni l'action en cessation devant le président du tribunal de première instance, visée aux articles 209 et suivants de cette loi, ni le recours devant la Cour d'appel contre les décisions de l'Organe de contrôle de l'information policière, visé à l'article 248 de cette même loi, ne sont applicables au traitement de données à caractère personnel dans la banque de données commune T.E.R.

B.56.8. Compte tenu de ce qui est dit en B.56.6, le caractère absolu de l'obligation d'information limitée prévue à l'article 146, alinéa 2, de la loi sur la protection des données et l'absence d'un contrôle juridictionnel effectif de la décision de l'Organe de contrôle de

l'information policière et du Comité permanent R relative à la vérification de la licéité du traitement, portent une atteinte disproportionnée au droit de la personne concernée à un recours juridictionnel effectif.

Il s'ensuit que l'article 4 de la loi attaquée, lu en combinaison avec l'article 146, alinéa 2, de la loi sur la protection des données, doit être annulé (1) en ce qu'il ne prévoit pas que lorsque, d'une part, la protection du droit de la personne concernée à un recours juridictionnel effectif contre la décision de clore le processus de vérification l'exige et que, d'autre part, les objectifs d'intérêt public en cause ne s'y opposent pas, l'information de la personne concernée peut aller au-delà des informations prévues à l'article 146, alinéa 2, de la loi sur la protection des données et (2) en ce qu'il ne prévoit pas que la personne concernée puisse former un recours auprès d'un organe juridictionnel disposant d'une compétence de pleine juridiction contre la décision de l'Organe de contrôle de l'information policière et du Comité permanent R.

B.56.9. Le grief des parties requérantes relatif à l'exercice des droits de la personne concernée par l'intermédiaire des autorités de contrôle est fondé dans la mesure visée en B.56.8.

Quant au deuxième moyen (droit à la liberté d'expression)

B.57. Les parties requérantes prennent le deuxième moyen de la violation, par la loi attaquée, des articles 10, 11 et 22 de la Constitution, lus en combinaison ou non avec l'article 10 de la Convention européenne des droits de l'homme et avec les articles 11 et 52 de la Charte.

B.58. L'article 10 de la Convention européenne des droits de l'homme garantit le droit à la liberté d'expression, qui comprend la liberté de recevoir ou de communiquer des informations ou des idées. L'article 11 de la Charte aussi garantit le droit à la liberté d'expression, qui comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées.

B.59. En l'espèce, l'examen de la loi attaquée au regard des normes de référence précitées ne conduit pas à une autre conclusion que celle qui résulte de l'examen du premier moyen.

Quant au troisième moyen (droits de l'enfant)

B.60. Le troisième moyen est pris de la violation des articles 10, 11, 22 et 22*bis* de la Constitution, lus en combinaison ou non avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 24 et 52 de la Charte et avec les articles 3, 9, 12 et 40, paragraphe 1, de la Convention relative aux droits de l'enfant.

B.61.1. L'article 22*bis*, alinéa 4, de la Constitution, prévoit que, dans toute décision qui le concerne, l'intérêt de l'enfant est pris en considération de manière primordiale. L'article 22*bis*, alinéa 5, de la Constitution donne par ailleurs au législateur la mission de garantir les droits de l'enfant.

B.61.2. L'article 2, paragraphe 2, de la Convention relative aux droits de l'enfant oblige les États parties à prendre « toutes les mesures appropriées pour que l'enfant soit effectivement protégé contre toutes formes de discrimination ou de sanction motivées par la situation juridique, les activités, les opinions déclarées ou les convictions de ses parents [...] ».

L'article 3, paragraphe 1, de la même Convention dispose que « dans toutes les décisions qui concernent les enfants, qu'elles soient le fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale ». L'article 3, paragraphe 2, de la même Convention dispose que « les États parties s'engagent à assurer à l'enfant la protection et les soins nécessaires à son bien-être, compte tenu des droits et des devoirs de ses parents [...], et ils prennent à cette fin toutes les mesures législatives et administratives appropriées ». L'article 3, paragraphe 3, de la même Convention dispose que « les États parties veillent à ce que le fonctionnement des institutions, services et établissements qui ont la charge des enfants et assurent leur protection soit conforme aux normes fixées par les autorités compétentes, particulièrement dans le domaine de la sécurité et de la santé et en ce qui concerne le nombre et la compétence de leur personnel ainsi que l'existence d'un contrôle approprié ».

Les articles 9 et 10 de cette Convention tendent à protéger la vie familiale de l'enfant avec ses parents, en disposant que « les Etats parties veillent à ce que l'enfant ne soit pas séparé de ses parents contre leur gré, à moins que les autorités compétentes ne décident [...] que cette séparation est nécessaire dans l'intérêt supérieur de l'enfant » (article 9) et que « toute demande faite par un enfant ou ses parents en vue d'entrer dans un Etat partie ou de le quitter aux fins de réunification familiale est considérée par les Etats parties dans un esprit positif, avec humanité et diligence » (article 10).

L'article 12 de la même Convention dispose que « les Etats parties garantissent à l'enfant qui est capable de discernement le droit d'exprimer librement son opinion sur toute question l'intéressant, les opinions de l'enfant étant dûment prises en considération eu égard à son âge et à son degré de maturité » (paragraphe 1) et qu'« à cette fin, on donnera notamment à l'enfant la possibilité d'être entendu dans toute procédure judiciaire ou administrative l'intéressant, soit directement, soit par l'intermédiaire d'un représentant ou d'une organisation appropriée, de façon compatible avec les règles de procédure de la législation nationale » (paragraphe 2).

L'article 16 de la même Convention dispose que « nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation » (paragraphe 1) et que « l'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes » (paragraphe 2).

L'article 40, paragraphe 1, de la même Convention dispose que « les Etats parties reconnaissent à tout enfant suspecté, accusé ou convaincu d'infraction à la loi pénale le droit à un traitement qui soit de nature à favoriser son sens de la dignité et de la valeur personnelle, qui renforce son respect pour les droits de l'homme et les libertés fondamentales d'autrui, et qui tienne compte de son âge ainsi que de la nécessité de faciliter sa réintégration dans la société et de lui faire assumer un rôle constructif au sein de celle-ci ». L'article 40, paragraphe 3, a), de la même Convention prévoit que « les États parties s'efforcent de promouvoir l'adoption de lois, de procédures, la mise en place d'autorités et d'institutions spécialement conçues pour les

enfants suspectés, accusés ou convaincus d'infraction à la loi pénale, et en particulier :
a) d'établir un âge minimum au-dessous duquel les enfants seront présumés n'avoir pas la capacité d'enfreindre la loi pénale ».

B.61.3. L'article 22*bis*, alinéa 4, de la Constitution, l'article 3, paragraphe 1, de la Convention relative aux droits de l'enfant et l'article 24, paragraphe 2, de la Charte, dans le champ d'application du droit de l'Union européenne, garantissent des droits fondamentaux analogues.

1. En ce qui concerne les mineurs âgés de douze ans ou plus (article 5 de la loi attaquée)

B.62.1. Selon les parties requérantes, l'article 5 de la loi attaquée est contraire aux normes de référence précitées en ce qu'il prévoit que les mineurs âgés de douze ans ou plus peuvent être enregistrés en tant qu'entités dans la banque de données commune T.E.R.

B.62.2. La critique des parties requérantes est dirigée en particulier contre l'article 5, alinéa 2, 5°, *a)*, de la loi attaquée.

Cette disposition étant indissociablement liée à l'article 2, 4°, et à l'article 6, § 2, alinéa 1er, 1°, 1), et 2°, de la même loi, la Cour examine ces dispositions conjointement.

B.63.1. L'article 2, 4°, de la loi attaquée définit notamment l'« entité » comme étant « toute personne physique majeure ou mineure de douze ans ou plus » qui répond aux critères d'un « foreign terrorist fighter », d'un « homegrown terrorist fighter », d'un extrémiste potentiellement violent, d'une personne condamnée pour terrorisme ou d'un propagandiste de haine (« entité validée ») ou dont il existe des indices sérieux qu'elle puisse relever de l'une de ces catégories (« entité pré-enquête »).

L'article 5, alinéa 2, 5°, de la même loi dispose :

« Les finalités de la banque de données commune T.E.R. sont les suivantes :

[...]

5° l'aide à la protection, à l'accompagnement et au suivi des personnes suivantes :

a) les mineurs de douze ans ou plus qui sont considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine;

b) les enfants mineurs d'un *foreign terrorist fighter* qui répond aux critères visés à l'article 2, 7°, a) ou c), et qui ne sont pas ou ne peuvent pas être considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine ».

L'article 6, § 2, alinéa 1er, 1°, 1), et 2°, de la même loi dispose :

« Les données à caractère personnel traitées dans la banque de données commune T.E.R. sont les données non classifiées au sens de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé suivantes :

1° les données des entités suivantes :

1) Si l'entité est une personne physique majeure ou mineure de douze ans ou plus :

a) les données d'identification suivantes :

i. nom, prénoms, alias;

ii. s'il échet, le numéro d'identification du Registre national des personnes physiques ou du registre des étrangers;

iii. l'adresse;

iv. le sexe et/ou le genre;

v. la date, le lieu et le pays de naissance;

vi. la ou les nationalité(s);

vii. la description physique;

viii. des photos;

ix. s'il échet, la référence dactyloscopique unique;

x. l'état civil;

xi. la situation familiale;

xii. la profession;

xiii. les éléments liés à sa localisation;

xiv. les moyens de communication;

b) les données d'identification visées au point *a)*, i. à v., des enfants mineurs visés à l'article 5, alinéa 2, 5°, *b)*;

c) les données relatives aux catégories particulières de données à caractère personnel suivantes :

i. l'origine ethnique;

ii. les opinions politiques;

iii. les convictions religieuses ou philosophiques;

iv. les données biométriques aux fins d'identifier une personne physique de manière unique;

v. les données concernant la santé;

d) les données relatives aux formations suivies;

e) les données relatives à la situation financière;

f) les données relatives aux fréquentations à risque;

g) les données relatives aux absences de réponse aux convocations de l'autorité;

h) les moyens de [transport].

[...]

2° les données administratives, judiciaires, en ce compris celles sur les faits qualifiés d'infraction, de police judiciaire, de police administrative et les informations relatives aux entités enregistrées, traitées conformément à la loi par les services de base et les services partenaires qui disposent d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R. et qui sont adéquates, pertinentes et non excessives au regard des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2; ».

B.63.2. Il ressort des articles 2, 4°, 5, alinéa 2, 5°, *a)*, et 6, § 2, alinéa 1er, 1°, 1), et 2°, précités, de la loi attaquée que les mineurs âgés de douze ans ou plus sont enregistrés en tant qu'entités dans la banque de données commune T.E.R., et que les données à caractère personnel les concernant (mentionnées à l'article 6, § 2, alinéa 2, précité) y sont traitées, s'ils satisfont aux critères de l'une des cinq catégories d'entités visées dans cette banque de données. Il

s'ensuit que « les mineurs de moins de 12 ans ne sont [...] pas enregistrés comme entité dans la banque de données commune T.E.R. » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 37). Par ailleurs, le fait de ne pas satisfaire à l'un des critères de la définition de l'une des cinq catégories d'entités visées à l'article 2, 7° à 11°, de la loi attaquée suffit pour qu'un mineur âgé de douze ans ou plus ne soit pas enregistré en tant qu'entité dans la banque de données commune T.E.R.

Il ressort également de l'article 5, alinéa 2, 5°, a), de la loi attaquée qu'outre les finalités visées à l'article 5, alinéa 2, 1° à 4° (« la concertation coordonnée entre les services de base et les services partenaires »; « la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des services de base et des services partenaires »; « l'aide à la prise de décisions par les autorités administratives ou à la prise de décisions de police administrative ou judiciaire »; « l'analyse, l'évaluation et le suivi, en ce compris la prise de mesures, des entités validées enregistrées dans la banque de données commune T.E.R., l'analyse, l'évaluation et le suivi des entités en pré-enquête enregistrées dans la banque de données commune T.E.R. et l'analyse, l'évaluation et le suivi du phénomène du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme »), la banque de données commune T.E.R. a également pour finalité d'aider à la protection, à l'accompagnement et au suivi des mineurs âgés de douze ans ou plus qui sont considérés comme des entités.

B.64.1. Le choix de l'âge de douze ans à partir duquel une personne physique peut être enregistrée en tant qu'entité dans la banque de données commune T.E.R. a été justifié par le fait qu'il s'agit « d'un âge pivot repris dans diverses législations » :

« En effet, il s'agit de l'âge à partir duquel des mesures peuvent être prises à l'égard de mineurs suspectés d'avoir commis un fait qualifié infraction. Avant cet âge, on privilégie le renvoi vers l'aide aux mineurs en danger et on ne peut en tout cas pas placer l'enfant sur la base du fait qualifié infraction (art. 37, § 2, de la loi du 8 avril 1965 relative à la protection de la jeunesse, à la prise en charge des mineurs ayant commis un fait qualifié infraction et à la réparation du dommage causé par ce fait).

En ce qui concerne la Flandre, le décret du 15 février 2019 sur le droit en matière de délinquance juvénile est entré en vigueur le 1er septembre 2019. Ce décret introduit une

présomption irréfragable de non-responsabilité pour un mineur de moins de 12 ans qui a commis un délit de mineur. Les faits, actes ou négligences dont cette personne est suspectée peuvent uniquement donner lieu à son renvoi vers les services d'aide à la jeunesse conformément au décret du 12 juillet 2013 relatif à l'aide intégrale à la jeunesse.

En Communauté française aussi l'âge de 12 ans est utilisé comme âge pivot pour prendre des mesures à l'encontre d'un mineur qui a commis des faits qualifiés infractions (FQI). Sauf la réprimande, aucune autre mesure n'est possible pour un mineur FQI de moins de 12 ans. Toutes les mesures (par ex. placement, prestation éducative d'intérêt général, offre restauratrice, ...) ne sont donc uniquement possibles à partir de 12 ans. L'âge de 14 ans est utilisé comme âge pivot pour le placement en IPPJ même si le placement à partir de 12 ans est possible sous certaines conditions (gravement porté atteinte à la vie/santé d'autrui et comportement particulièrement dangereux). (Décret du 18 janvier 2018 de la Communauté française relatif à la prévention, l'aide et la protection de la jeunesse).

Par ailleurs, 12 ans est l'âge à partir duquel un enfant peut être associé dans diverses procédures le concernant. Par [exemple], il doit donner son consentement à son adoption (art. 348-1 du Code civil), il doit être cité à comparaître devant le tribunal de la jeunesse en cas de procédure de mineur en danger ou de mineur poursuivi du chef d'un fait qualifié infraction (art. 46 de la loi du 8 avril 1965 relative à la protection de la jeunesse, à la prise en charge des mineurs ayant commis un fait qualifié infraction et à la réparation du dommage causé par ce fait), ou encore il doit être informé de son droit d'être entendu par le tribunal de la famille dans les procédures relatives à l'autorité parentale (art. 1004/1 du Code judiciaire) » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 38-39).

Ce choix a également été justifié par référence à l'observation générale du Comité des droits de l'enfant du 25 avril 2007 n° 10 (2007) sur « les droits de l'enfant dans le système de justice pour mineurs », aux termes de laquelle il serait « inacceptable sur le plan international de fixer l'âge minimum de la responsabilité pénale en-dessous de 12 ans » (*ibid.*, p. 39).

B.64.2. Au cours des travaux préparatoires, il a été répondu ce qui suit aux avis rendus sur ce point (respectivement les 14 juin, 21 juin et 16 juin 2023) par le délégué général aux droits de l'enfant, par le « Kinderrechtencommissariaat » (Commissariat aux droits de l'enfant) et par l'Autorité de protection des données :

« Le Délégué aux droits de l'enfant et le Commissaire aux droits de l'enfant se sont quant à eux montrés [critiques] sur la possibilité d'enregistrer des enfants de douze ans et plus dans la banque de données commune T.E.R. Il nous semble que ces deux avis abordent la problématique de ces enfants uniquement dans une optique pénale. Or, la banque de données

[commune], dans le cadre de ces enfants, ne s'inscrit pas uniquement dans cette perspective car il y a un aspect administratif et de suivi à prendre en considération également.

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données a également indiqué que ' le traitement des données à caractère personnel des enfants mineurs de certaines entités outrepassa les finalités de l'enregistrement dans une banque de données accessible à des services dont les missions sont autres que celles des services de renseignement ' (§ 105). Il faut néanmoins préciser que le traitement de données de ces enfants n'est pas un traitement ' au cas où ', comme le suggère l'Autorité de protection des données. En effet, ces données sont au contraire utilisées dans l'intérêt de ces mineurs, pour les accompagner dans une démarche préventive. [...]

Pour répondre à ces préoccupations, une nouvelle finalité a été ajoutée à la banque de données commune T.E.R. » (*ibid.*, pp. 39-40).

B.64.3. Lors de l'examen du projet de loi au sein de la commission de la justice de la Chambre, sur la justification de l'enregistrement de mineurs dans la banque de données commune T.E.R., le directeur général de l'OCAM a indiqué :

« Il est justifié du point de vue légal d'enregistrer les mineurs dans la BDC. L'accent est en effet placé sur l'approche protectionnelle, l'accompagnement et le suivi. Les enfants sont dans un premier temps considérés comme vulnérables. Le projet de loi [à] l'examen s'inscrit dans cette philosophie.

À ce jour, la BDC ne comprend que cinq mineurs, principalement âgés de 15 à 17 ans. Ce faible nombre montre que l'OCAM ne procède à l'enregistrement des mineurs dans la BDC que si celui-ci est réellement justifié. Et il y [a] parfois de bonnes raisons : de nombreux jeunes qui n'étaient auparavant pas soupçonnés d'extrémisme ou de radicalisation apparaissent sur les radars. Certains mineurs mettent par ailleurs en place une lourde propagande ou diffusent des contenus très explicites.

[...]

En ce qui concerne les mesures prévues à l'encontre des mineurs pour lesquels les services ont des informations qu'ils ont commis ou ont l'intention de commettre un fait qualifié infraction, la limite d'âge de 12 ans est appliquée. Il s'agit de l'âge à partir duquel un enfant peut en effet être associé à diverses procédures le concernant. La limite d'âge est conforme aux conventions et législations adoptées par les entités fédérées, l'autorité fédérale et les instances internationales.

[...]

[...] Les services de base et les services partenaires pourront en effet demander la réalisation d'une évaluation de la menace et l'insérer dans [le] dossier de la personne concernée, ce qui confèrera un caractère contradictoire à celui-ci. L'échange d'informations avec les centres fermés pour mineurs, entre autres, n'est pas chose aisée. Le projet de loi à l'examen vise à remédier à cette situation » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/002, pp. 17-18).

B.65.1. L'article 40, paragraphe 3, de la Convention relative aux droits de l'enfant implique certes l'obligation d'établir un âge minimal au-dessous duquel les enfants sont présumés n'avoir pas la capacité d'enfreindre la loi pénale, mais sans fixer cet âge.

Toutefois, un traitement de données à caractère personnel dans une banque de données commune, telle que la banque de données commune T.E.R., ne peut être considéré ni comme une incrimination ni comme une peine au sens des articles 12 et 14 de la Constitution, étant donné qu'il constitue seulement une mesure à caractère préventif ou une mesure d'investigation.

En permettant le traitement dans cette banque de données des données à caractère personnel de mineurs, la loi attaquée n'instaure donc pas une incrimination ou une peine qui dérogerait aux dispositions applicables en matière de protection de la jeunesse, lesquelles restent intégralement applicables.

Dans la mesure où l'article 40 de la Convention relative aux droits de l'enfant vise à accorder des droits aux enfants qui font l'objet d'une procédure tendant à les sanctionner pour avoir commis des faits déterminés, cette disposition ne peut dès lors pas s'appliquer en l'espèce. Il en va de même de l'observation générale du Comité des droits de l'enfant du 18 septembre 2019 n° 24 (2019) sur « les droits de l'enfant dans le système de justice pour enfants » qui, comme le soulignent les parties requérantes, remplace l'observation générale n° 10 (2007), précitée, du Comité des droits de l'enfant à laquelle il est fait référence dans les travaux préparatoires et qui, dans son paragraphe 22, encourage les États parties à la Convention à relever l'âge minimum de la responsabilité pénale à quatorze ans au moins.

B.65.2. L'article 22*bis*, alinéa 4, de la Constitution et l'article 3, paragraphe 1, de la Convention relative aux droits de l'enfant n'empêchent pas en soi le législateur de prévoir que des données à caractère personnel de mineurs peuvent être traitées par les services de base et services partenaires, afin de permettre à ceux-ci de remplir leurs missions légales. Ces missions, qui portent notamment sur le maintien de l'ordre public, la protection des personnes et des biens et la prévention et la recherche d'infractions, ne sont pas, par nature, exclusivement liées aux actes et comportements des personnes majeures.

Cependant, lorsqu'il établit les circonstances dans lesquelles des données à caractère personnel peuvent être traitées par les services de base et les services partenaires, le législateur doit tenir compte de la situation particulière des mineurs, notamment en ce qui concerne leur personnalité et leur degré de maturité.

B.66.1. À cet égard, l'ajout, à l'article 5, alinéa 2, de la loi attaquée, d'une cinquième finalité pour la banque de données commune T.E.R. consistant en « l'aide à la protection, à l'accompagnement et au suivi » des mineurs âgés de douze ans ou plus, à la suite des avis précités du délégué général aux droits de l'enfant, du Commissariat aux droits de l'enfant et de l'Autorité de protection des données, vise à respecter l'exigence de protection des mineurs imposée tant par la Constitution que par la Convention relative aux droits de l'enfant. Cette finalité doit être considérée comme primordiale lors du traitement, dans la banque de données commune T.E.R., de données à caractère personnel relatives aux mineurs âgés de douze ans ou plus.

B.66.2. La circonstance que les mineurs âgés de douze ans ou plus sont susceptibles d'être enregistrés en tant qu'entités dans la banque de données commune T.E.R. ne signifie pas qu'ils ne jouissent d'aucune garantie. En effet, les garanties prévues dans la loi attaquée relatives aux circonstances dans lesquelles des données à caractère personnel peuvent être traitées par les services de base et les services partenaires, relatives aux délais de conservation de ces données, à l'accès à ces données et au contrôle permanent sur le traitement de ces données, sont également applicables aux mineurs âgés de douze ans ou plus.

Plusieurs dispositions de la loi attaquée tiennent par ailleurs compte de la situation particulière des mineurs. Premièrement, comme il est dit en B.45.3, après le dernier enregistrement d'une donnée ou information dans la fiche de renseignement de l'entité validée, l'OCAM examine tous les trois ans si les données à caractère personnel relatives à des mineurs conservées dans la banque de données commune T.E.R. présentent toujours un lien direct avec l'une des finalités de celle-ci (tous les cinq ans pour les données relatives à des personnes majeures) (article 7, § 1er, alinéas 2 et 3, de la loi attaquée). Deuxièmement, les données relatives aux mineurs sont conservées de manière active dans la banque de données commune T.E.R. pendant une période de quinze ans maximum (trente ans pour les données relatives à des

personnes majeures) avant d'être archivées pour une durée de maximum trente ans (article 7, § 1er, alinéas 1er et 2, *juncto* le § 3, alinéa 1er). Troisièmement, « la situation de vulnérabilité de la personne concernée, en ce compris la minorité de la personne » est prise en compte lors de l'évaluation préalable à la communication à une autorité ou à une institution tierce de la carte d'information relative à une entité validée (article 23, alinéa 2, 3°) (voy. *Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 37).

En outre, les services de base et les services partenaires ne peuvent, aux termes des articles 14, 16 et 22 de la loi attaquée, traiter des données à caractère personnel dans la banque de données commune T.E.R. que pour autant qu'elles présentent « un caractère non excessif ». L'article 23 de la loi attaquée prévoit que la communication à une autorité ou à une institution tierce de la carte d'information relative à une entité validée ne peut intervenir que moyennant le respect de la même exigence. Lors de l'application de cette condition et du contrôle de cette application, il convient, en ce qui concerne les données des mineurs, de porter une attention particulière au jeune âge des intéressés et à l'incidence du traitement de leurs données à caractère personnel.

B.66.3. Dans leurs avis précités, le délégué général aux droits de l'enfant et le Commissariat aux droits de l'enfant ont relevé le caractère insuffisant des mesures visées en B.66.2 pour garantir un traitement différencié adapté pour les mineurs dans la banque de données commune T.E.R., spécialement en raison de l'absence de formation prévue pour le personnel amené à traiter les données relatives aux mineurs.

Le Commissariat aux droits de l'enfant a notamment relevé :

« Sans qu'une infraction ait été commise (sauf pour les personnes condamnées du chef de terrorisme), les services de base doivent évaluer si un signal donné par un mineur relève bien du terrorisme, de l'extrémisme ou de la radicalisation. Les membres des services de base doivent évaluer si les conceptions radicales et extrêmes de mineurs constituent effectivement une indication grave de menace à la sécurité nationale.

[...]

Ces appréciations nécessitent d'avoir des connaissances en matière de développement et de milieu de vie des mineurs et elles requièrent des définitions claires, précises, prévisibles et propres à l'enfant, sur lesquelles les membres des services de base peuvent se fonder.

[...]

- Si les membres des services de base ne sont pas suffisamment au fait du milieu de vie des enfants et des jeunes et qu'ils manquent de connaissances quant au développement de leur identité et aux différences entre jeunes de douze, treize, quatorze, quinze, seize et dix-sept ans, ces services risquent de trop vite juger et valider les mineurs comme des adultes ou de juger des jeunes de douze, treize ou quatorze ans comme autant responsables que des adultes.

- Si les membres des services de base ne sont pas suffisamment au fait des droits de l'enfant et de la perspective des enfants, ils risquent d'aborder les signaux de terrorisme, d'extrémisme et de radicalisation de manière trop unidimensionnelle. Ils possèdent effectivement une expertise en matière de surveillance de la sécurité nationale et de la sécurité des enfants et des adultes. C'est sur la base de cette expertise et dans le cadre de cette mission qu'ils examinent les signaux, avec pour risque de reléguer au second plan les nuances liées à l'âge des mineurs, au sens donné à leurs actes, à leurs intentions et à leur milieu de vie, ainsi qu'aux différences individuelles entre mineurs, et que des profils spécifiques de personnes susceptibles de menacer la sécurité nationale ressortent. Il est important de continuer à tenir compte des différences individuelles et d'être constamment attentif à la tension qui existe entre la sécurité, l'espace nécessaire au développement de l'identité et les droits de l'enfant » (Commissariat aux droits de l'enfant, avis n° 15/2023 du 21 juin 2023, pp. 9-10; traduction libre).

Bien qu'à la suite de ces avis, le législateur ait indiqué qu'« une telle formation devra être dispensée à l'attention du personnel concerné, notamment auprès du responsable opérationnel » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 37), il n'a toutefois pas adapté le projet de loi en conséquence. En effet, aucune disposition de la loi attaquée ne prévoit que le traitement de données à caractère personnel relatives à des mineurs dans la banque de données commune T.E.R. requiert l'intervention d'au moins un membre du personnel ayant suivi une formation spécifique et/ou disposant d'une expertise pertinente en ce qui concerne la situation psychosociale de mineurs dans le contexte du terrorisme, de l'extrémisme et de la radicalisation. Ainsi, il n'est pas garanti que, lors de l'évaluation visant à déterminer si la situation du mineur présente effectivement des éléments suffisants pour que ce dernier puisse être considéré comme une entité, le développement et le milieu de vie de la catégorie d'âge concernée sont pris en compte.

Partant, le troisième moyen est fondé dans cette mesure.

B.66.4. De surcroît, par son arrêt n° 108/2016 précité, la Cour s'est prononcée sur le traitement de données à caractère personnel relatives à des mineurs dans une banque de données ayant pour finalités la prévention et la sécurité. L'affaire qui est à l'origine de cet arrêt portait sur l'article 44/7, alinéa 2, de la loi sur la fonction de police, qui prévoit que l'enregistrement

des données visées à l'article 44/5, § 3, 1°, de cette loi (« les données relatives aux suspects d'un fait pénal et aux personnes condamnées ») dans la B.N.G. est subordonné à l'autorisation du magistrat compétent lorsqu'il s'agit de données concernant un mineur âgé de moins de quatorze ans. La Cour a jugé que « le législateur pouvait en principe, pour fixer l'âge à partir duquel l'autorisation d'un magistrat est requise pour le traitement de données à caractère personnel dans la B.N.G., s'inspirer de l'âge de quatorze ans fixé dans les lois [...] du 24 juin 2013 [relative aux sanctions administratives communales] et du 21 décembre 1998 [relative à la sécurité lors des matches de football] » (B.153) et que la mesure précitée ne portait pas une atteinte disproportionnée aux droits des mineurs âgés de plus de quatorze ans (B.154).

En l'espèce, le choix de principe de l'âge de douze ans comme l'âge à partir duquel un mineur est susceptible d'être enregistré en tant qu'entité dans la banque de données commune T.E.R. n'est pas déraisonnable, compte tenu des dispositions législatives auxquelles il est fait référence dans les travaux préparatoires cités en B.64.1. Il n'en demeure pas moins que des personnes particulièrement jeunes peuvent de ce fait être reprises dans la banque de données en raison d'indices de terrorisme, d'extrémisme et de radicalisation, y compris, plus spécifiquement, des mineurs de douze et treize ans, qui ne peuvent en principe être sanctionnés pour leurs actes ni pénalement, ni administrativement.

Vu leur irresponsabilité de principe et leur âge particulièrement jeune, le choix précité du législateur produit des effets disproportionnés à l'égard des mineurs de moins de quatorze ans, dès lors que la loi attaquée ne prévoit pas, à l'inverse de l'article 44/7 de la loi sur la fonction de police, l'intervention d'un magistrat indépendant pour que ces mineurs puissent être enregistrés en tant qu'entités dans la banque de données commune T.E.R. La loi n'offre donc pas les garanties nécessaires à la prise en compte de la situation particulière de ces mineurs, notamment en ce qui concerne leur personnalité et leur degré de maturité.

Dans cette mesure également, le troisième moyen est fondé.

B.67. Le troisième moyen, en son premier grief, est fondé dans la mesure indiquée en B.66.3 et en B.66.4. Il convient d'annuler la loi attaquée en ce qu'elle ne prévoit pas que, lors

du traitement de données à caractère personnel relatives à des mineurs dans la banque de données T.E.R., il faut que soit impliquée au moins une personne ayant suivi une formation spécifique et/ou disposant d'une expertise pertinente en ce qui concerne la situation psychosociale de mineurs dans le contexte du terrorisme, de l'extrémisme et de la radicalisation; et en ce qu'elle ne prévoit pas l'intervention d'un magistrat indépendant, lorsque des données à caractère personnel concernant des mineurs âgés de moins de quatorze ans sont enregistrées dans la banque de données commune T.E.R.

2. En ce qui concerne les enfants mineurs d'un « foreign terrorist fighter » (articles 5 et 6 de la loi attaquée)

B.68.1. Selon les parties requérantes, les articles 5 et 6 de la loi attaquée sont contraires aux normes de référence visées au troisième moyen en ce qu'ils prévoient le traitement, dans la base de données commune T.E.R., de données à caractère personnel relatives aux enfants mineurs d'un « foreign terrorist fighter » (combattant terroriste étranger).

B.68.2. La critique des parties requérantes est dirigée en particulier contre l'article 5, alinéa 2, 5°, b), et contre l'article 6, § 2, alinéa 1er, 1°, 1), a), i. à v., et b), de la loi attaquée.

B.69.1. L'article 6, § 2, alinéa 1er, 1°, 1), b), précité, de la loi attaquée dispose que « les données d'identification visées au point a), i. à v. » de cette disposition relatives à « des enfants mineurs visés à l'article 5, alinéa 2, 5°, b) » de la même loi sont traitées dans la banque de données commune T.E.R.

Les données d'identification visées à l'article 6, § 2, alinéa 1er, 1°, 1), a), i. à v., de la loi attaquée sont les « i. nom, prénoms, alias »; « ii. s'il échet, le numéro d'identification du Registre national des personnes physiques ou du registre des étrangers »; « iii. l'adresse »; « iv. le sexe et/ou le genre » et « v. la date, le lieu et le pays de naissance ».

Selon l'article 5, alinéa 2, 5°, b), précité, de la loi attaquée, la banque de données commune T.E.R. a notamment pour finalité l'aide à la protection, à l'accompagnement et au

suivi des « enfants mineurs d'un *foreign terrorist fighter* qui répond aux critères visés à l'article 2, 7°, a) ou c), et qui ne sont pas ou ne peuvent pas être considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine ».

Selon l'article 2, 7°, a) ou c), de la même loi, les « *foreign terrorist fighters* » sont « les personnes physiques résidant en Belgique ou ayant résidé en Belgique, ayant ou non la nationalité belge et qui, dans le but de se rallier à des groupements terroristes ou de leur fournir un soutien actif ou passif, se trouvent dans l'une des situations suivantes : a) elles se sont rendues dans une zone de conflit djihadiste; [...]; c) elles sont en route vers la Belgique ou sont revenues en Belgique après s'être rendues dans une zone de conflit djihadiste ».

Selon l'article 2, 6°, de la même loi, la « zone de conflit djihadiste » est « le territoire en proie à une lutte livrée afin de propager, d'imposer ou de protéger de manière violente une vision de la religion islamique et qui est défini par le Conseil national de sécurité sur proposition du responsable du traitement des données de la banque de données commune T.E.R. sur la base de l'analyse stratégique effectuée par l'Organe de coordination pour l'analyse de la menace ».

B.69.2. Il ressort de ces dispositions que les enfants mineurs, quel que soit leur âge, (1) d'un « *foreign terrorist fighter* » au sens de l'article 2, 7°, a) ou c), précité, de la loi attaquée (*i.e.* le « *foreign terrorist fighter* qui séjourne ou a séjourné en zone de conflit djihadiste », *Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 54) et (2) qui ne satisfont pas eux-mêmes aux critères de l'une des cinq catégories d'entités visées dans la banque de données commune T.E.R. (ci-après : les enfants mineurs d'un *foreign terrorist fighter* qui séjourne ou a séjourné en zone de conflit djihadiste), voient traitées dans la banque de données commune T.E.R. certaines catégories de données d'identification les concernant. Ces enfants ne sont pas enregistrés en tant qu'entités dans cette banque de données.

B.70.1. En ce qu'elles prévoient que les données visées en B.69.1 relatives aux enfants mineurs d'un « *foreign terrorist fighter* » qui séjourne ou a séjourné en zone de conflit djihadiste

peuvent être traitées dans la banque de données commune T.E.R., les dispositions attaquées limitent le droit au respect de la vie privée et familiale et le droit à la protection des données à caractère personnel des enfants concernés. Elles font en outre naître une différence de traitement entre enfants, sur la base de la situation juridique, des activités, des opinions ou des convictions de leurs parents au sens de l'article 2, paragraphe 2, précité, de la Convention relative aux droits de l'enfant, dès lors que les enfants mineurs d'un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit djihadiste voient des données à caractère personnel les concernant traitées dans la banque de données commune T.E.R., contrairement aux enfants mineurs dont aucun des parents n'est enregistré dans cette banque de données en tant que « foreign terrorist fighter » séjournant ou ayant séjourné en zone de conflit djihadiste.

B.70.2. Les travaux préparatoires mentionnent :

« En ce qui concerne la seconde [catégorie] de mineurs: seront [concernées] ici, les données relatives au nom, prénom, date de naissance et genre des enfants mineurs, biologiques ou adoptés d'un parent, personne physique qui est enregistré dans la banque de données commune T.E.R. comme *foreign terrorist fighter* qui séjourne ou a séjourné en zone de conflit djihadiste. Il ne s'agit ni de les reprendre dans la banque de données commune T.E.R. comme ' entités ' en tant que telles (ils ne sont donc pas repris à titre principal) ni d'enregistrer les enfants de toutes les entités enregistrées mais uniquement ceux qui séjournent ou ont [séjourné] en zone de conflit djihadiste. Ceci pour pouvoir mettre en place les mesures de protection et de suivi les plus appropriées en cas de retour.

L'objectif est d'une part de pouvoir avoir un aperçu le plus précis possible des enfants qui sont sur zones de combat djihadiste. En effet, la plupart de ces enfants sont nés sur zone et ne sont pas repris dans le registre national. Il est donc important de pouvoir disposer d'informations quant à leur existence et [au] lien avec un parent repris dans la banque de données commune T.E.R. comme entité ayant rejoint une organisation terroriste sur une zone de combat djihadiste.

Et, d'autre part, lors de leur retour, il est nécessaire de disposer des informations quant au lien qui existe avec un adulte dans le cadre du suivi socio-préventif de ses enfants. Par exemple, un[e] fois de retour de zone de combat djihadiste avec leur mère, lorsque celle-ci ira en prison, l'enfant sera pris en charge par des instances de protection de la jeunesse dans le cadre de sa protection et les mesures quant au suivi de sa santé, de son environnement de vie devront être prises. Et lors de la sortie de prison de la mère, il est important d'assurer un lien quant à l'évolution de la mère et de l'enfant. Ceci se fait en CSIL-R, plateforme socio-préventive créée

par la loi du 30 juillet 2018. Mais ici aussi, il est important de savoir que la mère [a] des enfants pour mettre en place les mesures et actions de réintégration respective.

Par ailleurs, les enfants de cette deuxième catégorie n'apparaissent pas dans la banque de données commune T.E.R. si leur nom est introduit. Comme explicité ci-avant, ils ne sont pas soumis au même suivi qu'une entité enregistrée en tant que telle. Ils sont également considérés comme des enfants en danger.

Ce n'est donc que dans les deux cas spécifiques précités (enfant d'un [*foreign terrorist fighter*] catégorie 1 ou catégorie 3) qu'un enfant est traité dans les données relatives à son parent, pour une finalité de protection, de suivi et de réintégration » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, pp. 54-55; voy. aussi DOC 55-3692/002, pp. 12-13).

« [...] [les données relatives aux enfants mineurs de certaines entités] sont [...] utilisées dans l'intérêt de ces mineurs, pour les accompagner dans une démarche préventive. À titre d'exemple, un enfant d'une entité avait été placé dans une école où le risque de radicalisation était très élevé. L'*information officer* est intervenu pour qu'il fréquente un autre établissement scolaire et ce, dans l'intérêt de cet enfant » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 40).

« En ce qui concerne les enfants de [*foreign terrorist fighters*] sur zones, seules des sources sur place permettent de déterminer leur existence. Étant donné que beaucoup de ces jeunes sont nés sur le [territoire] de l'ancien État islamique, ils n'ont pas d'acte de naissance.

L'objectif est d'accueillir le mieux possible les mineurs lors de leur retour en Belgique. Après ce retour, leurs parents sont en effet incarcérés pendant un certain temps. Les services doivent dès lors connaître l'âge des enfants, l'identité de leur famille, leur sexe, etc.

Si les parents sont enregistrés dans la BDC, on y ajoute le nom des enfants afin de préparer l'accueil de ces derniers. Il n'est pas possible d'effectuer directement des recherches dans la BDC à partir du nom des enfants. Ceux-ci ne sont donc pas enregistrés comme une entité dans la banque de données. [La] radiation du nom des parents de la BDC s'accompagne de la suppression de toute trace des enfants.

[...]

[...] L'OCAM pourra anticiper le retour de la famille en Belgique en informant les services concernés. L'OCAM effectuera une évaluation de la menace des parents, recueillera des informations contextuelles relatives aux enfants et les transmettra au magistrat de la jeunesse, lequel prévoira un trajet d'accompagnement et d'accueil tout en tenant compte de l'incarcération des parents » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/002, pp. 17-18).

B.70.3. Il ressort des travaux préparatoires précités que le traitement, dans la banque de données commune T.E.R., des données à caractère personnel visées en B.69.1 relatives aux enfants mineurs d'un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit

djihadiste vise à identifier les enfants qui se trouvent dans une zone de conflit djihadiste et à préparer leur retour en Belgique. Il ressort par ailleurs des mêmes travaux préparatoires et du fait que les enfants d'un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit djihadiste ne sont pas enregistrés eux-mêmes en tant qu'entités dans la banque de données commune T.E.R., que le traitement, dans cette banque de données, des données relatives à ces enfants est effectué uniquement dans une approche protectionnelle. Ainsi, pour cette catégorie de mineurs, les traitements effectués dans la banque de données commune T.E.R. ont pour seule finalité celle qui est mentionnée à l'article 5, alinéa 2, 5°, de la loi attaquée, c'est-à-dire l'aide à la protection, à l'accompagnement et au suivi de ces mineurs.

Conformément au principe de finalité, le traitement dans la banque de données commune T.E.R. de données relatives aux enfants d'un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit djihadiste est dès lors autorisé, d'une part, dans le but d'identifier les enfants qui se trouvent dans une zone de conflit djihadiste et de préparer leur retour en Belgique et, d'autre part, dans le but d'offrir à ces enfants un suivi protectionnel adéquat une fois de retour en Belgique.

Ces objectifs sont légitimes.

B.70.4. En vertu de l'article 2, 3°, 1), et de l'article 16, alinéa 1er, de la loi attaquée, l'administration générale des maisons de justice de la Communauté Française, le département Maison de justice du ministère de la Communauté germanophone, l'agence flamande pour la Justice et le Maintien, l'administration générale de l'Aide à la Jeunesse de la Communauté française, le département Aide à la jeunesse de la Communauté Germanophone et l'agence flamande « Opgroeien », disposent, en tant que services partenaires, d'un droit d'accès à la banque de données commune T.E.R. « dans le cadre de leurs missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions ». Il appartient au Roi de déterminer, pour chaque service partenaire, le type de droit d'accès à la banque de données commune T.E.R. et ses modalités d'exercice (article 16, alinéa 2, de la loi attaquée). Selon l'article 4, § 3, de l'arrêté royal du 14 juillet 2024, les services précités disposent d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R.

À ce propos, les travaux préparatoires de la loi attaquée mentionnent :

« En ce qui concerne particulièrement le suivi réalisé par les Maisons de Justice et les autres agences et services visés à l'article 2, 3°, point 1), dans le cadre de leurs missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions, celui-ci est limité aux personnes pour lesquelles ces services partenaires ont reçu une mission sous la forme d'un mandat de suivi par une instance habilitée par ou en vertu d'une loi, d'un décret ou d'une ordonnance, ou sur la base d'un accord de coopération. Pour cibler ces personnes connues dans la banque de données commune T.E.R. et qui doivent être suivies par les maisons de justice et les agences et services précités, il est nécessaire de comparer les personnes qui sont dans la banque de données commune T.E.R. avec les personnes pour lesquelles elles ont reçu un mandat de suivi » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 19).

Étant donné que les services précités ne peuvent être considérés comme services partenaires que « dans le cadre de leurs missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions », leurs droits d'accès ne peuvent pas concerner le suivi, en vue de leur protection, des enfants d'un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit djihadiste, dès lors que ces enfants ne sont pas auteurs de faits qualifiés infractions.

B.70.5. Le traitement critiqué de données à caractère personnel est en principe pertinent et proportionné au regard de l'objectif précité d'identifier les enfants qui se trouvent dans une zone de conflit djihadiste et de préparer leur retour en Belgique. Comme il ressort de ce qui est dit en B.69.1, ce traitement porte en effet uniquement sur un nombre limité de données d'identification, à savoir les données visées à l'article 6, § 2, 1°, 1), a), i. à v., de la loi attaquée. Il s'agit des nom, prénoms et alias (i.), du numéro d'identification du Registre national des personnes physiques ou du registre des étrangers (ii.), de l'adresse (iii.), du sexe et/ou du genre (iv.), et de la date, du lieu et du pays de naissance (v.). En revanche, aucune donnée d'identification n'est traitée en ce qui concerne, notamment, la description physique (vii.), des photos (viii.), les éléments liés à la localisation (xiii) ou les moyens de communication (xiv.) du mineur concerné, pas plus que les catégories particulières de données à caractère personnel visées à l'article 6, § 2, 1°, 1), c), de la loi attaquée. Les données à caractère personnel traitées ne dévoilent donc la vie privée du mineur concerné que de manière très limitée. Le traitement de ces données peut être considéré comme ne dépassant pas ce qui est strictement nécessaire pour connaître l'existence de l'enfant et son lien avec le « foreign terrorist fighter », afin qu'il

puisse être identifié en vue de sa protection et de son suivi éventuels en Belgique. De plus, les mineurs ne sont pas eux-mêmes enregistrés dans la banque de données commune T.E.R. en tant qu'entités, ce qui implique que leurs données ne s'affichent pas si une recherche est effectuée directement à partir de leur nom, ainsi qu'il ressort également des travaux préparatoires mentionnés en B.70.2. Le traitement des données en lien avec l'enfant dépend toujours de l'enregistrement du parent en tant qu'entité dans la banque de données et en est tributaire.

L'objectif poursuivi ne saurait toutefois justifier que, dès le retour en Belgique des enfants mineurs d'un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit djihadiste, les données de ces enfants puissent encore être accessibles pour des services autres que les services compétents pour leur suivi et leur protection. Une possibilité d'accès plus étendue va au-delà de ce qui est nécessaire pour réaliser l'objectif précité et porte dès lors une atteinte disproportionnée au droit au respect de la vie privée et au droit à la protection des données à caractère personnel des mineurs concernés.

Il appartient au législateur de limiter le droit d'accès aux données de la banque de données commune T.E.R. relatives aux enfants mineurs d'un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit djihadiste, après le retour de ces enfants en Belgique, aux services précités, en particulier aux services communautaires compétents en matière de protection de la jeunesse.

B.70.6. Par ailleurs, en ce qui concerne l'articulation entre les deux catégories de mineurs dont des données sont traitées dans la banque de données commune T.E.R. (d'une part, les mineurs âgés de douze ans ou plus enregistrés en tant qu'entités et, d'autre part, les enfants mineurs d'un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit djihadiste), les travaux préparatoires précisent en outre :

« Dans le cadre du phénomène de terrorisme et d'extrémisme, en ce compris le processus de radicalisation, des dossiers judiciaires et des suivis [Task Force locale] portent sur des mineurs concernés par des infractions terroristes. Qu'il s'agisse de mineurs emmenés par leurs parents sur zone de conflit djihadiste en vue d'intégrer une organisation terroriste, ou de mineurs ayant eux-mêmes adhéré à des idéologies extrémistes, en Belgique, le fait de pouvoir agir dans cette phase de vie où un système protectionnel existe est important pour intervenir le

plus tôt possible. Et compte tenu de ce suivi multidisciplinaire, les mesures les plus appropriées pourront être prises dans l'intérêt du jeune et de la société.

Certainement dans le cadre des mineurs qui ont été emmenés par un ou ses parent(s) alors qu'ils avaient moins de 12 ans, il est important de pouvoir les considérer comme entité à partir de 12 ans – au même titre que les autres catégories – pour déterminer leur évolution idéologique sur zone et [au contact] de personnes extrémistes. Les groupements terroristes utilisent aussi des mineurs et parce qu'ils ont grandi et évolué dans cet environnement, on ne peut pas exclure qu'ils peuvent représenter un danger. Le suivi à part entière – c'est-à-dire repris comme entité de la banque de données commune T.E.R. – est donc primordial par principe de précaution que ce soit pour le mineur ou la société.

Et s'ils devaient revenir en Belgique, cette prise en considération dans la banque de données commune T.E.R. et son évaluation de la menace (qui prend en compte les informations à charge et à décharge liées à [l'idéologie], les intentions, le contexte social, les éventuelles formations ou actions menées sur zones, la problématique psychique) permettront de prendre les mesures adéquates pour accompagner ces mineurs dans le meilleur environnement possible compte tenu de [leur] situation spécifique » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/001, p. 53).

Et :

« [Le directeur général de l'OCAM] souligne que les enfants ne sont enregistrés dans aucune base de données, si ce n'est [dans la banque de données commune T.E.R.] dans la fiche de leurs parents s'ils ont moins de 12 ans ou comme entités s'ils ont 12 ans et plus » (*Doc. parl.*, Chambre, 2023-2024, DOC 55-3692/002, p. 18).

Comme il est dit en B.63.2, il ressort des termes clairs de l'article 2, 4°, de l'article 5, alinéa 2, 5°, a), et de l'article 6, § 2, alinéa 1er, 1°, 1), et 2°, précités, de la loi attaquée qu'un mineur ne peut être enregistré en tant qu'entité dans la banque de données commune T.E.R. que s'il satisfait à la double condition, d'une part, d'avoir atteint l'âge de douze ans et, d'autre part, de répondre à l'ensemble des critères de la définition de l'une des cinq catégories d'entités visées à l'article 2, 7° à 11°, de la loi attaquée. Il en résulte que, contrairement à ce que les extraits précités des travaux préparatoires pourraient laisser entendre, l'enfant mineur d'un « foreign terrorist fighter » qui a été emmené en zone de conflit djihadiste alors qu'il avait moins de douze ans n'est pas automatiquement enregistré en tant qu'entité dans la banque de données commune T.E.R., à partir du jour où il atteint l'âge de douze ans et sur la seule base de ce fait. Cet enfant n'est susceptible d'être enregistré en tant qu'entité dans cette banque de données que s'il répond lui-même à l'ensemble des critères de la définition de l'une des catégories d'entités visées à l'article 2, 7° à 11°, de la loi attaquée.

B.71. Le troisième moyen, en son second grief, est fondé dans la mesure indiquée en B.70.5. Il y a lieu d'annuler la loi attaquée, en ce qu'elle ne limite pas le droit d'accès aux données de la banque de données commune T.E.R. relatives aux enfants mineurs d'un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit djihadiste, après le retour de ces enfants en Belgique, aux services compétents pour le suivi et la protection de ces enfants, en particulier les services communautaires compétents en matière de protection de la jeunesse.

Pour le surplus, sous réserve de l'interprétation mentionnée en B.70.6, le troisième moyen, en son second grief, n'est pas fondé.

Par ces motifs,

la Cour

1. annule :

- la loi du 29 mars 2024 « portant création de la banque de données commune ‘ Terrorisme, Extrémisme, processus de Radicalisation ’ (‘ T.E.R. ’) et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police »,

a. en ce qu’elle ne prévoit pas que, lors du traitement de données à caractère personnel relatives à des mineurs dans la banque de données T.E.R., il faut que soit impliqué au moins un membre du personnel ayant suivi une formation spécifique et/ou disposant d’une expertise pertinente en ce qui concerne la situation psychosociale de mineurs dans le contexte du terrorisme, de l’extrémisme et de la radicalisation;

b. en ce qu’elle ne prévoit pas l’intervention d’un magistrat indépendant lorsque des données à caractère personnel concernant des mineurs âgés de moins de quatorze ans sont enregistrées dans la banque de données commune T.E.R.;

c. en ce qu’elle ne limite pas le droit d’accès aux données de la banque de données commune T.E.R. relatives aux enfants mineurs d’un « foreign terrorist fighter » qui séjourne ou a séjourné en zone de conflit djihadiste, après leur retour en Belgique, aux services compétents pour le suivi et la protection de ces enfants, en particulier aux services communautaires compétents en matière de protection de la jeunesse;

- l’article 4 de la même loi,

a. en ce qu’il ne prévoit pas que, lorsque, d’une part, la protection du droit à un recours juridictionnel effectif de la personne concernée contre la décision de clore le processus de

vérification l'exige et que, d'autre part, les objectifs d'intérêt public en cause ne s'y opposent pas, l'information de la personne concernée peut aller au-delà des informations prévues à l'article 146, alinéa 2, de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel »;

b. en ce qu'il ne prévoit pas que la personne concernée puisse former un recours auprès d'un organe juridictionnel disposant d'une compétence de pleine juridiction contre la décision de l'Organe de contrôle de l'information policière et du Comité permanent R;

2. sous réserve des interprétations mentionnées en B.47.5 et B.70.6 et compte tenu de ce qui est dit en B.22.5, rejette le recours pour le surplus.

Ainsi rendu en langue française, en langue néerlandaise et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 12 mars 2026.

Le greffier,

Le président,

Nicolas Dupont

Pierre Nihoul