



CONSEIL D'ÉTAT
section de législation

avis 73.442/2
du 7 juin 2023

sur

un avant-projet de loi ‘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’

RAAD VAN STATE
afdeling Wetgeving

advies 73.442/2
van 7 juni 2023

over

een voorontwerp van wet ‘tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidszellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt’

Le 12 avril 2023, le Conseil d'État, section de législation, a été invité par le Vice-Premier Ministre et Ministre de la Justice et de la Mer du Nord à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi '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'.

L'avant-projet a été examiné par la deuxième chambre le 7 juin 2023. La chambre était composée de Pierre VANDERNOOT, président de chambre, Patrick RONVAUX et Christine HOREVOETS, conseillers d'État, Sébastien VAN DROOGHENBROECK, assesseur, et Esther CONTI, greffier assumé.

Le rapport a été présenté par Véronique SCHMITZ, premier auditeur.

La concordance entre la version française et la version néerlandaise de l'avis a été vérifiée sous le contrôle de Pierre VANDERNOOT.

L'avis, dont le texte suit, a été donné le 7 juin 2023.

*

Op 12 april 2023 is de Raad van State, afdeling Wetgeving, door de Vice-eersteminister en Minister van Justitie en Noordzee verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt'.

Het voorontwerp is door de tweede kamer onderzocht op 7 juni 2023. De kamer was samengesteld uit Pierre VANDERNOOT, kamervoorzitter, Patrick RONVAUX en Christine HOREVOETS, staatsraden, Sébastien VAN DROOGHENBROECK, assessor, en Esther CONTI, toegevoegd griffier.

Het verslag is uitgebracht door Véronique SCHMITZ, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre VANDERNOOT.

Het advies, waarvan de tekst hierna volgt, is gegeven op 7 juni 2023.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1^{er}, alinéa 1^{er}, 2^o, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet[‡], à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

FORMALITÉS PRÉALABLES

Même si, depuis la modification des lois coordonnées 'sur le Conseil d'État' par la loi du 2 avril 2003 'modifiant certains aspects de la législation relative à l'organisation et au fonctionnement de la section de législation du Conseil d'État', le non-accomplissement des formalités ne peut plus conduire à l'irrecevabilité des demandes d'avis, il n'en reste pas moins qu'en principe la section de législation ne peut être consultée qu'à l'issue des différentes étapes de la préparation administrative de l'avant-projet concerné et après que l'organe compétent pour l'établissement de celui-ci a eu la possibilité de l'adapter éventuellement à la lumière des éléments recueillis lors de l'accomplissement des formalités. Il serait ainsi évité que le Conseil d'État donne son avis sur un projet de texte non définitif et il serait garanti que l'avis soit rendu sur la base d'une information complète concernant tous les éléments pertinents en cause¹.

Cette observation s'applique *a fortiori* pour l'avis de l'Organe de Contrôle de l'Information Policière (ci-après : « le C.O.C. ») lorsqu'il s'agit d'avant-projets qui, comme celui à l'examen, concernent par excellence le traitement de données à caractère personnel, l'obligation consultative ayant précisément pour objectif de vérifier notamment si le régime en projet est bien conforme aux exigences juridiques imposées en matière de traitement de données à caractère personnel². Il en va de même pour l'avis de l'Autorité de protection des données (ci-après : « l'A.P.D. »), également requis. Dans la lettre de demande d'avis, il est par ailleurs mentionné que d'autres avis ont été sollicités mais ceux-ci n'ont pas été transmis à la section de législation du Conseil d'État : il s'agit des avis du Collège des Procureurs généraux, de l'Ordre des médecins et des délégués généraux aux droits de l'enfant.

Il ressort des mesures d'instruction prises par l'auditeur-rapporteur que ces avis n'ont pas encore été donnés.

[‡] S'agissant d'un avant-projet de loi, on entend par « fondement juridique » la conformité aux normes supérieures.

¹ Avis 41.417/AG à 41.420/AG donné le 6 octobre 2006 sur des avant-projets devenus respectivement la loi du 10 mai 2007 'modifiant la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme et la xénophobie', la loi du 10 mai 2007 'tendant à lutter contre la discrimination entre les femmes et les hommes', la loi du 10 mai 2007 'tendant à lutter contre certaines formes de discrimination' et la loi du 10 mai 2007 'adaptant le Code judiciaire à la législation tendant à lutter contre les discriminations et réprimant certains actes inspirés par le racisme ou la xénophobie' (Doc. parl., Chambre, 2006-2007, n° 51-2720/001, p. 126).

² En ce sens également, l'avis 69.369/1 donné le 4 juin 2021 sur un avant-projet devenu l'ordonnance de la Commission communautaire commune du 27 janvier 2022 'modifiant l'ordonnance du 11 mai 2017 concernant le parcours d'accueil des primo-arrivants' (Doc. parl., Parl. Rég. Brux.-Cap., 2021-2022, n° B-87/1, pp. 9 et s.).

La méthode consistant à saisir simultanément la section de législation du Conseil d'État, le C.O.C. et l'A.P.D. est donc, en l'espèce, particulièrement critiquable³. Elle ne permet en effet pas à la section de législation de disposer de l'ensemble des informations pertinentes pouvant être utiles à son examen, plus précisément sur la manière dont il aurait été tenu compte de ces avis et dont cette prise en compte aurait été traduite dans l'exposé des motifs et dans le commentaire des articles.

En tout état de cause, l'exposé des motifs doit fournir des éclaircissements quant à la manière dont les avis du C.O.C. et de l'A.P.D. auront été pris en compte par l'avant-projet.

Enfin, si l'examen par l'auteur de l'avant-projet de ces avis devait encore donner lieu à des modifications du texte soumis au Conseil d'État sur des points autres que de pure forme ou ne résultant pas également des suites réservées au présent avis, les dispositions modifiées ou ajoutées devraient être soumises à nouveau à l'avis de la section de législation conformément à l'article 3, § 1^{er}, alinéa 1^{er}, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973.

OBSERVATIONS PRÉALABLES SUR LA PORTÉE DE L'EXAMEN DE L'AVANT-PROJET

1. La lettre de demande d'avis est rédigée de la manière suivante :

« Le projet de loi que je sou mets à votre avis vise tout d'abord à transposer dans une loi autonome les dispositions relatives aux banques de données communes qui sont actuellement décrites à la sous-section 7bis 'Des banques de données communes' de la loi du 5 août 1992 sur la fonction de police et dans les arrêtés royaux du 21 juillet 2016 relatif à la banque de données communes 'Terrorist Fighters' et du 23 avril 2018 relatif à la banque de données commune 'Propagandistes de haine'.

Ce projet de loi est d'un part constitué de dispositions transférées sans modification de fond de la loi sur la fonction de police, ainsi que des [arrêtés royaux] 'Terrorist Fighters' et 'Propagandistes de haine'.

D'autre part, ce projet apporte des définitions et des précisions sur la notion d'entité enregistrée dans la banque de données commune (BDC) T.E.R., précise les différents types de supports d'extraits de données contenues dans la BDC T.E.R., précise les règles liées aux traitements de données des mineurs, énumère les catégories de données à caractère personnel qui peuvent être traitées dans la BDC TER, permet la communication de données enregistrées dans la BDC TER aux professionnels des soins de santé, prévoit que l'analyse de la menace d'une entité devra être mise à jour au moins deux fois par an, permet l'interconnexion de la banque de données commune avec d'autres banques de données et précise le fonctionnement des local task forces.

Ensuite, la loi cadre en matière de protection des données (loi du 30 juillet 2018) a été modifiée pour donner un traitement juridique clair aux données à caractère personnel concaténées par différents services au sein d'une même banque de données.

³ Voir en ce sens notamment l'avis 71.258/2 donné le 4 mai 2022 sur un avant-projet devenu la loi du 16 octobre 2022 'visant la création du Registre central pour les décisions de l'ordre judiciaire et relative à la publication des jugements et modifiant la procédure d'assises relative à la récusation des jurés', observation préalable n° 2 (*Doc. parl.*, Chambre, 2021-2022, n° 55-2754/001, pp. 68 et s.). Voir également l'avis 72.873/2 donné le 15 mai 2023 sur un avant-projet de loi 'modifiant la loi sur la fonction de police' (non publié à la date à laquelle le présent avis est donné).

Enfin, la loi sur la fonction de police a également été adaptée afin de donner une assise juridique claire à la coopération et la communication de données entre les différents services (services de police, services d'urgence et de secours et services de la santé) qui doivent intervenir en réponse à des incidents mineurs ou majeurs et, en particulier, à garantir l'intégrité physique et psychologique de la personne concernée elle-même et de toute personne susceptible d'entrer en contact avec elle dans le cadre de l'intervention des services précités et la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme, a été légèrement adaptée purement pour des questions de forme et de renvoi.

Le projet d'arrêté royal quant à lui rassemble dans un seul instrument plusieurs arrêtés royaux qui étaient relatifs à la banque de données commune et les rassemble dans un seul instrument ».

L'exposé des motifs explique que sont rassemblées au niveau législatif dans un texte autonome les dispositions légales et réglementaires existantes pour donner une base juridique *ad hoc* à la banque de données commune T.E.R., qui est commune à différents services et qui n'avait donc pas de raison spécifique d'être attachée à la loi du 5 août 1992 'sur la fonction de police', mais aussi parce que, « dans un souci d'une plus grande sécurité juridique, bon nombre de dispositions jugées essentielles qui se trouvaient énoncées dans les arrêtés royaux créant les banques de données '*Terrorist Fighters*' et '*Propagandistes de haine*' ont été ramenées au niveau de la loi ».

Techniquement, il ressort du commentaire de l'article 2 que la banque de données commune T.E.R. correspond à l'actuelle banque de données commune « *Terrorist fighters* » et « *Propagandistes de haine* »⁴ car, « dans les faits, au niveau informatique [...], il existe une seule et même banque de données commune pour toutes les catégories de personnes et entités listées dans les arrêtés royaux du 21 juillet 2016 et du 23 avril 2018 précités »⁵.

2. Il en résulte que, pour les dispositions qui sont reproduites des textes existants sans modification de fond⁶⁻⁷ tout en précisant la nouvelle appellation de la banque de données commune « T.E.R. », il est renvoyé aux avis qui ont été donnés par la section de législation sur ces dispositions.

⁴ Voir, dans le commentaire de l'article 2, le point 6), « Banque de données commune T.E.R. ».

⁵ Exposé des motifs et commentaire de l'article 3.

⁶ L'exposé des motifs comporte des explications à cet égard.

⁷ Les articles 51 et 52 de l'avant-projet ont pour objet, par voie de conséquence, d'abroger respectivement l'article 44/2, § 2, de la loi du 5 août 1992 'sur la fonction de police', inséré par la loi du 27 avril 2016 'relative à des mesures complémentaires en matière de lutte contre le terrorisme', et, dans le chapitre IV, section 12, de la loi du 5 août 1992, la sous-section 7bis, comportant les articles 44/11/3bis à 44/11/3quinquies/2, insérée par la loi du 27 avril 2016 et modifiée par la loi du 22 mai 2019 'modifiant diverses dispositions en ce qui concerne la gestion de l'information policière'.

Pour les dispositions relatives à la loi du 5 août 1992 ‘sur la fonction de police’ et à ses arrêtés d’exécution, il s’agit principalement des avis 58.729/AG donné le 26 janvier 2016 sur un avant-projet devenu la loi du 27 avril 2016 ‘relative à des mesures complémentaires en matière de lutte contre le terrorisme’⁸, 59.515/2 donné le 6 juillet 2016 sur un projet devenu l’arrêté royal du 21 juillet 2016 ‘relatif à la banque de données commune *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’, 62.629/2 et 62.630/2 donnés le 31 janvier 2018 sur deux projets devenus respectivement 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* 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 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 66.662/2 donné le 25 novembre 2019 sur un projet devenu l’arrêté royal du 20 décembre 2019 ‘modifiant l’arrêté royal du 21 juillet 2016 relatif [à] la banque de donn[ée]s 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’. Pour les dispositions 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 sont complétées ou auxquelles il est renvoyé, il s’agit de l’avis 63.192/2 donné le 19 avril 2018 sur un avant-projet devenu cette loi précitée⁹⁻¹⁰. Il en va de même pour l’avis 63.480/2 donné le 6 juin 2018 sur un avant-projet devenu la loi du 30 juillet 2018 ‘portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme’¹¹⁻¹².

Le tableau de correspondance des articles, l’exposé des motifs et le commentaire des articles seront complétés par la référence aux avis précités.

3. Un projet d’arrêté royal ‘relatif à la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »)’ a été soumis à l’avis de la section de législation concomitamment à l’avant-projet de loi à l’examen.

⁸ *Doc. parl.*, Chambre, 2015-2016, n° 54-1727/001, pp. 89 et s.

⁹ *Doc. parl.*, Chambre, 2017-2018, n° 54-3126/001, pp. 402 et s.

¹⁰ Les articles 34 à 49 complètent, pour la banque de données commune T.E.R., les dispositions existantes de la loi du 30 juillet 2018 ‘relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel’.

¹¹ *Doc. parl.*, Chambre, 2017-2018, n° 54-3209/001, pp. 14 et s.

¹² L’article 50 a pour seul objet d’adapter les renvois contenus dans l’article 4 de la loi du 30 juillet 2018 ‘portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme’.

L'avis 73.443/2 du 3 mai 2023 a déclaré cette demande d'avis prématurée au motif que le projet d'arrêté royal se donnait pour fondement légal des dispositions législatives figurant dans l'avant-projet faisant l'objet du présent avis, par hypothèse non encore adoptées ¹³.

En raison de la conception d'un nouveau texte législatif autonome rassemblant des dispositions légales et réglementaires existantes, il convient de prévoir que les dispositions qui sont issues des arrêtés royaux du 21 juillet 2016 'relatif à la banque de données communes « *Terrorist Fighters* »' ¹⁴ et 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' seront abrogées à la même date que la date d'entrée en vigueur de l'avant-projet.

OBSERVATIONS GÉNÉRALES

I. QUANT AU CADRE GÉNÉRAL RELATIF À L'ADMISSIBILITÉ DE RESTRICTIONS AUX DROITS ET LIBERTÉS FONDÉES SUR LA LUTTE CONTRE LE TERRORISME

La banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») implique des restrictions au droit au respect à la vie privée garanti par l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme.

Dans son avis 58.729/AG donné le 26 janvier 2016 sur un avant-projet devenu la loi du 27 avril 2016 'relative à des mesures complémentaires en matière de lutte contre le terrorisme', la section de législation a rappelé ce qui suit :

« La lutte contre le terrorisme fait incontestablement partie des motifs légitimes pouvant justifier des restrictions à ces libertés.

Ainsi, appelée à examiner les restrictions apportées aux droits de l'homme sur cette base, la Cour européenne des droits de l'homme

'rappelle qu'elle est pleinement consciente des difficultés que les États rencontrent pour protéger leur population contre la violence terroriste, laquelle constitue en elle-même une grave menace pour les droits de l'homme. Elle se garde donc de sous-estimer l'ampleur du danger que représente le terrorisme et la menace qu'il fait peser sur la collectivité (*Othman(Abu Qatada) c. Royaume-Uni*, n° 8139/09, § 183, CEDH 2012 (extraits), et références citées). Elle considère qu'il est légitime, devant une telle menace, que les États contractants fassent preuve d'une grande fermeté à l'égard de ceux qui contribuent à des actes de terrorisme (*idem*)' ¹⁵.

¹³ Cet avis n'est pas encore publié à la date à laquelle le présent avis est donné.

¹⁴ En vertu de l'article 1^{er} de 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* 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*', « [l']intitulé de 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 est remplacé par ce qui suit : 'Arrêté royal relatif à la banque de données commune *Terrorist Fighters*' ».

¹⁵ Note de bas de page n° 10 de l'avis cité : Cour eur. D. H., not. arrêt *Trabelsi c. Belgique*, 4 septembre 2014, § 117.

Il est également renvoyé à l'arrêt *Szabo et Vissy c. Hongrie* prononcé le 12 janvier 2016 par la Cour européenne des droits de l'homme, qui propose une synthèse récente relative aux normes et principes de protection de la vie privée en matière de lutte contre le terrorisme.

Les lignes directrices du Comité des Ministres du Conseil de l'Europe 'sur les droits de l'homme et la lutte contre le terrorisme', établissent de la manière suivante l'équilibre à établir entre les intérêts de la collectivité et les droits individuels en cause ¹⁶ :

'Le Comité des Ministres,

[a.] Considérant que le terrorisme porte gravement atteinte aux droits de l'homme, menace la démocratie et vise notamment à déstabiliser des gouvernements légitimement constitués et à saper la société civile pluraliste ;

[b.] Condamnant catégoriquement comme criminels et injustifiables tous les actes, méthodes ou pratiques terroristes, où qu'ils se produisent et quels qu'en soient les auteurs ;

[c.] Rappelant qu'un acte terroriste ne peut jamais être excusé ou justifié en invoquant les droits de l'homme et que l'abus de droit n'est jamais protégé ;

[d.] Rappelant qu'il est non seulement possible, mais absolument nécessaire, de lutter contre le terrorisme dans le respect des droits de l'homme, de la prééminence du droit et, lorsqu'il est applicable, du droit international humanitaire ;

[e.] Rappelant la nécessité pour les États de tout mettre en œuvre, et notamment de coopérer, afin que les auteurs, organisateurs et commanditaires présumés d'actes terroristes soient traduits en justice pour répondre de toutes les conséquences, notamment pénales et civiles, de leurs actes ;

[f.] Réaffirmant le devoir impératif des États de protéger les populations contre d'éventuels actes terroristes ;

[g.] Rappelant la nécessité pour les États, notamment pour des raisons d'équité et de solidarité sociale, de veiller à ce que les victimes d'actes terroristes puissent obtenir un dédommagement ;

[h.] Gardant à l'esprit que la lutte contre le terrorisme implique des mesures à long terme visant à prévenir les causes du terrorisme, en favorisant notamment la cohésion de nos sociétés et le dialogue multiculturel et inter-religieux ;

[i.] Réaffirmant l'obligation des États de respecter, dans leur lutte contre le terrorisme, les instruments internationaux de protection des droits de l'homme, et pour les États membres, tout particulièrement la Convention de Sauvegarde des Droits de l'Homme et des Libertés fondamentales ainsi que la jurisprudence de la Cour européenne des Droits de l'Homme ;

Adopte les lignes directrices suivantes et invite les États membres à en assurer une large diffusion auprès de toutes les autorités chargées de la lutte contre le terrorisme.

1. Obligation des États de protéger toute personne contre le terrorisme - Les États ont l'obligation de prendre les mesures nécessaires pour protéger les droits fondamentaux des personnes relevant de leur juridiction à l'encontre des actes terroristes, tout particulièrement leur droit à la vie. Cette obligation positive justifie pleinement la lutte des États contre le terrorisme, dans le respect des présentes lignes directrices.

¹⁶ Note de bas de page n° 11 de l'avis cité : Seules les parties les plus pertinentes en l'espèce de ces lignes directrices sont reproduites ci-après.

II. *Interdiction de l'arbitraire* - Les mesures prises par les États pour lutter contre le terrorisme doivent respecter les droits de l'homme et le principe de la prééminence du droit, en excluant tout arbitraire ainsi que tout traitement discriminatoire ou raciste, et faire l'objet d'un contrôle approprié.

III. *Légalité des mesures anti-terroristes* - 1. Toute mesure prise par les États pour lutter contre le terrorisme doit avoir une base juridique.

2. Lorsqu'une mesure restreint les droits de l'homme, les restrictions doivent être définies de façon aussi précise que possible et être nécessaires et proportionnées au but poursuivi.

[...]

V. *Collecte et traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État* - Dans le cadre de la lutte contre le terrorisme, la collecte et le traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État ne peuvent porter atteinte au respect de la vie privée des personnes que si la collecte et le traitement sont, notamment :

(i) régis par des dispositions appropriées en droit interne ;

(ii) proportionnés à l'objectif pour lequel cette collecte et ce traitement ont été prévus ;

(iii) susceptibles d'un contrôle par une autorité externe indépendante.

VI. *Mesures d'ingérence dans la vie privée* - 1. Les mesures dans la lutte contre le terrorisme qui constituent une ingérence dans la vie privée (notamment, les fouilles, les perquisitions, les écoutes, les écoutes téléphoniques, la surveillance de la correspondance et le recours à l'infiltration d'agents) doivent être prévues par la loi. Ces mesures doivent pouvoir faire l'objet d'un contrôle juridictionnel.

2. Les mesures prises pour lutter contre le terrorisme doivent être préparées et contrôlées par les autorités de façon à réduire au minimum, autant que faire se peut, le recours à la force meurtrière et, dans ce cadre, l'utilisation d'armes par les forces de sécurité doit être rigoureusement proportionnée à la défense d'autrui contre la violence illégale ou à la nécessité de procéder à une arrestation régulière.

VII. *Arrestation et garde à vue* - 1. L'arrestation d'une personne soupçonnée d'activités terroristes ne peut intervenir en l'absence de soupçons plausibles. Les motifs de l'arrestation doivent être communiqués à la personne arrêtée.

2. Une personne arrêtée ou détenue pour activités terroristes doit être aussitôt traduite devant un juge. La garde à vue doit être d'une durée raisonnable et son terme doit être fixé par la loi.

3. Une personne arrêtée ou détenue pour activités terroristes doit pouvoir contester la légalité de son arrestation ou de sa garde à vue devant un tribunal.

[...] » ¹⁷.

¹⁷ Avis 58.729/AG donnée le 26 janvier 2016 sur un avant-projet devenu la loi du 27 avril 2016 'relative à des mesures complémentaires en matière de lutte contre le terrorisme' (*Doc. parl.*, Chambre, 2015-2016, n° 54-1727/001, pp. 89 et s.).

C'est à la lumière de ces règles et principes, tels qu'ils ont encore été rappelés par l'arrêt *Big Brother Watch et autres c. Royaume-Uni* prononcé le 25 mai 2021 par la Cour européenne des droits de l'homme en Grande Chambre, que doivent également être examinées les dispositions de l'avant-projet en ce qu'elles complètent un dispositif juridique existant en matière de lutte contre le terrorisme.

Plus particulièrement, il s'agit par exemple des nouvelles dispositions qui ont pour objet d'ajouter des services partenaires à la liste existante figurant dans la loi du 5 août 1992 'sur la fonction de police' (article 2, 3°, de l'avant-projet), du fait que les catégories d'entités sont déterminées par le Roi (articles 2, 4°, et 6, § 2, alinéa 4, de l'avant-projet), qu'une « entité » peut être un mineur de plus de douze ans (lire : « douze ans et plus »)¹⁸ (article 2, 4°, de l'avant-projet) ou que la banque de données commune T.E.R. peut contenir des données relatives à un mineur (article 6, § 2, alinéa 1^{er}, 1°, 1), b), de l'avant-projet), de l'ajout de la finalité de la concertation coordonnée entre les services de base et les services partenaires (article 5, alinéa 2, 1°, de l'avant-projet), de la récolte des données santé et de la communication au prestataire de soins (article 6, § 2, alinéas 2 et 3, de l'avant-projet), des délais de conservation différents pour les données relatives aux mineurs (article 7, § 1^{er}, de l'avant-projet), de l'interconnexion à d'autres banques de données dont des sources authentiques (article 7 de l'avant-projet), de la notion de « brèches de sécurité » (article 13 de l'avant-projet), de la circonstance que l'évaluation de la menace est communiquée aux services partenaires lors de l'exercice du droit d'interrogation (article 23 de l'avant-projet), de la description du contenu de l'évaluation qui doit être effectuée avant la communication de la carte d'information à une autorité ou à une institution tierce (article 24, alinéa 2, de l'avant-projet), de la validation de l'évaluation de la menace par l'OCAM (article 27, alinéa 1^{er}, de l'avant-projet) ou encore de la création des « *Task force* locales », en abrégé « TFL », qui rassemblent des professionnels de la sécurité afin d'examiner l'opportunité de la prise de mesures à l'égard d'une « entité » enregistrée (articles 31 à 33 de l'avant-projet).

II. QUANT AU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

A. L'articulation des règles en matière de protection des données contenues dans l'avant-projet avec celles figurant dans la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel'

L'avant-projet, d'une part, élabore un dispositif autonome à la loi 'sur la fonction de police'¹⁹, dont l'objet est de porter création de la banque de données commune T.E.R. et, d'autre part, modifie notamment des dispositions dans la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel'.

¹⁸ Observation particulière n° 2 formulée sous l'article 2.

¹⁹ Ceci a également pour conséquence de modifier le statut du personnel qui sera affecté à la gestion de la banque de données commune puisque celui-ci ne tombera plus sous le régime de l'article 184 de la Constitution.

Le commentaire des articles 4 et 34 précise ce qui suit à ce sujet :

« 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 ».

Pour la protection des personnes physiques à l'égard du traitement des données à caractère personnel par la banque de données communes T.E.R., il résulte de ce qui précède que le dispositif autonome créé par l'avant-projet et les articles 138 à 167 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', tels qu'ils sont modifiés par l'avant-projet – et sous réserve des dérogations prévues par celui-ci –, s'appliquent complémentirement afin d'énoncer l'ensemble des règles en matière de traitement des données à caractère personnel pour les traitements ainsi concernés au regard du droit au respect de la vie privée et de l'admissibilité des ingérences dans l'exercice de ce droit en la matière.

Or, on constate notamment ce qui suit :

– l'article 4, alinéa 2, énonce que, par dérogation à l'article 162 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', la consultation des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. pour un traitement ultérieur à des fins historiques, scientifiques ou statistiques est autorisée par le responsable opérationnel après concertation avec les services de base, alors que l'article 46 de l'avant-projet entend compléter l'article 162 précité par un alinéa comportant une dérogation identique²⁰ ;

²⁰ Voir aussi l'observation formulée sous l'article 46.

– l'article 7, § 2, alinéa 5, est inutile dès lors qu'il est déjà prévu, à l'article 4, alinéa 1^{er}, de l'avant-projet que 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 loi précitée du 30 juillet 2018, qui comprend les articles 162 à 167, lesquels concernent le traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques ;

– l'article 29, § 3, 4°, et § 4, paraphrase inutilement l'article 157, § 3, alinéa 2, et § 4, de la même loi du 30 juillet 2018.

Interrogée à ce propos, la déléguée du Ministre a répondu ce qui suit :

« Il faut bien entendu éviter de répéter la [loi du 30 juillet 2018 relative à la relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel dans la loi [relative à la banque de données commune]. Les articles du projet de loi [...] vont être comparés avec le titre III de la loi sur la protection des données pour s'assurer qu'il n'y a pas de double emploi ».

L'avant-projet sera revu en ce sens.

B. Les principes de légalité et de proportionnalité liés à un traitement de données à caractère personnel.

1. Le fonctionnement de la banque de données commune T.E.R. implique un traitement de données à caractère personnel, qui doit être examiné au regard des principes de légalité et de proportionnalité se déduisant, en ce qui concerne le droit au respect de la vie privée, de l'article 22 de la Constitution et de l'article 8 de la Convention européenne des droits de l'homme.

B.1. Le principe de légalité

2.1. Sur le principe de légalité en la matière, dans son avis 70.542/AG donné le 24 décembre 2021 sur un avant-projet de loi 'relatif à la vaccination obligatoire des professionnels des soins de santé contre la COVID-19', la section de législation a observé ce qui suit :

« 62. Pour être admissible au regard des dispositions précitées, l'ingérence dans l'exercice du droit au respect de la vie privée doit être 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. Toute ingérence dans le droit au respect de la vie privée doit, en outre, reposer sur une justification objective et raisonnable et, par conséquent, être proportionnée aux buts poursuivis par le législateur ²¹.

²¹ Note de bas de page n° 122 de l'avis cité : Avis 63.192/2 donné le 19 avril 2018 sur un avant-projet devenu la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' (Doc. parl., Chambre, 2017-2018, n° 54-3126/001, pp. 402 à 456 ; <http://www.raadvst-consetat.be/dbx/avis/63192.pdf> ; avis 63.202/2 donné le 26 avril 2018 sur un avant-projet devenu la loi du 5 septembre 2018 'instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE' (Doc. parl., Chambre, 2017-2018, n° 54-3185/001, pp. 120 à 145, <http://www.raadvst-consetat.be/dbx/avis/63202.pdf>).

Si les ingérences prévues par le projet à l'examen poursuivent un objectif légitime (voy. *supra*, n^{os} 43 à 45), il convient de vérifier le respect des exigences de légalité (i), de pertinence et de proportionnalité (ii).

i) La légalité

63. Sur le principe de légalité inhérent au droit au respect de la vie privée garanti par l'article 22 de la Constitution, l'assemblée générale de la section de législation a exposé ce qui suit dans son avis 68.936/AG [donné le 7 avril 2021 sur un avant-projet devenu la loi du 14 août 2021 'relative aux mesures de police administrative lors d'une situation d'urgence épidémique' ²²] :

‘Conformément à l'article 22 de la Constitution, tout traitement de données à caractère personnel et, plus généralement, toute atteinte au droit à la vie privée, sont soumis au respect d'un principe de légalité formelle ²³.

En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout 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 porte sur l'exécution de mesures dont les ‘éléments essentiels’ sont fixés préalablement par le législateur ²⁴.

Par conséquent, les ‘éléments essentiels’ des traitements de données à caractère personnel doivent être fixés dans la loi elle-même. À cet égard, la section de législation considère que, quelle que soit la matière concernée, constituent, en principe, des ‘éléments essentiels’ les éléments suivants : 1°) les catégories de données traitées ; 2°) les catégories de personnes concernées ; 3°) la finalité poursuivie par le traitement ; 4°) les catégories de personnes ayant accès aux données traitées ; et 5°) le délai maximal de conservation des données’ ²⁵ » ²⁶.

La Cour constitutionnelle s'est prononcée dans le même sens dans ses arrêts n° 33/2022 du 10 mars 2022 ²⁷ et n° 110/2022 du 22 septembre 2022 ²⁸.

²² *Doc. parl.*, Chambre, 2021-2022, n° 55-2533/001, pp. 57 et s.

²³ *Note de bas de page n° 123 de l'avis cité* : Note de bas de page n° 174 de l'avis cité : Déjà invoqué plus avant, numéros 70 et s.

²⁴ *Note de bas de page n° 124 de l'avis cité* : Note de bas de page n° 175 de l'avis cité : Jurisprudence constante de la Cour constitutionnelle : voir notamment C.C., 18 mars 2010, n° 29/2010, B.16.1 ; C.C., 20 février 2020, n° 27/2020, B.17.

²⁵ *Note de bas de page n° 125 de l'avis cité* : Avis 68.936/AG précité, observation n° 101 (*Doc. parl.*, Chambre, 2020-2021, n° 55-1951/001, p. 119 ; <http://www.raadvst-consetat.be/dbx/avis/68936.pdf>).

²⁶ Avis 70.542/AG donné le 24 décembre 2021 sur un avant-projet de loi ‘relatif à la vaccination obligatoire des professionnels des soins de santé contre la COVID-19’, observations n^{os} 62 et 63 (*Doc. parl.*, Chambre, 2021-2022, n° 55-2533/001, pp. 98 et 99.

²⁷ C.C., n° 33/2022, 10 mars 2022, B.13.1.

²⁸ C.C., n° 110/2022, 22 septembre 2022, B.11.2.

2.2. Il y a lieu de constater que plusieurs éléments essentiels relatifs au traitement des données dans le cadre de la banque de données commune T.E.R. sont effectivement énoncés dans le texte en projet :

- les catégories de données à caractère personnel qui y sont traitées (article 6, § 2) (sous réserve des critiques formulées dans les observations n^{os} 2.5 à 2.7, ci-dessous) ;
- les finalités poursuivies (article 5, alinéa 2) (sous réserve de la critique formulée dans l'observation n^o 2.8, ci-dessous) ;
- le délai de conservation (article 7, §§ 1^{er} et 2) ;
- les catégories de personnes qui ont accès aux données traitées (articles 15, 16, 17 et 21 à 28).

Bien qu'ils ne constituent pas des éléments essentiels au sens de la jurisprudence et de la jurisprudence précitées, d'autres éléments sont par ailleurs également déterminés par l'avant-projet :

- le responsable du traitement (article 5, alinéa 1^{er}) ;
- la journalisation des données (article 8) ;
- les règles relatives au délégué à la protection des données et à la responsabilité de la qualité des données à caractère personnel, ainsi que des informations enregistrées (articles 29 et 30).

2.3. Le dispositif en projet appelle toutefois un certain nombre de critiques au regard du principe de légalité, exposées ci-dessous :

a) En ce qui concerne les catégories de personnes concernées par le traitement de données à caractère personnel

2.4. Les articles 2, 4^o, et 6, § 2, alinéa 4, de l'avant-projet chargent le Roi de déterminer, par arrêté délibéré en Conseil des ministres, les catégories d'« entités » à propos desquelles les données visées à l'alinéa 1^{er} de cette dernière disposition sont traitées, tandis que l'article 6, § 1^{er}, semble donner une autre portée à la catégorie de personnes dont les données à caractère personnel seront traitées dans la banque de données commune T.E.R. lorsqu'il y vise les « personnes, [...] groupements, [...] organisations [ou] phénomènes » et non plus la notion d'« entités », ce qui prête à confusion.

Interrogée à ce sujet, la délégué du Ministre a précisé que les catégories de personnes dont les données à caractère personnel pourront être traitées concernent cinq catégories d'entités, qui seront prévues dans l'arrêté royal à adopter en exécution de l'article 6, § 2, alinéa 4, de l'avant-projet, à savoir :

- 1° les *foreign terrorist fighters* ;
- 2° les *homegrown terrorist fighters* ;
- 3° les extrémistes potentiellement violents ;
- 4° les personnes condamnées pour terrorisme ;
- 5° les propagandistes de haine.

Dans le dernier alinéa du commentaire de l'article 6, on peut lire ce qui suit :

« L'article 6, § 2, alinéa 4, habilite le Roi à déterminer, par arrêté délibéré en Conseil des ministres, les catégories d'entités à propos desquelles les données visées à l'alinéa précédent sont traitées. En effet, ces catégories étant susceptibles d'évoluer en fonction des besoins opérationnels, tactiques ou stratégiques, il est dès lors préférable de les déterminer par arrêté royal. En outre, actuellement, ces catégories sont les suivantes : les '*Foreign Terrorist Fighters*', les '*Homegrown Terrorist Fighters*', les '*Propagandistes de haine*', les '*Extrémistes Potentiellement Violents*', les '*Personnes condamnées pour terrorisme*' et les entités en '*pré-enquête*', c'est-à-dire qui n'entrent pas, au moment de leur enregistrement dans la banque de données commune T.E.R., dans les critères pour être considérées comme *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou propagandiste de haine [...] ».

Les catégories d'« entités » constituent un élément central, et donc essentiel, du dispositif en projet, qui doit en conséquence être fixé par le législateur.

La circonstance que ces catégories d'« entités » sont susceptibles d'évoluer en fonction des besoins opérationnels, tactiques ou stratégiques ne peut dès lors justifier en soi une habilitation au Roi sur un point aussi essentiel, d'autant moins que le nombre de catégories d'entités est non seulement fixé mais qu'il est également limité.

Par ailleurs, ainsi que cela ressort du commentaire de l'article 6, l'auteur de l'avant-projet entend inclure dans le champ d'application des catégories de personnes dont les données à caractère personnel seront traitées, les « entités » en « pré-enquête ». Le même commentaire précise à cet égard que le but de la période de pré-enquête est le suivant :

« [...] Pour les entités en 'pré-enquête', il faut préciser que le but de cette période de 'pré-enquête' est de permettre la collecte temporaire (au maximum six mois) mais centralisées dans un seul système de traitement de l'information de données et d'informations qui pourront ou non justifier une validation de l'entité concernée en tant que *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou propagandiste de haine ('phase d'enrichissement'). À l'issue de cette période, sur la base des informations/renseignements disponibles, l'OCAM évaluera si les critères légaux sont rencontrés ou non. S'ils ne sont pas rencontrés, l'entité en pré-enquête sera automatiquement archivée. Il s'agit donc d'une situation temporaire à l'issue de laquelle cette entité sera ou non maintenue dans la banque de données commune T.E.R. ».

Or le dispositif en projet n'apporte aucun élément quant aux contours de la notion de « pré-enquête » ni au régime juridique qui devrait s'appliquer aux « entités » relevant de cette catégorie.

Pour rappel, il faut pouvoir appréhender de manière prévisible les différentes hypothèses dans lesquelles le législateur autorise une ingérence dans le droit au respect de la vie privée en fixant dans l'avant-projet les catégories de personnes, qualifiées d'« entités » par l'avant-projet, pour lesquelles il est admissible de rassembler les différentes catégories de données à caractère personnel dans la banque de données commune T.E.R.

Les articles 2, 4^o et 6, §§ 1^{er} et 2, alinéa 4, doivent être revus en ce sens.

Le dispositif sera également complété afin de préciser le régime juridique applicable à la catégorie des « entités » en « pré-enquête », dont la notion sera par ailleurs définie.

2.5. L'article 6, § 2, alinéa 1^{er}, 1^o, 1), b), de l'avant-projet contient une habilitation au Roi en ce qui concerne les données relatives aux enfants mineurs biologiques ou adoptés d'une « entité » personne physique enregistrée dans la banque de données commune T.E.R.

Le commentaire de cette disposition ajoute une information importante puisqu'il précise que cette disposition concerne uniquement les enfants mineurs qui séjournent ou ont séjournés en zone de conflit djihadiste.

Interrogée sur ce point, la déléguée du Ministre a répondu qu'à l'heure actuelle c'est en effet la seule hypothèse envisagée puisque, ainsi qu'elle l'a expliqué,

« [...] dans le but de les identifier de manière certaine, les données d'identification visées des enfants mineurs des deux catégories d'entités suivantes, seront enregistrées dans la [banque de données commune] T.E.R. :

1° les *foreigns terrorist fighters* qui se sont rendus dans une zone de conflit djihadiste (FTF catégorie 1) ;

2° les *foreigns terrorist fighters* qui sont en route vers la Belgique ou sont revenus en Belgique après s'être rendus dans une zone de conflit djihadiste (FTF catégorie 3) ».

Dès lors qu'il y a lieu de définir le plus précisément possible les hypothèses dans lesquelles un traitement de données à caractère personnel concernant des enfants mineurs peut être réalisé dans une banque de données telle que la banque de données commune T.E.R., ces précisions relatives à cette catégorie de données doivent figurer dans le dispositif en projet.

L'article 6, § 2, alinéa 1^{er}, 1°, 1), b), sera revu en conséquence.

b) En ce qui concerne les catégories de données à caractère personnel traitées

2.6. L'article 2, 4°, de l'avant-projet définit la notion d'« entité » comme étant

« toute personne physique majeure ou mineure de plus de douze ans ou toute personne morale, association de fait, ainsi que l'ensemble des moyens utilisés, déterminés par le Roi [...] ».

Il est précisé dans le commentaire de la disposition qu'il s'agit de viser

« non seulement les personnes physiques et morales mais aussi les moyens de transport, ou les numéros de téléphone/compte utilisés ».

On peut encore y lire ce qui suit à ce sujet :

« Le concept d'entité, reprend également, outre toute personne physique ou morale ou association de fait, les moyens utilisés. Ces moyens devant être entendus comme vecteurs de radicalisation. Il est parfois difficile au début d'une enquête d'identifier l'entité en tant que personne physique ou morale ou association de fait. Souvent, il sera plus aisé d'identifier le moyen utilisé (site Internet, radio, presse, etc.). Dans ce cas, les moyens doivent être repris dans la banque de données commune T.E.R. Le suivi des moyens utilisés repris dans la banque de données permet alors de prendre, le cas échéant, les mesures adéquates ».

L'ensemble du dispositif est conçu en manière telle, que lorsqu'il vise la notion d'« entité », celle-ci semble couvrir des personnes physiques, morales ou des associations de fait dont les données peuvent faire l'objet d'un traitement dans la banque de données commune T.E.R. Lorsque ces données portent sur des personnes physiques, il s'agit de données à caractère personnel au sens de l'article 4, point 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)' (dans la suite de l'avis : « le RGPD ») et de l'article 3, point 1), 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'²⁹⁻³⁰.

Or, lorsqu'il entend étendre la définition d'« entité » à celle des « moyens utilisés », il s'agit davantage de viser des catégories de données que des catégories de personnes ou d'associations en tant que telles. Compte tenu de ce constat, la notion de « moyens utilisés » trouverait mieux sa place dans l'article 6 de l'avant-projet, où elle serait alors précisée, au même titre que le sont les autres catégories de données qui y sont déjà visées et compte tenu des particularités qui entourent cette notion, ainsi que cela ressort du commentaire de la disposition.

²⁹ Cette directive a été transposée par le titre 2 (« De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ») de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', ainsi que le confirme l'article 25 de cette loi.

Aux termes de son article premier, paragraphe 1,

« [l]a [...] directive [2016/680] établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces » (voir aussi l'article 27 de la loi précitée du 30 juillet 2018).

Certains des services de base et des services partenaires susceptibles de traiter des données à caractère personnel visées par l'avant-projet tombent dans le champ d'application de l'avant-projet, compte tenu également des finalités de ces traitements telles qu'elles sont énoncées par l'article 5, alinéa 2, de l'avant-projet. D'autres de ces services relèvent du RGPD (article 2, paragraphes 1 et 2, d), du RGPD), étant entendu que les services de renseignement et de sécurité sont soumis à un régime particulier (article 3, paragraphe 2, a), de la directive 2016/680 ; article 2, paragraphe 2, a), du RGPD ; voir l'exposé des motifs du projet devenu la loi précitée du 30 juillet 2018, *Doc. parl.*, 2017-2018, Chambre, n° 54-3126/001, notamment, pp. 124 à 126 et 128), organisé par le titre 3, sous-titre 1^{er} (« De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les services de renseignements et de sécurité »), de la loi précitée du 30 juillet 2018.

³⁰ La définition de la notion de « donnée à caractère personnel », limitant son champ d'application aux « personnes physiques », issue de la définition énoncée par l'article 3, point 1), de la directive, figure également à l'article 26, 1°, de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel'.

En conséquence, les signe et mots « ainsi que l'ensemble des moyens utilisés, » seront omis de la définition de la notion d'« entité » telle qu'elle figure à l'article 2, 4°, de l'avant-projet ; le terme « déterminés » sera également remplacé par le mot « déterminées » dans la version française de l'avant-projet.

2.7. L'habilitation conférée au Roi par l'article 9, § 1^{er}, alinéa 2, de l'avant-projet est rédigée en des termes trop larges en ce qu'elle prévoit, sans en définir les éléments essentiels, une extension du contenu de la banque de données commune T.E.R. aux informations provenant d'autres banques de données via une interconnexion mais sans en fixer les finalités, les catégories de données à caractère personnel interconnectées et les règles relatives à cette interconnexion ³¹.

Par conséquent, l'article 9, § 1^{er}, alinéa 2, doit être revu au regard du principe de légalité déduit de l'article 22 de la Constitution et des exigences résultant du RGPD, ainsi que de la directive 2016/680.

c) En ce qui concerne les finalités du traitement de données à caractère personnel

2.8. Le deuxième alinéa que l'article 46 de l'avant-projet tend à insérer à l'article 162 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' dispose que toute demande adressée aux Archives de l'État de traitement ultérieur de données à caractère personnel enregistrées dans la banque de données commune T.E.R. à d'autres fins qu'à des fins historiques, scientifiques ou statistiques est refusée « à moins que la finalité soit légitime », sans autre précision.

Or, ainsi qu'il a été rappelé plus haut ³², les finalités du traitement de données à caractère personnel constituent un élément essentiel qui doit figurer dans la loi.

Le dispositif sera complété en ce sens, le cas échéant, à la lumière des exemples cités dans le commentaire de la disposition, lequel précise ce qui suit :

« [...] Par exemple, l'article 164 prévoit que si la finalité historique ne peut être obtenue avec des informations pseudonymisées, l'OCAM peut autoriser la consultation des info 'claires' s'il n'y a pas une atteinte disproportionnée à la vie privée (c'est donc un critère qui permet d'apprécier la légitimité de la demande). Par ailleurs, les travaux parlementaires de la loi du 30 juillet 2018 relative à la protection des données précise au sujet de l'article 99, al. 2, que '[p]our répondre à l'avis du Conseil d'État, en page 35, l'alinéa 2 de cet article est reformulé : il est précisé qu'un traitement ultérieur sans finalités historiques, statistiques ou scientifiques est refusé sauf si la finalité est légitime et que la consultation n'est pas susceptible de porter [atteinte] aux intérêts à protéger qui sont visés à l'alinéa premier. Ainsi, il est clair qu'il n'est pas question d'autoriser une finalité – celle-ci devant en elle-même et au préalable être légitime – mais bien une consultation de données dans certains cas. Les critères étant déterminés, il ne s'agit pas d'un pouvoir discrétionnaire. Les modalités sont celles fixées dans le présent chapitre et, le cas échéant, dans d'autres lois (par exemple la loi du 11 décembre 1998) ».

³¹ À comparer avec l'article 9, § 2, qui énumère les données dans les hypothèses d'une interconnexion avec les banques de données sources authentiques.

³² Observation générale n° II, B, 2.1.

B.2. Le principe de proportionnalité

3. L'exigence de proportionnalité est explicitée par la Cour constitutionnelle dans les termes suivants :

« B.12.1. 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 doit également répondre à un besoin social impérieux dans une société démocratique et être proportionnée au but légitime poursuivi.

Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait ménagé un juste équilibre entre tous les droits et intérêts en cause. Pour juger de cet équilibre, la Cour européenne des droits de l'homme tient compte notamment des dispositions de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après : la Convention n° 108) et de la recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (ci-après : recommandation n° R (87) 15) (CEDH, 25 février 1997, *Z c. Finlande*, § 95 ; grande chambre, 12 janvier 2010, *S. et Marper c. Royaume-Uni*, § 103).

B.12.2. Une ingérence dans l'exercice du droit au respect de la vie privée par un traitement de données à caractère personnel doit reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur. S'agissant du caractère proportionné, la Cour européenne des droits de l'homme tient compte de la présence ou de l'absence de garanties dans la réglementation concernée, destinées à éviter les abus lors du traitement de données à caractère personnel :

'35. La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article. Cette nécessité se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. Le droit interne doit notamment s'assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. Le droit interne doit aussi contenir des garanties de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (*S. et Marper c. Royaume-Uni*, précité, § 103, *Gardel c. France*, précité, § 62, CEDH 2009, et *M.K. c. France*, précité, § 35).

36. Pour apprécier le caractère proportionné de la durée de conservation des informations au regard du but poursuivi par leur mémorisation, la Cour tient compte de l'existence ou non d'un contrôle indépendant de la justification de leur maintien dans le système de traitement, exercé sur la base de critères précis tels que la gravité de l'infraction, les arrestations antérieures, la force des soupçons pesant sur la personne ou toute autre circonstance particulière (*S. et Marper c. Royaume-Uni*, précité, § 119, et *B.B. c. France*, précité, § 68).

37. Enfin, il appartient à la Cour d'être particulièrement attentive au risque de stigmatisation de personnes qui, à l'instar du requérant, n'ont été reconnues coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence. Si, de ce point de vue, la conservation de données privées n'équivaut pas à l'expression de soupçons, encore faut-il que les conditions de cette conservation ne leur donne pas l'impression de ne pas être considérés comme innocents (*S. et Marper*, précité, § 122, et *M.K.*, précité, § 36)' (CEDH, 18 septembre 2014, *Brunet c. France*, §§ 35-37).

Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel dans des banques de données par les services de police, il convient dès lors de tenir compte notamment 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 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 abusif, par les services de police, des données à caractère personnel traitées (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 59 ; grande chambre, 12 janvier 2010, *S. et Marper c. Royaume-Uni*, §§ 101-103, 119, 122 et 124; 18 avril 2013, *M.K. c. France*, §§ 37 et 42-44) »³³.

Ainsi que le précise l'exposé des motifs, le dispositif en projet a pour objet de préciser, d'explicitier et de développer certains aspects actuellement prévus par la loi du 5 août 1992 'sur la fonction de police' ou par la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' pour garantir la protection des données dans le cadre du fonctionnement de la banque de données commune T.E.R.

À propos du traitement des données à caractère personnel, il est posé, à l'article 6, § 1^{er}, le principe suivant :

« La banque de données commune T.E.R. nécessite le traitement de différentes catégories de données à caractère personnel relatives aux personnes, aux groupements, aux organisations et aux phénomènes 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.

Les données à caractère personnel visées à l'alinéa 1^{er} présentent un lien direct avec la finalité du traitement ».

³³ C.C., 14 juillet 2016, n°108/2016, B.12.

Il est rappelé que le traitement ne peut porter que sur des données à caractère personnel et informations relatives aux missions de prévention et de suivi du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme par les services concernés dans le cadre exclusif de leurs compétences légales (article 3, alinéa 1^{er}, de l'avant-projet) et dans le respect strict des quatre finalités énumérées à l'article 5, alinéa 2, de l'avant-projet (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 » 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 sur base d'une évaluation de la menace).

Concernant la durée strictement nécessaire de conservation, il est prévu que 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 traitement, à l'exception des données à caractère personnel relatives à des mineurs, qui sont conservées au maximum quinze ans après le dernier traitement (article 7, § 1^{er}, de l'avant-projet). Après le dernier traitement, le responsable opérationnel (à savoir l'Organe de la coordination pour l'analyse de la menace, qui, selon l'exposé des motifs, sera désigné en cette qualité en application de l'article 12 de l'avant-projet) examine tous les cinq ans (tous les trois ans pour les mineurs) si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités de l'article 5, alinéa 2, et, si tel n'est pas le cas, les données sont archivées (article 7, § 1^{er}, alinéas 2 et 3, de l'avant-projet).

Pour éviter un usage abusif des données, il ressort des informations transmises par la déléguée du Ministre qu'il sera prévu, en exécution de l'article 6, § 2, alinéa 5, de l'avant-projet, ce qui suit :

« Pour faciliter la gestion des accès, chaque service devra identifier les membres de son personnel autorisés à exercer les droits d'accès à la banque de données commune T.E.R. et devra transmettre une liste de ces personnes au gestionnaire qui gère les accès. Les membres du personnel doivent être titulaires d'une habilitation de sécurité de niveau 'secret' sauf pour les services de police afin de leur permettre d'évaluer correctement l'attitude à adopter à l'égard d'une personne dans les situations d'urgence » (voir, par ailleurs, le contenu des fichiers de journalisation décrit par l'article 8, § 1^{er}, alinéa 2, 2°, de l'avant-projet).

Enfin, les autorités de contrôle sont, en vertu de l'article 2, 15°, de l'avant-projet, l'Organe de contrôle de l'information policière visé à l'article 71 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' et le Comité permanent de contrôle des services de renseignements et de sécurité visé à l'article 1^{er} de la loi du 18 juillet 1991 'organique du contrôle des services de police et de renseignement et de l'Organe de coordination de la menace'.

Au stade préventif du contrôle exercé par la section de législation du Conseil d'État, il n'apparaît pas dans ce contexte que l'avant-projet ne respecterait pas le principe de proportionnalité inhérent à toute intrusion dans le droit au respect de la vie privée.

III. QUANT AUX HABILITATIONS AU ROI

1. L'avant-projet contient plusieurs habilitations au Roi.

Il est renvoyé aux observations générales n^{os} 2.4 à 2.7 pour ce qui concerne leur admissibilité au regard du principe de légalité déduit de l'article 22 de la Constitution.

2. Certaines habilitations appellent en outre, en tout état de cause, l'observation suivante.

La déléguée du Ministre a admis que plusieurs d'entre elles s'avèrent inutiles ou font double emploi avec d'autres.

Tel est le cas des habilitations contenues dans les dispositions suivantes :

– l'article 8, § 1^{er}, alinéa 4 :

« Le Roi peut, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer d'autres types de traitements pour lesquels les fichiers de journalisation sont établis » ;

– l'article 10 :

« Le Roi peut, par arrêté royal délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer des modalités complémentaires de gestion de la banque de données commune T.E.R. » ;

– l'article 18, alinéa 2 :

« Le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, les modalités d'exercice du droit de création visé à l'alinéa premier » ;

– l'article 28, § 4 :

« Le Roi peut déterminer les modalités de la communication visée aux § 2 et § 3 » ;

– l'article 29, § 2, 3^o :

« En complément des dispositions de l'article 157 de la loi relative à la protection des données, le délégué à la protection des données est chargé :

[...]

3^o de l'exécution des autres missions relatives à la protection des données et à la sécurisation qui sont déterminées par le Roi ou qui lui sont confiées par les ministres de l'Intérieur et de la Justice » ;

– l'article 32, § 2, alinéa 2 :

« Le Roi peut, par arrêté délibéré en Conseil des ministres, déterminer d'autres missions de la TFL » ;

– l'article 54, alinéa 1^{er} :

« Le Roi peut remplacer les références existantes dans les lois aux dispositions de la loi sur la fonction de police par les références aux dispositions correspondantes de la présente loi ».

Ces habilitations au Roi seront omises.

En conséquence, elles ne sont pas examinées dans la suite du présent avis, en ce compris quant à leur compatibilité avec le principe de légalité.

OBSERVATIONS PARTICULIÈRES

Article 2

1. Le commentaire de l'article 2 ne contient pas d'explication sur la nécessité de considérer les services visés à l'article 2, 3°, i) et j) (respectivement « le service des cultes et de la laïcité du Service [p]ublic fédéral Justice » et « l'Administration générale de la Trésorerie du Service [p]ublic fédéral Finances »), comme étant des services partenaires.

Interrogée à ce propos, la déléguée du Ministre a répondu ce qui suit :

« L'exposé des motifs sera précisé pour ces partenaires.

Pour le service des cultes, la motivation est la suivante : [l]e Service des Cultes et de la Laïcité du SPF Justice, service partenaire doit pouvoir bénéficier d'un droit d'interrogation dans la banque de données commune T.E.R. Le service des Cultes et de la Laïcité du SPF Justice est légalement compétent pour la reconnaissance des cultes et des organisations non confessionnelles. Il paie en outre les traitements des ministres des cultes et des délégués des communautés philosophiques non confessionnelles. Dans le cadre de ses compétences, il est nécessaire que ce service puisse interroger la banque de données commune T.E.R.

Pour la trésorerie, la motivation est la suivante : [l]'Administration générale de la Trésorerie, l'autorité compétente en matière de sanctions financières par le gel des fonds et des ressources économiques des personnes et entités qui commettent ou tentent de commettre des infractions terroristes, les facilitent ou y participent, aura un droit de lecture et d'écriture dans la banque de données commune T.E.R., en tant que service partenaire. La trésorerie est gestionnaire des sanctions financières et acquiert donc à cet effet la connaissance d'infractions et de données à caractère financier qui doivent être centralisées dans la banque de données commune pour assurer un échange de données intégré et optimal.

Dans la pratique, les avoirs de toutes les personnes qui ont rejoint un groupe terroriste en Syrie/Irak (FTF catégorie 1) ont été gelés. En outre, les avoirs d'un certain nombre d'autres entités ont déjà été gelés, notamment les avoirs de personnes condamnées pour des infractions terroristes. En outre, la Trésorerie est régulièrement contactée par des institutions financières lorsqu'elles entrent en contact avec des personnes dont les avoirs ont été gelés (ou pour lesquelles d'autres mesures financières ont été prises) par d'autres États (par exemple les États-Unis) dans un contexte de terrorisme, mais pas en Belgique. La Trésorerie doit procéder aux vérifications nécessaires et informer les institutions financières des conséquences éventuelles. L'un des éléments importants à cet égard est l'information consistant à savoir si la personne a été ou non reprise dans la banque de données commune T.E.R. La Trésorerie doit alors avoir la possibilité de vérifier quelles entités sont reprises en tant que telles dans la banque de données commune T.E.R.

Par ailleurs, l'Administration générale de la Trésorerie doit avoir la possibilité d'insérer elle-même les décisions qu'elle prend ainsi que de nombreuses informations pertinentes recueillies dans le cadre de sa compétence en matière de sanctions financières comme décrit dans l'arrêté royal du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme et la loi du 13 mai 2003 relative à la mise en œuvre des mesures restrictives adoptées par le Conseil de l'Union européenne à l'encontre d'États, de certaines personnes et entités. Sont visés ici : des montants financiers gelés, d'éventuels mouvements sur des comptes bancaires ou encore des assurances de tout type faisant l'objet d'une mesure de gel dans cette banque de données commune. Il est évident que ceci porte uniquement sur les informations relatives aux entités ayant déjà été reprises dans la Banque de données commune selon la procédure appropriée ».

L'exposé des motifs et le commentaire seront complétés en conséquence.

2. L'article 2, 4°, définit l'« entité » notamment comme étant « toute personne physique majeure ou mineure de plus de douze ans ».

Aux termes du commentaire de l'article, les personnes ainsi visées sont les mineurs de douze ans et plus³⁴ et non « de plus de douze ans » ; le dispositif sera revu en ce sens. C'est dans cette lecture que l'observation qui suit est formulée.

L'avant-projet instaure ainsi une différence de traitement entre les mineurs, avec pour conséquence qu'ils ne seront enregistrés dans la banque de données commune T.E.R. qu'à la double condition d'avoir atteint l'âge de douze ans³⁵ et que les autres conditions liées à l'enregistrement d'une entité soient réunies³⁶.

³⁴ Voir ci-dessous.

³⁵ Sous réserve de l'article 6, § 2, alinéa 1^{er}, 1°, 1), b).

³⁶ Ce n'est qu'en cas d'indices qu'une personne représente une menace pour la sécurité nationale que celle-ci y figurera (exposé des motifs, p. 14).

Pareil dispositif doit être mis en rapport avec les considérations suivantes émises par la Cour constitutionnelle :

« B.148.1. [...] [U]n traitement de données à caractère personnel dans des banques de données policières 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 des données à caractère personnel de mineurs dans les banques de données policières, la loi attaquée n'instaure donc pas une incrimination ou une peine qui dérogerait aux dispositions de la loi relative à la protection de la jeunesse, laquelle reste intégralement applicable.

[...]

B.149. Tant l'article 22*bis*, alinéa 4, de la Constitution que l'article 3, paragraphe 1, de la Convention relative aux droits de l'enfant imposent aux autorités de prendre en compte, de manière primordiale, l'intérêt de l'enfant dans les procédures le concernant. L'article 22*bis*, alinéa 5, de la Constitution donne par ailleurs au législateur la mission de garantir que l'intérêt de l'enfant soit pris en considération de manière primordiale.

Ces dispositions n'empêchent pas en elles-mêmes le législateur de prévoir que des données à caractère personnel de mineurs peuvent être traitées par les services de police, afin de permettre à ces services 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 police, le législateur doit tenir compte de la situation particulière des mineurs, notamment en ce qui concerne leur personnalité et leur degré de maturité »³⁷.

À propos du choix de l'âge à partir duquel une personne physique peut être enregistrée dans la banque de données commune T.E.R., le commentaire de l'article 2 expose ce qui suit :

« Ce projet de loi est aussi plus précis à propos des critères d'enregistrement dans la banque de données T.E.R. liés à l'âge d'une personne physique : les personnes physiques majeures et mineures à partir de douze ans peuvent être enregistrées dans la banque de données commune T.E.R. si elles correspondent aux critères d'enregistrement. Les mineurs de moins de 12 ans ne sont donc pas enregistrés comme entité dans la banque de données commune T.E.R. Pour les mineurs à partir de 12 ans jusqu'à 18 ans inclus, des mesures de protection additionnelles sont en outre prévues. Ainsi, le délai de conservation maximum dans la banque de données commune T.E.R. après le dernier traitement n'est pas de 30 ans mais de 15 ans et le responsable opérationnel est tenu d'évaluer la nécessité d'archiver les données le concernant tous les 3 ans minimum et pas tous les 5 ans. Enfin, lors de l'évaluation préalable à la communication de données via une carte d'information, le statut de minorité doit être pris en compte pour évaluer la nécessité de réaliser cette communication.

Le seuil de douze ans a été choisi car il s'agit d'un âge pivot repris dans diverses législations.

³⁷ C.C., 14 juillet 2016, n° 108/2016, B.148.1 et B.149. Voir également C.C., 23 avril 2015, n° 44/2015, B.51.3.

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).

Par ailleurs, 12 ans est l'âge à partir duquel un enfant peut être associé dans diverses procédures le concernant. Par exemples, 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).

Au niveau international, le Comité des droits de l'enfant (chargé de surveiller l'application par les États de la Convention internationale des droits de l'enfant) a été très clair dans ses observations n° 10 (2017) relatives aux droits de l'enfant dans le système de justice pour mineurs.

Il précise ce qui suit (n° 32, page 54) : '[l']article 4 des Règles de Beijing prescrit, dans les systèmes juridiques qui reconnaissent la notion de seuil de responsabilité pénale, de ne pas fixer ce seuil trop bas eu égard aux problèmes de maturité affective, psychologique et intellectuelle. Conformément à cette règle, le Comité a recommandé à des États parties de ne pas fixer à un niveau trop bas l'âge minimum de la responsabilité pénale ou bien de relever cet âge minimum, là où il est trop faible, pour le porter à un niveau acceptable sur le plan international. Il ressort de ces recommandations que le Comité considère comme inacceptable sur le plan international de fixer l'âge minimum de la responsabilité pénale en dessous de 12 ans. Des États parties sont encouragés à relever l'âge trop bas de la responsabilité pénale pour le porter à 12 ans, âge qui constitue un minimum absolu, et à continuer de le relever progressivement' ».

La différence de traitement entre les mineurs selon qu'ils ont atteint ou non l'âge de douze ans semble raisonnablement justifiée en l'espèce au regard de la jurisprudence de la Cour constitutionnelle étant donné que le législateur peut en principe, pour fixer l'âge à partir duquel des données à caractère personnel peuvent être traitées dans un instrument tel que la banque de données commune T.E.R., s'inspirer de l'âge de douze ans qui est fixé dans les lois précitées³⁸.

Article 6

1. Au paragraphe 2, 1°, 1), a), ii., parmi les catégories de données pouvant être traitées, figure, « s'il échet, le numéro d'identification du registre national des personnes physiques ».

La question se pose de savoir s'il n'y a pas lieu de prévoir également une identification liée à d'autres registres comme par exemple le registre des étrangers.

³⁸ C.C., 14 juillet 2016, n° 108/2016, B.145 à B.156.

Interrogée à ce sujet, la déléguée du Ministre a répondu que le numéro du registre des étrangers est une donnée qui permet aussi d'avoir une identification unique et qu'elle sera ajoutée à la liste.

L'article 6 sera complété en conséquence. Il en va de même pour le commentaire, qui doit contenir une justification quant à l'ajout de cette donnée supplémentaire.

2. L'article 6, § 2, alinéa 1^{er}, 1^o, 1), c), énumère les données relatives aux catégories particulières de données à caractère personnel, dont les données concernant la santé (v.). Pour celles-ci, l'article 6, § 2, alinéa 2, prévoit dans quelles limites ces données dites « sensibles » peuvent être récoltées et l'article 6, § 2, alinéa 3, énonce l'hypothèse dans laquelle elles peuvent être communiquées.

Ces données figurent parmi celles visées par l'article 9, paragraphes 1 et 2, du RGPD et par l'article 10 de la directive (UE) 2016/680 précitée ³⁹.

Aux termes de l'article 10 de cette directive,

« [...] le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé [...] est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :

- a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre ;
- b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou
- c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée » ⁴⁰.

³⁹ Sur le champ d'application du RGPD et de la directive (UE) 2016/680 précitée, il est renvoyé à l'observation générale n° II, B, 2.6.

⁴⁰ Voir aussi l'article 34, § 1^{er}, de la loi précitée du 30 juillet 2018, qui transpose l'article 10 de la directive. L'article 34 de la loi comprend également un paragraphe 2, rédigé comme suit :

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

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

Dans le RGPD, c'est l'article 9 qui règle le même objet en visant en son paragraphe 1 les mêmes traitements que ceux mentionnés à l'article 10 de la directive (UE) 2016/680 pour les interdire avant d'énoncer en son paragraphe 2 une série de cas de figure dans lesquels cette interdiction ne s'applique pas, notamment lorsque :

« i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ».

Le commentaire de l'article 6 de l'avant-projet explique ce qui suit :

« Le traitement de toutes les catégories particulières de données à caractère personnel précitées est assorti des garanties appropriées exigées par la loi relative à la protection des données. En effet, les données contenues dans la banque de données commune T.E.R. sont accessibles sur base de différents droits d'accès que le Roi va donner aux services énumérés dans la loi sur la base du principe du besoin d'en connaître pour l'exercice de leurs missions visées à l'article 3 et conformément aux finalités de l'article 5, alinéa 2. En outre, chaque service devra identifier les membres de son personnel autorisés à exercer les droits d'accès à la banque de données commune T.E.R. et devra transmettre une liste de ces personnes au gestionnaire qui gère les accès. Cette liste pourra, le cas échéant, être mise à la disposition du délégué à la protection des données et au responsable opérationnel dans le cadre de leurs missions respectives. Il est également précisé que les membres du personnel doivent être titulaires d'une habilitation de sécurité de niveau 'secret', pour accéder à la banque de données commune T.E.R. ».

Pour les données dites « sensibles », il y aura lieu de tenir compte, lors de la mise en œuvre de l'habilitation au Roi contenue dans l'article 6, § 2, alinéa 5, consistant à déterminer par arrêté délibéré en Conseil des Ministres et après avis des autorités de contrôle, les mesures nécessaires en vue d'assurer la gestion et la sécurité des données à caractère personnel et des informations traitées dans la banque de données communes T.E.R., des obligations imposées par l'article 10 de la directive 2016/680 et par l'article 9 du RGPD, spécialement le paragraphe 2, i), de cette dernière disposition. Cela implique, pour les traitements tombant dans le champ d'application de la directive, de prévoir des « garanties appropriées pour les droits et libertés de la personne concernée » et, pour ceux relevant du RGPD, de « prévoir[r] des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel », compte tenu également de l'article 34, § 2, de la loi précitée du 30 juillet 2018.

Article 13

1. L'article 13, § 2, prévoit que le responsable opérationnel procède soit à une information (alinéas 1^{er} et 2), soit à une notification (alinéa 3) à des personnes ou à des organismes mentionnés quant à l'existence de « brèches de sécurité » de la banque de données commune T.E.R.. Par ailleurs l'article 13, § 3, décrit le contenu de la notification « visée au paragraphe 2, alinéas 2 et 3 ».

Or, l'alinéa 2 du paragraphe 2 utilise la notion d'« information » et non celle de « notification » et l'alinéa 1^{er} du paragraphe 2 ne serait donc pas concerné.

Interrogée sur ce point, la déléguée du Ministre a proposé d'harmoniser les paragraphes 2 et 3 pour viser uniquement la notification.

L'article 13 sera revu en conséquence.

2. Au paragraphe 2, alinéa 3, dès lors qu'il est prévu qu'en cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable opérationnel est tenu de la notifier aux autorités de contrôle dans les meilleurs délais, il est inutile de préciser que cette notification doit être faite « si possible 72 heures après » que le responsable opérationnel en ait eu connaissance. Ainsi rédigé, ce membre de phrase pourrait en outre être interprété comme impliquant que la notification doit intervenir au plus tôt dans ce délai, ce qui manquerait de pertinence.

Les mots « et si possible, 72 heures après en avoir pris connaissance » seront omis.

Article 16

L'article 16 de l'avant-projet octroie aux autorités de contrôle exclusivement un droit de lecture dans la banque de données commune active ainsi que dans les archives.

Or, il est expliqué à plusieurs reprises dans l'exposé des motifs que le droit de lecture est toujours lié au droit d'écriture ⁴¹.

Comme en a convenu la déléguée du Ministre, tel n'est pas le cas dans le cadre de l'article 16, qui constitue donc une exception puisque le binôme « droit de lecture/droit d'écriture » ne vaut pas pour les organes de contrôles vu leur fonction de contrôle, qui ne nécessite pas un droit d'écriture mais uniquement un droit de lecture.

L'exposé des motifs et le commentaire seront clarifiés en conséquence.

⁴¹ Voir par exemple le commentaire introductif de la section 5 du chapitre 2 (« le droit de lecture va de pair avec le droit/l'obligation d'écriture ») et le commentaire de l'article 17 (« les droits de lecture et d'écriture sont indissociables »).

Article 19

1. En introduisant le membre de phrase « qui bénéficient d'un droit de lecture et d'un droit d'écriture » par une virgule, l'alinéa 1^{er} doit être lu comme signifiant que non seulement les services de base mais également les services partenaires disposent nécessairement de ces droits.

Or, aux termes de l'article 17, ces services ne deviennent titulaires de ces droits que si le Roi le leur accorde.

Il y a donc lieu d'omettre cette virgule en manière telle que le texte soit dépourvu d'ambiguïté, à l'instar de la rédaction, *mutatis mutandis*, de l'article 23, alinéa 1^{er}, de l'avant-projet pour ce qui concerne le droit d'interrogation qui aurait été accordé aux services partenaires par le Roi.

2. Il est prévu que les services de base et les services partenaires qui bénéficient d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R. sont tenus de consulter la banque de données et d'y introduire d'office leurs propres données à caractère personnel et les informations pertinentes, qui « proviennent des données à caractère personnel et [des] informations qui sont à [leur] disposition [...] dans le cadre de leurs missions respectives et des finalités qui y sont liées ».

Or il ressort de l'article 18 que seul un service de base dispose d'un droit de création d'une « entité » dans la banque de données commune T.E.R.

Compte tenu de l'obligation pesant sur les services partenaires d'introduire dans la banque de données les données à caractère personnel et les informations dont ils disposent, il s'indiquera de préciser les modalités qui permettront à ces services d'être informés de la création d'une « entité » dans la banque de données. À défaut, les services concernés seraient confrontés à l'obligation de se tenir informés à leur initiative de l'éventualité de la création d'une « entité » à propos de laquelle ils disposeraient de données ou d'informations, ce qui, sur le plan pratique, ne saurait se concevoir que difficilement.

Article 30

Le commentaire de l'article 30 ne contient pas d'explication sur la portée du paragraphe 4, qui contient une nouvelle habilitation au Roi prévoyant qu'

« [il] peut par arrêté délibéré en Conseil des Ministres et après avis des autorités de contrôle, déterminer d'autres règles de responsabilité en matière de protection des données à caractère personnel des services de base et des services partenaires traitant ces données ».

Interrogé à ce sujet, la déléguée du Ministre a apporté les précisions suivantes :

« Un premier contrôle de qualité est opéré au sein même du service qui transmet une donnée ou une information à la [banque de données commune (BDC)] T.E.R. Les services disposant d'un droit de lecture et d'écriture dans la BDC doivent mettre en place un système de validation interne de leurs propres données afin d'avoir des données adéquates, pertinentes et non excessives au regard des missions et des finalités de la BDC (art. 14). L'article 15 prévoit qu'un service partenaire peut ajouter des données à propos d'une entité déjà enregistrée sans modifier/supprimer celles qui existent déjà. Seul le service qui a enregistré une donnée peut la modifier, la rectifier et la supprimer. Si un autre service estime qu'une donnée doit être modifiée, rectifiée ou supprimée, il en informe le service qui l'a enregistrée en vue de procéder le cas échéant aux adaptations nécessaires. En cas de désaccord, le responsable opérationnel prend la décision finale ».

Ces explications figureront utilement dans le commentaire de la disposition.

Articles 31 et 32

1. Aux termes de l'article 31 de l'avant-projet,

« [...] 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 et aux habilitations, attestations et avis de sécurité, sont échangées au sein d'une ou de 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 ».

Il est prévu à l'article 32, § 1^{er}, alinéa 4, de l'avant-projet que le président de cette Task Force locale, en concertation avec ses « participants », à savoir les services de renseignements et de sécurité, l'Organe de coordination pour l'analyse de la menace, la police fédérale, la police locale, la Direction générale de l'Office des étrangers du Service public fédéral Intérieur et le Ministère public,

« 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 articles 31 et 32 de l'avant-projet sont placés dans un chapitre 3 portant comme intitulé « Enrichissement des données relatives aux entités et suivi d'une entité validée dans la banque de données communes T.E.R. ».

2. Tel qu'il est libellé, le début de l'article 31 fait apparaître que l'échange de données au sein des Task Force locales a pour objectif

« d'assurer l'enrichissement des données à caractère personnel et informations relatives aux entités ainsi que le suivi et la prise de mesures à l'égard des entités validées dans la banque de données commune T.E.R. ».

Interrogée à ce sujet, la déléguée du Ministre a précisé ce qui suit à propos de l'échange de données ou d'informations au sein de la Task force locale et de ce qu'il y avait lieu d'entendre quant à la notion d'enrichissement des données :

« L'avant-projet de loi utilise en effet à plusieurs reprises la notion d'enrichissement des données/informations. Cette notion doit être comprise d'une part comme une contextualisation des données et d'autre part comme la mise à jour de l'information déjà enregistrée et/ou l'ajout des informations nouvelles.

Pourquoi faut-il contextualiser ?

La [banque de données 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 T.E.R.] ne reprend pas, par exemple, le contenu *in extenso* des procès-verbaux) et la contextualisation permet donc de donner tout le contexte relatif à la donnée enregistrée dans la [banque de données T.E.R.] (personne, véhicule, ...).

Pourquoi faut-il mettre à jour ?

Lors de la [Task force locale] et de la discussion avec les différents services présents, il peut ressortir qu'il y ait des nouvelles données à enregistrer et qu'il faille donc 'enrichir' la banque de données ou qu'il soit nécessaire de mettre de l'information déjà enregistrées à jour.

Telles qu'elles sont définies à l'article 2, 5° et 6°, de l'avant-projet, les données à caractère personnel et les informations qui peuvent être insérées dans la banque de données commune T.E.R. sont des données et des informations non classifiées.

[...]

Comme l'article 2, points [5]° et [6]°, le prévoit, la [banque de données T.E.R.] ne contient pas de données classifiées. Utiliser une banque de données qui peut contenir des données classifiées a des implications majeures en termes de développement, sécurité de la banque de données, ce qui n'est pas le cas de la banque de données commune T.E.R..

Lors des réunions des [Task forces locales], dans le cadre de l'enrichissement des données, entre partenaires qui disposent d'une habilitation de sécurité et du besoin d'en connaître, des informations classifiées sur une personne enregistrée dans la banque de données T.E.R. peuvent être échangées ».

Il ressort des explications ainsi fournies que l'échange de données au sein de la Task force locale peut amener à préciser des données à caractère personnel ou des informations qui sont déjà contenues dans la banque de données commune T.E.R., à mettre à jour ces données ou à en introduire de nouvelles.

Toutefois, compte tenu des définitions prescrites par les 5° et 6° de l'article 2 de l'avant-projet, et afin d'assurer la cohérence de l'ensemble du dispositif, l'article 31 de l'avant-projet ne pourrait 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.

Sous réserve de cette interprétation, l'article 31 de l'avant-projet est admissible.

3. Interrogée quant à la portée de l'article 32, § 1^{er}, alinéa 4, en projet, la déléguée du Ministre a également apporté les précisions qui suivent :

« Lors des réunions de la [Task Force locale], les principes de base (chapitre 2 sections 5 et 7) contenus dans le projet de loi en matière d'accès ou de communication de données sont respectés.

Chaque membre présent travaille sur la base du principe du besoin d'en connaître.

Si un membre externe est invité, il est présent dans le but exclusif de fournir des données, éclairer un point précis par son expertise et pas pour recevoir des données. Il est présent pour 'son point' et quitte ensuite la réunion après son exposé ».

Il résulte de ces explications que l'article 32, § 1^{er}, 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.

C'est ici encore sous réserve de cette interprétation que l'article 32 de l'avant-projet est admissible.

Article 32

L'article 32, § 1^{er}, prévoit la composition de la « Task force locale », dénommée TFL.

Cependant, il n'y a pas d'indication quant au nombre de membres par catégories ni quant aux modalités de fonctionnement de celle-ci.

Interrogée à cet égard, la déléguée du Ministre a répondu ce qui suit :

« Le texte va être réexaminé pour prévoir éventuellement la présence au minimum d'une personne par autorité présente à la TLF. Le texte va être réexaminé pour prévoir éventuellement un nombre minimum de réunion par an ».

Articles 34 à 49

Comme en a convenu la déléguée du Ministre, l'exposé des motifs et le commentaire seront complétés par une explication article par article des dispositions en projet afin d'expliquer les modifications qui sont apportées à la loi du 30 juillet 2018.

Article 46

L'article 46 tend à compléter l'article 162 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard de traitement de données à caractère personnel' par deux alinéas nouveaux, formant les alinéas 3 et 4.

Il résulte de l'alinéa 3 en projet que, par dérogation à l'alinéa 1^{er} actuel de l'article 162, la consultation de données à caractère personnel relatives aux entités enregistrées dans la banque de données commune T.E.R. par un responsable du traitement ultérieur, à des fins historiques, scientifiques ou statistiques, est autorisée par le responsable opérationnel de la banque de données après concertation avec les services de base.

La question se pose de savoir pour quel motif une telle dérogation est apportée à l'article 162, alinéa 1^{er}, de la loi précitée en ne prévoyant pas une réserve à l'autorisation de consultation dans l'hypothèse où cette dernière nuirait à l'exercice de l'action publique, à la sécurité d'une personne ou à la relation avec un service répressif d'un État étranger, cette réserve étant d'ailleurs également prévue par l'article 20 de l'avant-projet.

À défaut de justification sur ce point, le dispositif sera complété afin d'envisager cette hypothèse.

Par ailleurs, dans la version néerlandaise de l'alinéa 3, il y a lieu d'insérer le verbe « toestaan » entre le mot « entiteiten » et les mots « door de operationeel verantwoordelijke ».

Article 54

Comme en a convenu la déléguée du Ministre, il y a lieu de compléter l'alinéa 2, *in fine*, afin de prévoir que le Roi puisse remplacer les références existantes dans les lois aux dispositions des arrêtés royaux abrogés par les références aux dispositions correspondantes « de la présente loi ou de ses arrêtés d'exécution ».

Article 56

L'article 56 est rédigé de la manière suivante :

« La présente loi entre en vigueur à la date fixée par le Roi et au plus tard le xx/xx/xxxx ».

Interrogée sur le fait que la date ultime d'entrée en vigueur n'est pas complétée dans l'avant-projet, la déléguée du Ministre a précisé ce qui suit :

« Il était en effet important que la loi et l'arrêté royal portant exécution de celle-ci entrent en vigueur en même temps, et ce, pour permettre une application complète de la législation en matière de la [banque de données communes] T.E.R. Le but est que le projet de loi et d'arrêté royal entrent en vigueur encore sous cette législature. Nous proposons donc de prendre une date ultime (et au plus tard) fin 2024 ».

La date sera complétée dans l'article 56 conformément aux règles de légistique sur ce point ⁴². Par voie de conséquence, le commentaire contiendra une explication du choix de cette entrée en vigueur.

OBSERVATIONS FINALES

L'avant-projet sera revu sur les points suivants :

– à l'article 2, 5°, il y a lieu de reproduire l'intitulé complet 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)', de préciser qu'il est abrégé en « RGPD » et d'utiliser cette abréviation pour la suite de l'avant-projet ;

– de même dans la version française de l'article 33, § 2, 6°, il y a lieu de reproduire l'intitulé exact de la loi du 18 septembre 2017 'relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces' ;

– dans la version française de l'article 2, 15°, il y a lieu de supprimer le doublon du mot « organique » ;

– à l'article 6, § 2, alinéa 1^{er}, 1), c), i., de la version française, il y a lieu d'omettre le mot « de ».

– enfin, les renvois d'articles doivent être vérifiés ou précisés, comme par exemple dans les articles 7, § 2, alinéa 3, 4°, 11, alinéa 2, 5°, 16, 39, 44 et 50 ; il en va de même pour l'article 32, § 1^{er}, alinéa 3, qui contient une erreur de renvoi car il y a lieu d'y viser l'article 4, alinéa 3, de la loi du 11 décembre 1998 'relative à la classification et aux habilitations, attestations et avis de sécurité' et pour l'article 32, § 2, alinéa 1^{er}, 1°, qui doit renvoyer à l'article 31 et non à l'article 32 de l'avant-projet.

*

⁴² *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet « Technique législative », recommandations n^{os} 154.1 à 154.1.2 et formule F 4-5-2-4.

Aangezien de adviesaanvraag is ingediend op basis van artikel 84, § 1, eerste lid, 2°, van de wetten ‘op de Raad van State’, gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,[‡] de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

VOORAFGAANDE VORMVEREISTEN

Sinds de wijziging van de gecoördineerde wetten ‘op de Raad van State’ bij de wet van 2 april 2003 ‘tot wijziging van sommige aspecten van de wetgeving met betrekking tot de inrichting en de werkwijze van de afdeling wetgeving van de Raad van State’, kan de niet-vervulling van vormvereisten er weliswaar niet meer toe leiden dat adviesaanvragen onontvankelijk zijn maar het beginsel blijft dat de afdeling Wetgeving pas om advies kan worden gevraagd nadat het betrokken voorontwerp alle achtereenvolgende stadia van de administratieve voorbereiding heeft doorlopen en nadat het orgaan dat bevoegd is om het voorontwerp vast te stellen de mogelijkheid heeft gehad het eventueel aan te passen in het licht van de elementen die bij het vervullen van de vormvereisten naar voren zijn gekomen. Aldus wordt vermeden dat de Raad van State advies zou uitbrengen over een niet-definitieve ontwerp tekst en wordt gewaarborgd dat het advies kan worden uitgebracht met volledige kennis van alle ter zake relevante elementen.¹

Die opmerking geldt *a fortiori* voor het advies van het Controleorgaan op de politieke informatie (afgekort en hierna: “het COC”) wanneer het om ontwerpen gaat die, zoals het voorliggende voorontwerp, bij uitstek betrekking hebben op de verwerking van persoonsgegevens: de adviesverplichting strekt er precies toe onder meer na te gaan of de ontworpen regeling wel in overeenstemming is met de juridische vereisten die gelden voor de verwerking van persoonsgegevens². Hetzelfde geldt voor het – eveneens vereiste – advies van de Gegevensbeschermingsautoriteit (hierna: “de GBA”). In de brief met de adviesaanvraag wordt bovendien vermeld dat nog om andere adviezen is verzocht maar dat die niet zijn overgezonden aan de afdeling Wetgeving van de Raad van State: het gaat om de adviezen van het College van procureurs-generaal, de Orde der artsen en de algemeen afgevaardigden voor de rechten van het kind.

[‡] Aangezien het om een voorontwerp van wet gaat, wordt onder “rechtsgrond” de overeenstemming met de hogere rechtsnormen verstaan.

¹ Adviezen 41.417/AV tot 41.420/AV van 6 oktober 2006 over voorontwerpen die hebben geleid tot respectievelijk de wet van 10 mei 2007 ‘tot wijziging van de wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden’, de wet van 10 mei 2007 ‘ter bestrijding van discriminatie tussen vrouwen en mannen’, de wet van 10 mei 2007 ‘ter bestrijding van bepaalde vormen van discriminatie’ en de wet van 10 mei 2007 ‘tot aanpassing van het Gerechtelijk Wetboek aan de wetgeving ter bestrijding van discriminatie en tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden’ (Parl.St. Kamer 2006-07, nr. 51-2720/001, 126).

² Zie in die zin eveneens advies 69.369/1 van 4 juni 2021 over een voorontwerp dat heeft geleid tot de ordonnantie van de Gemeenschappelijke Gemeenschapscommissie van 27 januari 2022 ‘tot wijziging van de ordonnantie van 11 mei 2017 betreffende het inburgeringstraject voor de nieuwkomers’ (Parl.St. Br.Parl. 2021-22, nr. B-87/1, 9 e.v.).

Uit het onderzoek van de auditeur-rapporteur blijkt dat die adviezen nog niet gegeven zijn.

De methode die erin bestaat tegelijk het advies van de afdeling Wetgeving van de Raad van State, van het COC en van de GBA aan te vragen, is *in casu* dan ook ten eerste af te keuren.³ De afdeling Wetgeving kan dan immers niet over alle relevante informatie beschikken die mogelijk nuttig is voor haar onderzoek, meer in het bijzonder betreffende de wijze waarop met die adviezen rekening zou zijn gehouden en hoe dit in de memorie van toelichting en in de artikelsgewijze bespreking naar voren zou zijn gebracht.

In de memorie van toelichting moet hoe dan ook worden verduidelijkt hoe in het voorontwerp rekening zou zijn gehouden met de adviezen van het COC en de GBA.

Indien de aan de Raad van State voorgelegde tekst, ingevolge het onderzoek van die adviezen door de steller van het voorontwerp, nog wijzigingen zou ondergaan die niet louter vormelijk zijn of die niet eveneens voortvloeien uit het gevolg dat aan dit advies wordt gegeven, moeten de gewijzigde of toegevoegde bepalingen ten slotte opnieuw om advies aan de afdeling Wetgeving worden voorgelegd overeenkomstig artikel 3, § 1, eerste lid, van de wetten ‘op de Raad van State’, gecoördineerd op 12 januari 1973.

VOORAFGAANDE OPMERKINGEN OVER DE DRAAGWIJDTE VAN HET ONDERZOEK VAN HET VOORONTWERP

1. De brief met de adviesaanvraag is gesteld als volgt:

“Le projet de loi que je soumets à votre avis vise tout d’abord à transposer dans une loi autonome les dispositions relatives aux banques de données communes qui sont actuellement décrites à la sous-section 7bis ‘Des banques de données communes’ de la loi du 5 août 1992 sur la fonction de police et dans les arrêtés royaux du 21 juillet 2016 relatif à la banque de données communes ‘Terrorist Fighters’ et du 23 avril 2018 relatif à la banque de données commune ‘Propagandistes de haine’.

Ce projet de loi est d’un part constitué de dispositions transférées sans modification de fond de la loi sur la fonction de police, ainsi que des [arrêtés royaux] ‘Terrorist Fighters’ et ‘Propagandistes de haine’.

³ Zie in die zin onder meer advies 71.258/2 van 4 mei 2022 over een voorontwerp dat heeft geleid tot de wet van 16 oktober 2022 ‘tot oprichting van het Centraal register voor de beslissingen van de rechterlijke orde en betreffende de bekendmaking van de vonnissen en tot wijziging van de assisenprocedure betreffende de wraking van de gezworenen’, voorafgaande opmerking 2 (*Parl.St.* Kamer 2021-22, nr. 55-2754/001, 68 e.v.). Zie eveneens advies 72.873/2 van 15 mei 2023 over een voorontwerp van wet ‘tot wijziging van de wet op het politieambt’ (niet bekendgemaakt op de datum waarop dit advies wordt gegeven).

D'autre part, ce projet apporte des définitions et des précisions sur la notion d'entité enregistrée dans la banque de données commune (BDC) T.E.R., précise les différents types de supports d'extraits de données contenues dans la BDC T.E.R., précise les règles liées aux traitements de données des mineurs, énumère les catégories de données à caractère personnel qui peuvent être traitées dans la BDC TER, permet la communication de données enregistrées dans la BDC TER aux professionnels des soins de santé, prévoit que l'analyse de la menace d'une entité devra être mise à jour au moins deux fois par an, permet l'interconnexion de la banque de données commune avec d'autres banques de données et précise le fonctionnement des local task forces.

Ensuite, la loi cadre en matière de protection des données (loi du 30 juillet 2018) a été modifiée pour donner un traitement juridique clair aux données à caractère personnel concaténées par différents services au sein d'une même banque de données.

Enfin, la loi sur la fonction de police a également été adaptée afin de donner une assise juridique claire à la coopération et la communication de données entre les différents services (services de police, services d'urgence et de secours et services de la santé) qui doivent intervenir en réponse à des incidents mineurs ou majeurs et, en particulier, à garantir l'intégrité physique et psychologique de la personne concernée elle-même et de toute personne susceptible d'entrer en contact avec elle dans le cadre de l'intervention des services précités et la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme, a été légèrement adaptée purement pour des questions de forme et de renvoi.

Le projet d'arrêté royal quant à lui rassemble dans un seul instrument plusieurs arrêtés royaux qui étaient relatifs à la banque de données commune et les rassemble dans un seul instrument."

In de memorie van toelichting wordt uitgelegd dat de bestaande wettelijke en verordenende bepalingen worden samengebracht in een op zichzelf staande wetgevende tekst teneinde een ad-hocrechtsgrondslag te geven aan de gemeenschappelijke gegevensbank T.E.R., die gemeenschappelijk is voor verschillende diensten en dus niet specifiek aan de wet van 5 augustus 1992 'op het politieambt' gekoppeld diende te zijn, maar ook omdat, "ter wille van een grotere rechtszekerheid, heel wat essentieel geachte bepalingen die in de koninklijke besluiten tot oprichting van de gegevensbanken 'Terrorist Fighters' en 'Haatpropagandisten' waren opgenomen, [worden] vastgelegd in de wet".

Uit de bespreking van artikel 2 blijkt dat, technisch gesproken, de gemeenschappelijke gegevensbank T.E.R. bestaat uit de huidige gemeenschappelijke gegevensbanken "Terrorist Fighters" en "Haatpropagandisten"⁴ want "in feite [bestaat er] vanuit informatica oogpunt (...) slechts één gemeenschappelijke gegevensbank voor alle categorieën van personen of entiteiten die in de voornoemde koninklijke besluiten van 21 juli 2016 en 23 april 2018 worden opgesomd".⁵

⁴ Zie punt 6), "Gemeenschappelijke gegevensbank T.E.R." in de bespreking van artikel 2.

⁵ Memorie van toelichting en bespreking van artikel 3.

2. Dientengevolge wordt, wat de bepalingen betreft die zonder wezenlijke wijziging⁶⁻⁷ worden overgenomen uit de bestaande teksten maar die wel de precisering bevatten betreffende de nieuwe benaming van de gemeenschappelijke gegevensbank “T.E.R.”, verwezen naar de adviezen die de afdeling Wetgeving over die bepalingen heeft gegeven.

Voor de bepalingen betreffende de wet van 5 augustus 1992 ‘op het politieambt’ en betreffende de besluiten tot uitvoering van die wet, gaat het hoofdzakelijk om de adviezen 58.729/AV van 26 januari 2016 over een voorontwerp dat heeft geleid tot de wet van 27 april 2016 ‘inzake aanvullende maatregelen ter bestrijding van terrorisme’,⁸ 59.515/2 van 6 juli 2016 over een ontwerp dat heeft geleid tot het koninklijk besluit van 21 juli 2016 ‘betreffende de gemeenschappelijke gegevensbank Terrorist Fighters en tot uitvoering van sommige bepalingen van de afdeling 1bis “Het informatiebeheer” van hoofdstuk IV van de wet op het politieambt’, 62.629/2 en 62.630/2 van 31 januari 2018 over twee ontwerpen die hebben geleid tot respectievelijk het koninklijk besluit van 23 april 2018 ‘betreffende de gemeenschappelijke gegevensbank Foreign Terrorist Fighters en tot uitvoering van sommige bepalingen van de afdeling 1bis “Het informatiebeheer” van hoofdstuk IV van de wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank Foreign Terrorist Fighters naar de gemeenschappelijke gegevensbank Terrorist Fighters’ en het koninklijk besluit van 23 april 2018 ‘betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis “Het informatiebeheer” van hoofdstuk IV van de wet op het politieambt’ en 66.662/2 van 25 november 2019 over een ontwerp dat heeft geleid tot het koninklijk besluit van 20 december 2019 ‘tot wijziging van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters en van het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis “Het informatiebeheer” van hoofdstuk IV

⁶ De memorie van toelichting geeft daar uitleg over.

⁷ De artikelen 51 en 52 van het voorontwerp strekken dientengevolge tot opheffing van respectievelijk artikel 44/2, § 2, van de wet van 5 augustus 1992 ‘op het politieambt’, ingevoegd bij de wet van 27 april 2016 ‘inzake aanvullende maatregelen ter bestrijding van terrorisme’, en, in hoofdstuk IV, afdeling 12, van de wet van 5 augustus 1992, van onderafdeling 7bis, met daarin de artikelen 44/11/3bis tot 44/11/3quinquies/2, ingevoegd bij de wet van 27 april 2016 en gewijzigd bij de wet van 22 mei 2019 ‘tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft’.

⁸ *Parl.St.* Kamer 2015-16, nr. 54-1727/001, 89 e.v.

van de wet op het politieambt'. Wat betreft de bepalingen van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens' die worden aangevuld of waarnaar wordt verwezen, gaat het om advies 63.192/2 van 19 april 2018 over een voorontwerp dat heeft geleid tot die voornoemde wet.⁹⁻¹⁰ Hetzelfde geldt voor advies 63.480/2 van 6 juni 2018 over een voorontwerp dat heeft geleid tot de wet van 30 juli 2018 'tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme'.¹¹⁻¹²

De tabel met de overeenstemming tussen de artikelen, de memorie van toelichting en de bespreking van de artikelen moeten worden aangevuld met een verwijzing naar de voornoemde adviezen.

3. Gelijktijdig met het voorliggende voorontwerp van wet is een ontwerp van koninklijk besluit 'betreffende de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.")' aan de afdeling Wetgeving voorgelegd.

In advies 73.443/2 van 3 mei 2023 werd gesteld dat die adviesaanvraag voorbarig was omdat als rechtsgrond voor dat ontwerp van koninklijk besluit wetgevende bepalingen werden opgegeven die in het voorontwerp staan waarover dit advies gegeven wordt, en die *a fortiori* nog niet waren aangenomen.¹³

Aangezien een nieuwe op zichzelf staande wetgevende tekst wordt ontworpen die bestaande wettelijke en verordenende bepalingen samenbrengt, dient te worden voorzien dat de bepalingen die afkomstig zijn van het koninklijk besluit van 21 juli 2016 'betreffende de gemeenschappelijke gegevensbank Terrorist Fighters'¹⁴ en van het koninklijk besluit van 23 april 2018 'betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt' worden opgeheven op dezelfde datum als de datum van inwerkingtreding van het voorontwerp.

⁹ Parl.St. Kamer 2017-18, nr. 54-3126/001, 402 e.v.

¹⁰ De artikelen 34 tot 49 strekken tot aanvulling, wat de gemeenschappelijke gegevensbank T.E.R. betreft, van de bestaande bepalingen van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens'.

¹¹ Parl.St. Kamer 2017-18, nr. 54-3209/001, 14 e.v.

¹² Artikel 50 strekt alleen tot aanpassing van de verwijzingen vervat in artikel 4 van de wet van 30 juli 2018 'tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme'.

¹³ Dat advies is op de datum waarop dit advies wordt gegeven, nog niet bekendgemaakt.

¹⁴ Krachtens artikel 1 van het koninklijk besluit van 23 april 2018 'tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank *Foreign Terrorist Fighters* en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank *Foreign Terrorist Fighters* naar de gemeenschappelijke gegevensbank *Terrorist Fighters*,
« [wordt] het opschrift van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank *Foreign Terrorist Fighters* en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt (...) vervangen als volgt: 'Koninklijk besluit betreffende de gemeenschappelijke gegevensbank *Terrorist Fighters*.' »

ALGEMENE OPMERKINGEN

I. ALGEMEEN KADER WAARBINNEN BEPERKINGEN VAN RECHTEN EN VRIJHEDEN OP GROND VAN DE BESTRIJDING VAN TERRORISME KUNNEN WORDEN AANVAARD

De gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) impliceert beperkingen van het recht op eerbiediging van het privéleven, dat wordt gewaarborgd bij artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens.

In advies 58.729/AV van 26 januari 2016 over een voorontwerp dat heeft geleid tot de wet van 27 april 2016 ‘inzake aanvullende maatregelen ter bestrijding van terrorisme’ heeft de afdeling Wetgeving op het volgende gewezen:

“De bestrijding van terrorisme is onmiskenbaar één van de wettige redenen die beperkingen van die vrijheden kunnen rechtvaardigen.

Toen het Europees Hof voor de Rechten van de Mens zich diende te buigen over de beperkingen die op grond daarvan aan de rechten van de mens werden opgelegd, heeft dat Hof eraan herinnerd

‘qu’elle est pleinement consciente des difficultés que les États rencontrent pour protéger leur population contre la violence terroriste, laquelle constitue en elle-même une grave menace pour les droits de l’homme. Elle se garde donc de sous-estimer l’ampleur du danger que représente le terrorisme et la menace qu’il fait peser sur la collectivité (*Othman (Abu Qatada) c. Royaume-Uni*, n° 8139/09, § 183, CEDH 2012 (extraits), et références citées). Elle considère qu’il est légitime, devant une telle menace, que les États contractants fassent preuve d’une grande fermeté à l’égard de ceux qui contribuent à des actes de terrorisme (*idem*).’¹⁵

Er wordt eveneens verwezen naar het arrest *Szabo en Vissy t. Hongarije* dat op 12 januari 2016 door het Europees Hof voor de Rechten van de Mens is uitgesproken en waarin een actuele synthese wordt gemaakt van de rechtsregels en de beginselen met betrekking tot de bescherming van de persoonlijke levenssfeer die van toepassing zijn op het vlak van de bestrijding van terrorisme.

In de richtsnoeren van het Comité van Ministers van de Raad van Europa ‘over de rechten van de mens en de bestrijding van terrorisme’ wordt over het evenwicht dat moet worden nagestreefd tussen de belangen van de samenleving in haar geheel en de in het geding zijnde individuele rechten het volgende vermeld:¹⁶

‘Le Comité des Ministres,

[a.] Considérant que le terrorisme porte gravement atteinte aux droits de l’homme, menace la démocratie et vise notamment à déstabiliser des gouvernements légitimement constitués et à saper la société civile pluraliste;

[b.] Condamnant catégoriquement comme criminels et injustifiables tous les actes, méthodes ou pratiques terroristes, où qu’ils se produisent et quels qu’en soient les auteurs;

¹⁵ Voetnoot 10 van het geciteerde advies: EHRM inzonderheid 4 september 2014, *Trabelsi t. België*, § 117.

¹⁶ Voetnoot 11 van het geciteerde advies: Hierna worden alleen de *in casu* meest relevante passages van die richtsnoeren opgenomen.

[c.] Rappelant qu'un acte terroriste ne peut jamais être excusé ou justifié en invoquant les droits de l'homme et que l'abus de droit n'est jamais protégé;

[d.] Rappelant qu'il est non seulement possible, mais absolument nécessaire, de lutter contre le terrorisme dans le respect des droits de l'homme, de la prééminence du droit et, lorsqu'il est applicable, du droit international humanitaire;

[e.] Rappelant la nécessité pour les États de tout mettre en œuvre, et notamment de coopérer, afin que les auteurs, organisateurs et commanditaires présumés d'actes terroristes soient traduits en justice pour répondre de toutes les conséquences, notamment pénales et civiles, de leurs actes;

[f.] Réaffirmant le devoir impératif des États de protéger les populations contre d'éventuels actes terroristes;

[g.] Rappelant la nécessité pour les États, notamment pour des raisons d'équité et de solidarité sociale, de veiller à ce que les victimes d'actes terroristes puissent obtenir un dédommagement;

[h.] Gardant à l'esprit que la lutte contre le terrorisme implique des mesures à long terme visant à prévenir les causes du terrorisme, en favorisant notamment la cohésion de nos sociétés et le dialogue multiculturel et inter-religieux;

[i.] Réaffirmant l'obligation des États de respecter, dans leur lutte contre le terrorisme, les instruments internationaux de protection des droits de l'homme, et pour les États membres, tout particulièrement la Convention de Sauvegarde des Droits de l'Homme et des Libertés fondamentales ainsi que la jurisprudence de la Cour européenne des Droits de l'Homme;

Adopte les lignes directrices suivantes et invite les États membres à en assurer une large diffusion auprès de toutes les autorités chargées de la lutte contre le terrorisme.

I. *Obligation des États de protéger toute personne contre le terrorisme* - Les États ont l'obligation de prendre les mesures nécessaires pour protéger les droits fondamentaux des personnes relevant de leur juridiction à l'encontre des actes terroristes, tout particulièrement leur droit à la vie. Cette obligation positive justifie pleinement la lutte des États contre le terrorisme, dans le respect des présentes lignes directrices.

II. *Interdiction de l'arbitraire* - Les mesures prises par les États pour lutter contre le terrorisme doivent respecter les droits de l'homme et le principe de la prééminence du droit, en excluant tout arbitraire ainsi que tout traitement discriminatoire ou raciste, et faire l'objet d'un contrôle approprié.

III. *Légalité des mesures anti-terroristes* - 1. Toute mesure prise par les États pour lutter contre le terrorisme doit avoir une base juridique.

2. Lorsqu'une mesure restreint les droits de l'homme, les restrictions doivent être définies de façon aussi précise que possible et être nécessaires et proportionnées au but poursuivi.

(...)

V. *Collecte et traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État* - Dans le cadre de la lutte contre le terrorisme, la collecte et le traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État ne peuvent porter atteinte au respect de la vie privée des personnes que si la collecte et le traitement sont, notamment:

- (i) régis par des dispositions appropriées en droit interne;
- (ii) proportionnés à l'objectif pour lequel cette collecte et ce traitement ont été prévus;
- (iii) susceptibles d'un contrôle par une autorité externe indépendante.

VI. *Mesures d'ingérence dans la vie privée* - 1. Les mesures dans la lutte contre le terrorisme qui constituent une ingérence dans la vie privée (notamment, les fouilles, les perquisitions, les écoutes, les écoutes téléphoniques, la surveillance de la correspondance et le recours à l'infiltration d'agents) doivent être prévues par la loi. Ces mesures doivent pouvoir faire l'objet d'un contrôle juridictionnel.

2. Les mesures prises pour lutter contre le terrorisme doivent être préparées et contrôlées par les autorités de façon à réduire au minimum, autant que faire se peut, le recours à la force meurtrière et, dans ce cadre, l'utilisation d'armes par les forces de sécurité doit être rigoureusement proportionnée à la défense d'autrui contre la violence illégale ou à la nécessité de procéder à une arrestation régulière.

VII. *Arrestation et garde à vue* - 1. L'arrestation d'une personne soupçonnée d'activités terroristes ne peut intervenir en l'absence de soupçons plausibles. Les motifs de l'arrestation doivent être communiqués à la personne arrêtée.

2. Une personne arrêtée ou détenue pour activités terroristes doit être aussitôt traduite devant un juge. La garde à vue doit être d'une durée raisonnable et son terme doit être fixé par la loi.

3. Une personne arrêtée ou détenue pour activités terroristes doit pouvoir contester la légalité de son arrestation ou de sa garde à vue devant un tribunal.

(...)'.”¹⁷

In zoverre de bepalingen van het voorontwerp een bestaand juridisch dispositief inzake terrorismebestrijding aanvullen, moeten ze eveneens worden onderzocht in het licht van die regels en beginselen, zoals die nog in herinnering zijn gebracht in arrest-*Big Brother Watch e.a. t. Verenigd Koninkrijk*, uitgesproken op 25 mei 2021 door de Grote Kamer van het Europees Hof voor de Rechten van de Mens.

Meer in het bijzonder gaat het bijvoorbeeld om de nieuwe bepalingen die ertoe strekken partnerdiensten toe te voegen aan de bestaande lijst die is opgenomen in de wet van 5 augustus 1992 ‘op het politieambt’ (artikel 2, 3°, van het voorontwerp), om het feit dat de categorieën van entiteiten worden bepaald door de Koning (artikelen 2, 4°, en 6, § 2, vierde lid, van het voorontwerp), dat een “entiteit” een minderjarige ouder dan twaalf jaar kan zijn (lees: “van twaalf jaar en ouder”)¹⁸ (artikel 2, 4°, van het voorontwerp) of dat de gemeenschappelijke gegevensbank T.E.R. gegevens kan bevatten over een minderjarige (artikel 6, § 2, eerste lid, 1°, 1),

¹⁷ Advies 58.729/AV van 26 januari 2016 over een voorontwerp dat heeft geleid tot de wet van 27 april 2016 ‘inzake aanvullende maatregelen ter bestrijding van terrorisme’ (*Parl.St.* Kamer 2015-16, nr. 54-1727/001, 89 e.v.).

¹⁸ Bijzondere opmerking 2 bij artikel 2.

b), van het voorontwerp). Voorts gaat het om de toevoeging van de doelstelling van het gecoördineerde overleg tussen de basisdiensten en de partnerdiensten (artikel 5, tweede lid, 1°, van het voorontwerp), het verzamelen van gezondheidsgegevens en de mededeling aan de zorgverlener (artikel 6, § 2, tweede en derde lid, van het voorontwerp), de verschillende termijnen voor de bewaring van de gegevens over minderjarigen (artikel 7, § 1, van het voorontwerp), de koppeling aan andere gegevensbanken waaronder authentieke gegevensbronnen (artikel 7 van het voorontwerp), het begrip “inbreuken op de beveiliging” (artikel 13 van het voorontwerp), de omstandigheid dat de dreigingsevaluatie wordt meegedeeld aan de partnerdiensten bij de uitoefening van het vraagrecht (artikel 23 van het voorontwerp), de beschrijving van de inhoud van de evaluatie die moet worden uitgevoerd vóór de mededeling van de informatiekaart aan een derde overheid of instelling (artikel 24, tweede lid, van het voorontwerp), de validering van de dreigingsevaluatie door het OCAD (artikel 27, eerste lid, van het voorontwerp) of nog de oprichting van “lokale task forces” (lees: “lokale taskforces”), afgekort “LTF”, waarin veiligheidsprofessionals samen de wenselijkheid onderzoeken van het nemen van maatregelen ten aanzien van een geregistreerde entiteit (artikelen 31 tot 33 van het voorontwerp).

II. VERWERKING VAN PERSOONSGEGEVENS

A. Afstemming van de regels inzake gegevensbescherming vervat in het voorontwerp op de regels vervat in de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’

Enerzijds werkt het voorontwerp een op zichzelf staand dispositief uit ten opzichte van de wet ‘op het politieambt’,¹⁹ dat ertoe strekt de gemeenschappelijke gegevensbank T.E.R. op te richten, en anderzijds wijzigt het onder meer bepalingen in de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’.

In de bespreking van de artikelen 4 en 34 wordt daarover het volgende gezegd:

“Dit wetsontwerp regelt de gegevensbeschermingskwesties die specifiek zijn voor de verwerking van gegevens in de gemeenschappelijke gegevensbank T.E.R., namelijk welke soorten persoonsgegevens daar worden verwerkt, voor welke doeleinden, hoe lang, wie verantwoordelijk is voor de verwerking, welke autoriteiten de databank moeten voeden, met welke categorieën gegevens, welke categorieën autoriteiten toegang kunnen krijgen tot of mededeling kunnen doen van alle of een deel van de gegevens, de verplichting om de gegevens vast te leggen, en welke gegevensbeschermingsautoriteiten bevoegd zijn.

Voorts heeft de wetgever met het oog op de samenhang ervoor gekozen om de andere regels inzake gegevensbescherming (verplichting van de voor de verwerking verantwoordelijken, keuze van een verwerker, rechten van de betrokkenen, ...) naar analogie te relateren aan titel 3, subtitel 4, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, die gewijd is aan de verwerking van persoonsgegevens door het OCAD. Hoewel de context rond de verwerkingen van persoonsgegevens door het OCAD door middel van de eigen informatiesystemen ervan sterk verschilt van de specifieke context

¹⁹ Dat heeft ook een wijziging tot gevolg van het statuut van het personeel dat zal worden ingezet voor het beheer van de gemeenschappelijke gegevensbank, aangezien dat personeel niet meer onder de regeling van artikel 184 van de Grondwet zal vallen.

rond de verwerkingen van persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R., vinden we in beide gevallen een mutualisering terug van persoonsgegevens en informatie afkomstig van verwerkingsverantwoordelijken die niet allemaal onderworpen zijn aan dezelfde verplichtingen inzake bescherming van persoonsgegevens. Om een zo groot mogelijke rechtszekerheid te waarborgen maar ook op het stuk van leesbaarheid voor de betrokken personen – en bijgevolg om de uitoefening van hun rechten te vergemakkelijken, moet een gemeenschappelijke regeling voor die verwerkingen worden bepaald.”

Wat betreft de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de gemeenschappelijke gegevensbank T.E.R., blijkt uit het voorgaande dat het op zichzelf staande dispositief dat in het voorontwerp wordt ontworpen en de artikelen 138 tot 167 van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’ zoals ze bij het voorontwerp worden gewijzigd – en onder voorbehoud van de afwijkingen waarin het voorontwerp voorziet – aanvullend van toepassing zijn, en zo alle regels in verband met de verwerking van persoonsgegevens bevatten die voor de betreffende verwerkingen gelden in het licht van het recht op eerbiediging van het privéleven en de toelaatbaarheid van inmengingen in de uitoefening van dat recht in deze aangelegenheid.

Men stelt echter met name het volgende vast:

– artikel 4, tweede lid, stelt dat, in afwijking van artikel 162 van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’, de raadpleging van de persoonsgegevens en de informatie geregistreerd in de gemeenschappelijke gegevensbank T.E.R. voor een verdere verwerking voor historische, wetenschappelijke of statistische doeleinden, wordt toegestaan door de operationeel verantwoordelijke na overleg met de basisdiensten; artikel 46 van het voorontwerp strekt er echter toe het voornoemde artikel 162 aan te vullen met een lid dat een identieke afwijking bevat;²⁰

– artikel 7, § 2, vijfde lid, is overbodig aangezien in artikel 4, eerste lid, van het voorontwerp al wordt bepaald dat de regels inzake de gegevensbescherming en inzake de rechten van de betrokken persoon die zijn welke worden bedoeld in titel 3, ondertitel 4, van de voornoemde wet van 30 juli 2018, waartoe de artikelen 162 tot 167 behoren, die betrekking hebben op de verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden;

– artikel 29, § 3, 4°, en § 4, is een overbodige parafrase van artikel 157, § 3, tweede lid, en § 4, van dezelfde wet van 30 juli 2018.

²⁰ Zie ook de opmerking bij artikel 46.

Op een vraag daarover heeft de gemachtigde van de minister het volgende geantwoord:

“Il faut bien entendu éviter de répéter la [loi du 30 juillet 2018 relative à la relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel dans la loi [relative à la banque de données commune]. Les articles du projet de loi (...) vont être comparés avec le titre III de la loi sur la protection des données pour s'assurer qu'il n'y a pas de double emploi.”

Het voorontwerp moet in die zin worden herzien.

B. Het legaliteitsbeginsel en het evenredigheidsbeginsel in verband met een verwerking van persoonsgegevens

1. De werkwijze van de gemeenschappelijke gegevensbank T.E.R. impliceert een verwerking van persoonsgegevens. Deze dient te worden onderzocht in het licht van het legaliteitsbeginsel en het evenredigheidsbeginsel, die, wat het recht op eerbiediging van het privéleven betreft, voortvloeien uit artikel 22 van de Grondwet en uit artikel 8 van het Europees Verdrag voor de rechten van de mens.

B.1. Legaliteitsbeginsel

2.1. Over het legaliteitsbeginsel ter zake heeft de afdeling Wetgeving in haar advies 70.542/AV van 24 december 2021 over een voorontwerp van wet ‘betreffende de verplichte vaccinatie tegen COVID-19 van gezondheidszorgbeoefenaars’ het volgende opgemerkt:

“62. Om in het licht van de voornoemde bepalingen aanvaardbaar te zijn, moet de inmenging in het recht op eerbiediging van het privéleven geformuleerd worden in duidelijke en voldoende nauwkeurige bewoordingen die het mogelijk maken te voorzien in welke gevallen de wetgever een dergelijke inmenging toestaat. Elke inmenging in het recht op eerbiediging van het privéleven moet bovendien steunen op een objectieve en redelijke verantwoording en bijgevolg evenredig zijn met de door de wetgever nagestreefde doelstellingen.²¹ Hoewel met de inmengingen waarin voorliggend voorontwerp van wet voorziet een legitiem doel nagestreefd wordt (cf. *supra*, opmerkingen 43 tot 45), dient nagegaan te worden of aan de vereisten van legaliteit (i), relevantie en proportionaliteit (ii) voldaan wordt.

i) Legaliteit

²¹ Voetnoot 122 van het geciteerde advies: Adv.RvS 63.192/2 van 19 april 2018 over een voorontwerp dat heeft geleid tot de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’, *Parl.St.* Kamer 2017-18, nr. 54-3126/001, 402 tot 456, <http://www.raadvst-consetat.be/dbx/adviezen/63192.pdf>; adv.RvS 63.202/2 van 26 april 2018 verstrekt over een voorontwerp dat heeft geleid tot de wet van 5 september 2018 ‘tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG’, *Parl.St.* Kamer 2017-18, nr. 54-3185/001, 120 tot 145, <http://www.raadvstconsetat.be/dbx/adviezen/63202.pdf>.

63. Met betrekking tot het legaliteitsbeginsel, dat onlosmakelijk verbonden is met het recht op eerbiediging van het privéleven gewaarborgd in artikel 22 van de Grondwet, heeft de algemene vergadering van de afdeling Wetgeving het volgende uiteengezet in voornoemd advies 68.936/AV [van 7 april 2021 over een voorontwerp dat geleid heeft tot de wet van 14 augustus 2021 ‘betreffende de maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie’]²²:

‘Krachtens artikel 22 van de Grondwet geldt voor elke verwerking van persoonsgegevens en, meer in het algemeen, voor elke schending van het recht op het privéleven, dat het formeel legaliteitsbeginsel²³ dient te worden nageleefd.

Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering. Een delegatie aan een andere macht is evenwel niet in strijd met het wettelijkheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de ‘essentiële elementen’ voorafgaandelijk door de wetgever vastgesteld zijn.²⁴

Bijgevolg moeten de ‘essentiële elementen’ van de verwerking van persoonsgegevens in de wet zelf worden vastgelegd. In dat verband is de afdeling Wetgeving van oordeel dat ongeacht de aard van de betrokken aangelegenheid, de volgende elementen in beginsel ‘essentiële elementen’ uitmaken : 1°) de categorie van verwerkte gegevens; 2°) de categorie van betrokken personen; 3°) de met de verwerking nagestreefde doelstelling; 4°) de categorie van personen die toegang hebben tot de verwerkte gegevens; en 5°) de maximumtermijn voor het bewaren van de gegevens.’²⁵,²⁶

Het Grondwettelijk Hof heeft zich in dezelfde zin uitgesproken in zijn arresten nr. 33/2022 van 10 maart 2022²⁷ en nr. 110/2022 van 22 september 2022.²⁸

²² *Parl.St.* Kamer 2021-22, nr. 55-2533/001, 57 e.v.

²³ *Voetnoot 123 van het geciteerde advies*: Voetnoot 174 van het geciteerde advies: Wat dit beginsel betreft, zie *supra* randnummers 70 en v.

²⁴ *Voetnoot 124 van het geciteerde advies*: Voetnoot 175 van het geciteerde advies: Vaste rechtspraak van het Grondwettelijk Hof: zie inzonderheid GwH 18 maart 2010, nr. 29/2010, B.16.1; GwH 20 februari 2020, nr. 27/2020, B.17.

²⁵ *Voetnoot 125 van het geciteerde advies*: Voornoemd adv.RvS 68.936/AV, opmerking 101 (*Parl.St.* Kamer 2020-21, nr. 55-1951/001, 119 ; <http://www.raadvst-consetat.be/dbx/avis/68936.pdf>).

²⁶ Advies 70.542/AV van 24 december 2021 over een voorontwerp van wet ‘betreffende de verplichte vaccinatie tegen COVID-19 van gezondheidszorgbeoefenaars’, opmerkingen 62 en 63 (*Parl.St.* Kamer 2021-22, nr. 55-2533/001, 98 en 99).

²⁷ GwH 10 maart 2022, nr. 33/2022, B.13.1.

²⁸ GwH 22 september 2022, nr. 110/2022, B.11.2.

2.2. Er dient te worden vastgesteld dat de ontworpen tekst inderdaad verschillende essentiële elementen vermeldt betreffende de gegevensverwerking in het kader van de gemeenschappelijke gegevensbank T.E.R.:

- de categorieën van persoonsgegevens die daarin worden verwerkt (artikel 6, § 2) (onder voorbehoud van de kritiek die in de opmerkingen 2.5 tot 2.7, *infra*, wordt geformuleerd);

- de nagestreefde doeleinden (artikel 5, tweede lid) (onder voorbehoud van de kritiek die in opmerking 2.8, *infra*, wordt geformuleerd);

- de bewaartermijn (artikel 7, §§ 1 en 2);

- de categorieën van personen die toegang hebben tot de verwerkte gegevens (artikelen 15, 16, 17 en 21 tot 28).

Het voorontwerp stelt voorts andere gegevens vast, hoewel die geen essentiële elementen zijn in de zin van de bovenvermelde adviespraktijk en rechtspraak:

- de verantwoordelijke voor de verwerking (artikel 5, eerste lid);

- de logbestanden van de gegevens (artikel 8);

- de regels betreffende de functionaris voor gegevensbescherming en betreffende de verantwoordelijkheid voor de kwaliteit van de persoonsgegevens en voor de geregistreerde informatie (artikelen 29 en 30).

2.3. Ten aanzien van het legaliteitsbeginsel geeft het ontworpen dispositief evenwel aanleiding tot de volgende punten van kritiek:

a) Wat betreft de categorieën van personen wier persoonsgegevens worden verwerkt

2.4. De artikelen 2, 4°, en 6, § 2, vierde lid, van het voorontwerp belasten de Koning ermee bij een besluit vastgesteld na overleg in de Ministerraad de categorieën van “entiteiten” te bepalen waarvan de in het eerste lid van die laatstgenoemde bepaling vermelde gegevens worden verwerkt. Artikel 6, § 1, verwijst dan weer naar “personen, groeperingen, organisaties en fenomenen” in plaats van naar “entiteiten” en lijkt op die manier een andere inhoud te geven aan de categorie van personen wier persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R. zullen worden verwerkt. Dat creëert onduidelijkheid.

Naar aanleiding van een vraag daarover heeft de gemachtigde van de minister uitgelegd dat de categorieën van personen wier persoonsgegevens mogen worden verwerkt, betrekking hebben op vijf categorieën van entiteiten, die opgesomd zullen worden in het koninklijk besluit dat ter uitvoering van artikel 6, § 2, vierde lid, van het voorontwerp, moet worden vastgesteld, te weten:

- 1° de *foreign terrorist fighters*;
- 2° de *homegrown terrorist fighters*;
- 3° de potentieel gewelddadige extremisten;
- 4° de terrorismeveroordeelden;
- 5° de haatpropagandisten.

In de laatste alinea van de bespreking van artikel 6 staat het volgende te lezen:

“Artikel 6, § 2, vierde lid, machtigt de Koning ertoe, bij een in Ministerraad overlegd besluit, de categorieën van entiteiten te bepalen waarvan de in het vorige lid bedoelde gegevens verwerkt worden. Aangezien die categorieën kunnen evolueren op grond van de operationele, tactische of strategische behoeften, is het derhalve wenselijk om deze bij koninklijk besluit te bepalen. Momenteel gaat het om de volgende categorieën: de ‘Foreign Terrorist Fighters’, de ‘Homegrown Terrorist Fighters’, de ‘Haatpropagandisten’, de ‘Potentieel Gewelddadige Extremisten’, de ‘Terrorismeveroordeelden’ en de entiteiten in ‘vooronderzoek’, d.w.z. die, op het ogenblik van hun registratie in de gegevensbank T.E.R., niet beantwoorden aan de criteria om als een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist of haatpropagandist beschouwd te worden (...).”

De categorieën van “entiteiten” vormen een kernaspect en dus een essentieel element van het ontworpen dispositief, dat bijgevolg door de wetgever dient te worden vastgesteld.

De omstandigheid dat die categorieën van “entiteiten” kunnen evolueren in functie van de operationele, tactische of strategische behoeften, kan op zich niet rechtvaardigen dat de Koning op zo’n essentieel punt een machtiging wordt verleend, des te minder daar het aantal categorieën van entiteiten niet enkel wordt vastgesteld maar ook wordt beperkt.

Voorts wil de steller van het voorontwerp, zoals uit de bespreking van artikel 6 blijkt, de “entiteiten in ‘vooronderzoek’” opnemen in het toepassingsgebied van de categorieën van personen wier persoonsgegevens worden verwerkt. In dat verband wordt in diezelfde bespreking gepreciseerd wat het doel is van de periode van vooronderzoek:

“(…) Voor de entiteiten in ‘vooronderzoek’ moet worden gespecificeerd dat het doel van die periode van ‘vooronderzoek’ namelijk is om tijdelijk (maximaal zes maanden) maar gecentraliseerd in één enkel informatieverwerkingssysteem gegevens en informatie te kunnen inzamelen die al dan niet een validering van de betrokken entiteit als foreign terrorist fighter, homegrown terrorist fighter, potentieel gewelddadige extremist of haatpropagandist zullen onderbouwen (‘verrijkingsfase’). Na afloop ervan zal het OCAD, op basis van de beschikbare informatie/inlichtingen, evalueren of de wettelijke criteria al dan niet vervuld zijn. Indien deze niet vervuld zijn, zal de entiteit in vooronderzoek automatisch gearchiveerd worden. Het betreft bijgevolg een tijdelijke situatie. Na afloop ervan zal deze entiteit al dan niet in de gemeenschappelijke gegevensbank T.E.R. geregistreerd blijven.”

In het ontworpen dispositief wordt het begrip “vooronderzoek” echter op geen enkele wijze afgebakend, en wordt evenmin iets bepaald in verband met de juridische regeling die zou gelden voor de “entiteiten” die onder die categorie vallen.

Er wordt aan herinnerd dat men steeds duidelijk de verschillende gevallen moet kunnen voorzien waarin de wetgever een inmenging in het recht op eerbiediging van het privéleven toestaat. Daartoe dient het voorontwerp te bepalen voor welke categorieën van personen, die in het voorontwerp “entiteiten” worden genoemd, kan worden aanvaard dat de verschillende categorieën van persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R worden verzameld.

De artikelen 2, 4°, en 6, §§ 1 en 2, vierde lid, moeten in die zin worden herzien.

Ook moet in het dispositief aanvullend worden gepreciseerd welke juridische regeling van toepassing is op de categorie “entiteiten” in “vooronderzoek”, een begrip dat overigens nog dient te worden gedefinieerd.

2.5. Artikel 6, § 2, eerste lid, 1°, 1), b), van het voorontwerp verleent een machtiging aan de Koning voor wat betreft de gegevens betreffende de biologische of geadopteerde minderjarige kinderen van een natuurlijke persoon-“entiteit” die in de gemeenschappelijke gegevensbank T.E.R. is geregistreerd.

De bespreking van die bepaling bevat belangrijke aanvullende informatie: ze stelt dat die bepaling enkel betrekking heeft op minderjarige kinderen die in een jihadistisch conflictgebied verblijven of hebben verbleven.

Op een vraag daarover heeft de gemachtigde van de minister geantwoord dat dat momenteel inderdaad het enige geval is dat wordt beoogd. Ze geeft daarvoor de volgende uitleg:

“(…) dans le but de les identifier de manière certaine, les données d’identification visées des enfants mineurs des deux catégories d’entités suivantes, seront enregistrées dans la [banque de données commune] T.E.R.:

1° les *foreigns terrorist fighters* qui se sont rendus dans une zone de conflit djihadiste (FTF catégorie 1);

2° les *foreigns terrorist fighters* qui sont en route vers la Belgique ou sont revenus en Belgique après s’être rendus dans une zone de conflit djihadiste (FTF catégorie 3).”

Aangezien de gevallen waarin persoonsgegevens van minderjarige kinderen mogen worden verwerkt in een gegevensbank zoals de gemeenschappelijke gegevensbank T.E.R., zo nauwkeurig mogelijk moeten worden omschreven, moeten die preciseringen met betrekking tot deze categorie van gegevens in het ontworpen dispositief worden opgenomen.

Artikel 6, § 2, eerste lid, 1°, 1°, b), moet dienovereenkomstig worden herzien.

b) Wat betreft de categorieën van verwerkte persoonsgegevens

2.6. In artikel 2, 4°, van het voorontwerp wordt het begrip “entiteit” gedefinieerd als

“elke meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon ouder dan twaalf jaar of elke rechtspersoon, feitelijke vereniging alsook alle aangewende middelen, bepaald door de Koning (...).”

In de bespreking van de bepaling wordt nader bepaald dat die term

“niet alleen [doelt] op natuurlijke en rechtspersonen, maar ook op vervoersmiddelen of gebruikte telefoon-/rekeningnummers.”

Daarin staat in dat verband nog het volgende te lezen:

“Het begrip ‘entiteit’ herneemt, behalve elke natuurlijke persoon of rechtspersoon of feitelijke vereniging, ook de middelen die aangewend worden. Deze middelen moeten worden opgevat als vectoren van radicalisering. Het is bij het begin van een onderzoek echter soms moeilijk om de entiteit te identificeren als een natuurlijke persoon, een rechtspersoon of als feitelijke vereniging. Het identificeren van het gebruikte middel (website, radio, pers, ...) is vaak eenvoudiger. In dit geval moeten de middelen zelf opgenomen worden in de gemeenschappelijke gegevensbank T.E.R. De opvolging van de aangewende middelen hernomen in de gegevensbank laat toe om desgewenst de gepaste maatregelen te nemen.”

Het volledige dispositief is aldus opgevat dat verwijzingen naar het begrip “entiteit” lijken te slaan op natuurlijke personen, rechtspersonen of feitelijke verenigingen waarvan de gegevens in de gemeenschappelijke gegevensbank T.E.R. kunnen worden verwerkt. Wanneer die gegevens betrekking hebben op natuurlijke personen, gaat het om persoonsgegevens in de zin van artikel 4, punt 1), van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 ‘betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)’ (verderop in het advies: “de AVG”) en in de zin van artikel 3, punt 1), van richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 ‘betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad’.²⁹⁻³⁰

Wanneer het dispositief de definitie van “entiteit” wil uitbreiden tot de definitie van “aangewende middelen”, gaat het echter veeleer om categorieën van gegevens dan om categorieën van personen of van verenigingen als zodanig. Gelet op die vaststelling hoort het begrip “aangewende middelen” veeleer thuis in artikel 6 van het voorontwerp, waar het dan zou moeten worden verduidelijkt, net zoals het geval is met de andere categorieën van gegevens die daar reeds worden vermeld, en rekening houdend met de bijzondere kenmerken van dat begrip, zoals blijkt uit de bespreking van de bepaling.

²⁹ Die richtlijn is omgezet bij titel 2 (“De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid”) van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’, zoals in artikel 25 van die wet wordt bevestigd.

Luidens artikel 1, lid 1, van richtlijn 2016/680 worden

“[b]ij deze richtlijn de regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid” (zie eveneens artikel 27 van de voornoemde wet van 30 juli 2018).

Sommige van de basis- en partnerdiensten die de in het voorontwerp bedoelde persoonsgegevens kunnen verwerken, vallen in het toepassingsgebied van het voorontwerp, tevens gelet op de doeleinden van die verwerkingen zoals ze in artikel 5, tweede lid, van het voorontwerp worden vermeld. Andere dergelijke diensten vallen onder de AVG (artikel 2, lid 1 en 2, d), van de AVG), met dien verstande dat voor de inlichtingen- en veiligheidsdiensten een bijzondere regeling geldt (artikel 3, lid 2, a), van richtlijn 2016/680; artikel 2, lid 2, a), van de AVG; zie de memorie van toelichting bij het ontwerp dat heeft geleid tot de voornoemde wet van 30 juli 2018, *Parl.St.* Kamer 2017-18, nr. 54-3126/001, met name 124 tot 126 en 128), waarin titel 3, ondertitel 1 (“De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten”), van de voornoemde wet van 30 juli 2018 voorziet.

³⁰ De definitie van het begrip “persoonsgegeven”, die het toepassingsgebied van dat begrip beperkt tot “natuurlijke personen” en die voortkomt uit de definitie vermeld in artikel 3, punt 1), van de richtlijn, staat ook in artikel 26, 1°, van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’.

Bijgevolg moeten de woorden “alsook alle aangewende middelen,” worden weggelaten uit de definitie van het begrip “entiteit” zoals die in artikel 2, 4°, van het voorontwerp staat; ook moet het woord “déterminés” in de Franse tekst worden vervangen door het woord “déterminées”.

2.7. De machtiging die bij artikel 9, § 1, tweede lid, van het voorontwerp aan de Koning wordt verleend, is te ruim geformuleerd. Zonder dat haar essentiële elementen worden omschreven, bepaalt ze namelijk dat de inhoud van de gemeenschappelijke gegevensbank T.E.R. wordt uitgebreid tot informatie die via een koppeling uit andere gegevensbanken afkomstig is, maar er wordt verzuimd de doeleinden van die koppeling, de onderling verbonden categorieën van persoonsgegevens en de regels inzake die koppeling vast te stellen.³¹

Bijgevolg moet artikel 9, § 1, tweede lid, worden herzien in het licht van het legaliteitsbeginsel, dat voortvloeit uit artikel 22 van de Grondwet, en van de vereisten voortvloeiend uit de AVG en uit richtlijn 2016/680.

c) Wat betreft de doeleinden van de verwerking van persoonsgegevens

2.8. Het tweede lid dat bij artikel 46 van het voorontwerp zou worden ingevoegd in artikel 162 van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’ bepaalt dat elk verzoek aan het Rijksarchief om verdere verwerking van persoonsgegevens die geregistreerd staan in de gemeenschappelijke gegevensbank T.E.R. voor andere dan historische, wetenschappelijke of statistische doeleinden, wordt geweigerd “tenzij het doel legitiem is”. Dat laatste wordt niet nader gepreciseerd.

Zoals hierboven in herinnering is gebracht,³² vormen de doeleinden van de verwerking van persoonsgegevens echter een essentieel element dat in de wet moet staan.

Het dispositief moet, in voorkomend geval, in die zin worden aangevuld in het licht van de voorbeelden aangehaald in de bespreking van de bepaling, waarin het volgende wordt gesteld:

“(…) Zo bijvoorbeeld bepaalt artikel 164 dat, indien gepseudonimiseerde gegevens niet toelaten om de historische doeleinden te verwezenlijken, het OCAD de raadpleging van ‘clear’ info kan toestaan indien dit geen onevenredige afbreuk doet aan het privéleven (het betreft dus een criterium waarmee de legitimiteit van de vraag kan worden beoordeeld). Voorts wordt in het kader van de parlementaire voorbereidingen voor de wet van 30 juli 2018 betreffende de bescherming van de persoonsgegevens in verband met artikel 99, tweede lid, bepaald: ‘Om te antwoorden op het advies van de Raad van State (pagina 35) wordt het tweede lid van dit artikel opnieuw geformuleerd: er wordt verduidelijkt dat een verdere verwerking zonder historische, statistische of wetenschappelijke doeleinden geweigerd wordt behalve indien het doeleinde wettelijk is en de raadpleging geen afbreuk kan doen aan de belangen bedoeld in het eerste lid. Zo moet het duidelijk zijn dat er geen sprake is van het toelaten van een doeleinde – deze dient op

³¹ Vergelijk met artikel 9, § 2, waarin wordt opgesomd in welke gevallen een koppeling met de gegevensbanken authentieke bronnen tot stand kan worden gebracht.

³² Algemene opmerking II, B, 2.1.

zich en voorafgaand wettelijk te zijn – maar wel een raadpleging van gegevens in bepaalde gevallen. Aangezien de criteria vastliggen betreft het geen[s]zins een discretionaire bevoegdheid. De modaliteiten zijn deze die zijn vastgelegd in huidig hoofdstuk en, desgevallend, in andere wetten (bijvoorbeeld de wet van 11 december 1998).”

B.2. Evenredigheidsbeginsel

3. Het Grondwettelijk Hof geeft de volgende expliciete invulling aan het evenredigheidsvereiste:

“B.12.1. Een overheidsinmenging in het recht op eerbiediging van het privéleven dient niet alleen te steunen op een voldoende precieze wettelijke bepaling, maar ook te beantwoorden aan een dwingende maatschappelijke behoefte in een democratische samenleving en evenredig te zijn met de daarmee nagestreefde wettige doelstelling.

De wetgever beschikt ter zake over een appreciatiemarge. Die appreciatiemarge is evenwel niet onbegrensd: opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk evenwicht heeft gevonden tussen alle rechten en belangen die in het geding zijn. Bij de beoordeling van dat evenwicht houdt het Europees Hof voor de Rechten van de Mens onder meer rekening met de bepalingen van het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (hierna: Verdrag nr. 108) en de aanbeveling nr. R (87) 15 van het Comité van Ministers aan de verdragsstaten tot regeling van het gebruik van persoonsgegevens in de politiesector (hierna: aanbeveling nr. R (87) 15) (EHRM, 25 februari 1997, *Z t. Finland*, § 95; grote kamer, 12 januari 2010, *S. en Marper t. Verenigd Koninkrijk*, § 103).

B.12.2. Een inmenging in het recht op eerbiediging van het privéleven door middel van een verwerking van persoonsgegevens, moet berusten op een redelijke verantwoording en dient evenredig te zijn met de door de wetgever nagestreefde doelstellingen. Wat de evenredigheid betreft, houdt het Europees Hof voor de Rechten van de Mens rekening met het al dan niet aanwezig zijn van waarborgen in de betrokken regeling ter voorkoming van misbruiken bij de verwerking van persoonsgegevens:

“35. De bescherming van persoonsgegevens speelt een fundamentele rol voor de uitoefening van het recht op eerbiediging van het privé- en gezinsleven, dat is vastgelegd bij artikel 8 van het Verdrag. De interne wetgeving moet dus in gepaste waarborgen voorzien om elk gebruik van persoonsgegevens dat niet zou overeenstemmen met de in dat artikel bepaalde waarborgen, te verhinderen. Die noodzaak is des te groter wanneer het gaat om de bescherming van persoonsgegevens die automatisch worden verwerkt, in het bijzonder wanneer die gegevens worden gebruikt voor politionele doeleinden. Het interne recht moet meer bepaald ervoor zorgen dat die gegevens ter zake dienend en niet overmatig zijn uitgaande van de doeleinden waarvoor zij worden opgeslagen, en dat zij worden bewaard in een zodanige vorm dat de betrokkene hierdoor niet langer te identificeren is dan strikt noodzakelijk is voor het doel waarvoor de gegevens zijn opgeslagen. Het interne recht moet ook waarborgen bevatten om de opgeslagen persoonsgegevens op doeltreffende wijze te beschermen tegen oneigenlijk gebruik en misbruik (*S. en Marper t. Verenigd Koninkrijk*, voormeld, § 103, *Gardel t. Frankrijk*, voormeld, § 62, EHRM 2009, en *M.K. t. Frankrijk*, voormeld, § 35).

36. Om het evenredige karakter van de bewaringstermijn van de informatie te beoordelen in het licht van het doel dat met het opslaan van die informatie wordt nagestreefd, houdt het Hof rekening met het al dan niet voorhanden zijn van een onafhankelijke controle op de verantwoording voor het behoud ervan in het verwerkingssysteem, controle die wordt uitgeoefend op grond van precieze criteria zoals de ernst van het misdrijf, de vroegere arrestaties, de mate van verdenking die op de persoon weegt, of enige andere bijzondere omstandigheid (*S. en Marper t. Verenigd Koninkrijk*, voormeld, § 119, en *B.B. t. Frankrijk*, voormeld, § 68).

37. Ten slotte komt het Hof toe bijzondere aandacht te hebben voor het risico van stigmatisering van personen die, zoals de verzoeker, niet schuldig zijn bevonden aan enig misdrijf en het vermoeden van onschuld kunnen genieten. Ook al staat, uit dat oogpunt, het bewaren van privégegevens niet gelijk met het uiten van een verdenking, toch mogen de voorwaarden van die bewaring niet de indruk geven dat die personen niet als onschuldig worden beschouwd (*S. en Marper*, voormeld, § 122, en *M.K.*, voormeld, § 36)' (EHRM, 18 september 2014, *Brunet t. Frankrijk*, §§ 35-37).

Bij de beoordeling van de evenredigheid van maatregelen met betrekking tot de verwerking van persoonsgegevens in databanken door de politiediensten, dient aldus rekening te worden gehouden met, onder meer, de pertinentie en het al dan niet buitensporige karakter van de gegevens die worden verwerkt, het al dan niet voorhanden zijn van maatregelen die de duur van de bewaring van de gegevens beperken, het al dan niet voorhanden zijn van een systeem van onafhankelijk toezicht dat toelaat na te gaan of de bewaring van de gegevens nog langer is vereist, het al dan niet voorhanden zijn van waarborgen ter voorkoming van stigmatisering van de personen van wie de gegevens worden verwerkt, en het al dan niet voorhanden zijn van waarborgen ter voorkoming van foutief gebruik door de politiediensten van de verwerkte persoonsgegevens (EHRM, grote kamer, 4 mei 2000, *Rotaru t. Roemenië*, § 59; grote kamer, 12 januari 2010, *S. en Marper t. Verenigd Koninkrijk*, §§ 101-103, 119, 122 en 124; 18 april 2013, *M.K. t. Frankrijk*, §§ 37 en 42-44)".³³

Zoals in de memorie van toelichting wordt uiteengezet, strekt het ontworpen dispositief tot precisering, explicitering en uitwerking van sommige aspecten die momenteel worden bepaald door de wet van 5 augustus 1992 'op het politieambt' of door de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens' om ervoor te zorgen dat de werkwijze van de gemeenschappelijke gegevensbank T.E.R. garanties inhoudt voor de gegevensbescherming.

In verband met de verwerking van persoonsgegevens wordt in artikel 6, § 1, als principe het volgende gesteld:

“De gemeenschappelijke gegevensbank T.E.R. vereist de verwerking van verschillende categorieën van persoonsgegevens met betrekking tot personen, groeperingen, organisaties en fenomenen die toereikend, ter zake dienend en niet overmatig zijn in verhouding tot de opdrachten bedoeld in artikel 3, en de doeleinden bedoeld in artikel 5, tweede lid.

De persoonsgegevens bedoeld in het eerste lid staan in rechtstreeks verband met het doeleinde van de verwerking.”

³³ GwH 14 juli 2016, nr. 108/2016, B.12.

Er wordt aan herinnerd dat de verwerking enkel mogelijk is als ze betrekking heeft op persoonsgegevens en informatie betreffende opdrachten inzake de voorkoming en de opvolging van terrorisme en van extremisme ingeval dat tot terrorisme kan leiden, als ze wordt verricht door de betrokken diensten binnen het exclusieve kader van hun wettelijke bevoegdheden (artikel 3, eerste lid, van het voorontwerp), en met strikte inachtneming van de vier doeleinden die in artikel 5, tweede lid, van het voorontwerp worden opgesomd (1° het gecoördineerde overleg tussen de basisdiensten en de partnerdiensten; 2° de strategische, tactische of operationele noodzaak om gezamenlijk persoonsgegevens en informatie te verwerken voor het uitoefenen van de respectieve opdrachten van de basisdiensten en de partnerdiensten; 3° de hulp bij het nemen van beslissingen door de bestuurlijke overheden of bij het nemen van beslissingen van bestuurlijke of gerechtelijke politie; 4° de analyse, de evaluatie en de opvolging, daaronder begrepen het nemen van maatregelen, van de in de gemeenschappelijke gegevensbank T.E.R. geregistreerde “entiteiten” en de analyse, de evaluatie en de opvolging van het fenomeen van terrorisme en extremisme ingeval het tot terrorisme kan leiden, op grond van een dreigingsevaluatie).

Wat de strikt noodzakelijke bewaringstermijn betreft, wordt bepaald dat de in de gemeenschappelijke gegevensbank T.E.R. bewaarde persoonsgegevens worden gearchiveerd vanaf het ogenblik dat de doeleinden bedoeld in artikel 5, tweede lid, niet meer worden bereikt, en ten hoogste dertig jaar na de laatste verwerking, met uitzondering van de persoonsgegevens van minderjarigen, die tot maximaal vijftien jaar na de laatste verwerking worden bewaard (artikel 7, § 1, van het voorontwerp). Na de laatste verwerking onderzoekt de operationeel verantwoordelijke (namelijk het Coördinatieorgaan voor de dreigingsanalyse, dat volgens de memorie van toelichting met toepassing van artikel 12 van het voorontwerp in deze hoedanigheid zal worden aangewezen) om de vijf jaar (om de drie jaar voor minderjarigen) of de persoonsgegevens nog steeds een rechtstreeks verband vertonen met een van de doeleinden van artikel 5, tweede lid, en, als dat niet het geval is, worden de gegevens gearchiveerd (artikel 7, § 1, tweede en derde lid, van het voorontwerp).

Om onrechtmatig gebruik van de gegevens te voorkomen, zal, blijkens de inlichtingen die de gemachtigde van minister heeft verstrekt, in uitvoering van artikel 6, § 2, vijfde lid, van het voorontwerp het volgende worden bepaald:

“Pour faciliter la gestion des accès, chaque service devra identifier les membres de son personnel autorisés à exercer les droits d'accès à la banque de données commune T.E.R. et devra transmettre une liste de ces personnes au gestionnaire qui gère les accès. Les membres du personnel doivent être titulaires d'une habilitation de sécurité de niveau 'secret' sauf pour les services de police afin de leur permettre d'évaluer correctement l'attitude à adopter à l'égard d'une personne dans les situations d'urgence” (zie voorts de inhoud van de logbestanden, beschreven in onder meer artikel 8, § 1, tweede lid, 2°, van het voorontwerp).

Tot slot zijn de toezichthoudende overheden, krachtens artikel 2, 15°, van het voorontwerp, het Controleorgaan op de politionele informatie, bedoeld in artikel 71 van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’, en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, bedoeld in artikel 1 van de wet van 18 juli 1991 ‘tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse’.

In het preventieve stadium van de controle die de afdeling Wetgeving van de Raad van State uitvoert, blijkt in dat verband niet dat het voorontwerp het evenredigheidsbeginsel, dat inherent is aan elke inmenging in het recht op eerbiediging van het privéleven, niet in acht zou nemen.

III. MACHTIGINGEN VERLEEND AAN DE KONING

1. Het voorontwerp verleent verscheidene machtigingen aan de Koning.

Voor wat betreft hun toelaatbaarheid in het licht van het legaliteitsbeginsel dat uit artikel 22 van de Grondwet voortvloeit, wordt verwezen naar de algemene opmerkingen 2.4 tot 2.7.

2. Voorts geven sommige machtigingen hoe dan ook aanleiding tot de volgende opmerking.

De gemachtigde van de minister heeft toegegeven dat verscheidene van die machtigingen overbodig blijken te zijn of andere machtigingen overlappen.

Dat is het geval met de machtigingen die in de volgende bepalingen vervat zijn:

– artikel 8, § 1, vierde lid:

“De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, andere types van verwerking bepalen waarvoor logbestanden moeten worden opgesteld;”

– artikel 10:

“De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, bijkomende nadere beheersregels van de gemeenschappelijke gegevensbank T.E.R. bepalen;”

– artikel 18, tweede lid:

“De Koning bepaalt, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, de nadere regels voor het creatierecht bedoeld in het eerste lid;”

– artikel 28, § 4:

“De Koning kan de nadere regels van de in § 2 en § 3 bedoelde mededeling bepalen;”

– artikel 29, § 2, 3°:

“Aanvullend op de bepalingen van artikel 157 van de wet gegevensbescherming wordt de functionaris voor gegevensbescherming belast met de volgende opdrachten:

(...)

3° het uitvoeren van andere opdrachten inzake de bescherming en beveiliging van gegevens die bepaald worden door de Koning of die hem door de ministers van Binnenlandse Zaken en Justitie worden toevertrouwd;”

– artikel 32, § 2, tweede lid:

“De Koning kan, bij een in Ministerraad overlegd besluit, andere opdrachten van de LTF bepalen;”

– artikel 54, eerste lid:

“De Koning kan de bestaande verwijzingen in wetten naar bepalingen van de wet op het politieambt vervangen door verwijzingen naar de ermee overeenstemmende bepalingen van deze wet.”

Die aan de Koning verleende machtigingen moeten worden weggelaten.

Bijgevolg worden ze verderop in dit advies niet onderzocht, ook niet wat betreft hun verenigbaarheid met het legaliteitsbeginsel.

BIJZONDERE OPMERKINGEN

Artikel 2

1. In de bespreking van artikel 2 wordt niet uitgelegd waarom het nodig is de in artikel 2, 3°, i) en j), beoogde diensten (respectievelijk “de dienst Erediensten en Vrijzinnigheid van de Federale Overheidsdienst Justitie” en “de Algemene administratie van de Thesaurie van de Federale Overheidsdienst Financiën”) te beschouwen als partnerdiensten.

Op een vraag daarover heeft de gemachtigde van de minister het volgende geantwoord:

“L'exposé des motifs sera précisé pour ces partenaires.

Pour le service des cultes, la motivation est la suivante : [l]e Service des Cultes et de la Laïcité du SPF Justice, service partenaire doit pouvoir bénéficier d'un droit d'interrogation dans la banque de données commune T.E.R. Le service des Cultes et de la Laïcité du SPF Justice est légalement compétent pour la reconnaissance des cultes et des organisations non confessionnelles. Il paie en outre les traitements des ministres des cultes et des délégués des communautés philosophiques non confessionnelles. Dans le cadre de ses compétences, il est nécessaire que ce service puisse interroger la banque de données commune T.E.R.

Pour la trésorerie, la motivation est la suivante : [l]'Administration générale de la Trésorerie, l'autorité compétente en matière de sanctions financières par le gel des fonds et des ressources économiques des personnes et entités qui commettent ou tentent de commettre des infractions terroristes, les facilitent ou y participent, aura un droit de lecture et d'écriture dans la banque de données commune T.E.R., en tant que service partenaire. La trésorerie est gestionnaire des sanctions financières et acquiert donc à cet effet la connaissance d'infractions et de données à caractère financier qui doivent être centralisées dans la banque de données commune pour assurer un échange de données intégré et optimal.

Dans la pratique, les avoirs de toutes les personnes qui ont rejoint un groupe terroriste en Syrie/Irak (FTF catégorie 1) ont été gelés. En outre, les avoirs d'un certain nombre d'autres entités ont déjà été gelés, notamment les avoirs de personnes condamnées pour des infractions terroristes. En outre, la Trésorerie est régulièrement contactée par des institutions financières lorsqu'elles entrent en contact avec des personnes dont les avoirs ont été gelés (ou pour lesquelles d'autres mesures financières ont été prises) par d'autres États (par exemple les États-Unis) dans un contexte de terrorisme, mais pas en Belgique. La Trésorerie doit procéder aux vérifications nécessaires et informer les institutions financières des conséquences éventuelles. L'un des éléments importants à cet égard est l'information consistant à savoir si la personne a été ou non reprise dans la banque de données commune T.E.R. La Trésorerie doit alors avoir la possibilité de vérifier quelles entités sont reprises en tant que telles dans la banque de données commune T.E.R.

Par ailleurs, l'Administration générale de la Trésorerie doit avoir la possibilité d'insérer elle-même les décisions qu'elle prend ainsi que de nombreuses informations pertinentes recueillies dans le cadre de sa compétence en matière de sanctions financières comme décrit dans l'arrêté royal du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme et la loi du 13 mai 2003 relative à la mise en œuvre des mesures restrictives adoptées par le Conseil de l'Union européenne à l'encontre d'États, de certaines personnes et entités. Sont visés ici : des montants financiers gelés, d'éventuels mouvements sur des comptes bancaires ou encore des assurances de tout type faisant l'objet d'une mesure de gel dans cette banque de données commune. Il est évident que ceci porte uniquement sur les informations relatives aux entités ayant déjà été reprises dans la Banque de données commune selon la procédure appropriée."

De memorie van toelichting en de bespreking moeten dienovereenkomstig worden aangevuld.

2. In artikel 2, 4°, wordt "entiteit" gedefinieerd als onder meer "elke meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon ouder dan twaalf jaar".

Luidens de bespreking van het artikel zijn de aldus beoogde personen minderjarigen van twaalf jaar of ouder³⁴ en niet "ouder dan twaalf jaar"; het dispositief moet in die zin worden herzien. Het is in het kader van die acceptie dat de hiernavolgende opmerking wordt geformuleerd.

Het voorontwerp voert aldus een verschil in behandeling in tussen minderjarigen onderling, met als gevolg dat dezen pas in de gemeenschappelijke gegevensbank T.E.R. zullen worden geregistreerd als ze de leeftijd van twaalf jaar hebben bereikt³⁵ én als daarbovenop de andere voorwaarden met betrekking tot de registratie van een entiteit worden vervuld.³⁶

³⁴ Zie hieronder.

³⁵ Onder voorbehoud van artikel 6, § 2, eerste lid, 1°, 1), b).

³⁶ Het is pas als er aanwijzingen zijn dat een persoon een gevaar vormt voor de nationale veiligheid, dat deze persoon in de gegevensbank wordt opgenomen (memorie van toelichting, 14).

In verband met een dergelijk dispositief moet worden gewezen op de hiernavolgende overwegingen van het Grondwettelijk Hof:

“B.148.1. (...) [E]en verwerking van persoonsgegevens in politionele databanken [kan] niet worden beschouwd als een strafbaarstelling, noch als een strafsanctie in de zin van de artikelen 12 en 14 van de Grondwet, aangezien zij slechts een maatregel van preventieve of onderzoekende aard is.

Door een verwerking van de persoonsgegevens van minderjarigen in de politionele databanken toe te laten, voert de bestreden wet aldus geen strafbaarstelling of strafsanctie in die zou afwijken van de bepalingen van de Jeugdbeschermingswet, die onverkort van toepassing blijft.

(...)

B.149. Zowel artikel 22bis, vierde lid, van de Grondwet als artikel 3, lid 1, van het Verdrag inzake de rechten van het kind verplichten de overheid om in de eerste plaats het belang van het kind in aanmerking te nemen bij elke beslissing die het kind aangaat. Artikel 22bis, vijfde lid, van de Grondwet geeft de wetgever overigens de opdracht te waarborgen dat het belang van het kind de eerste overweging is.

Die bepalingen verhinderen op zich de wetgever niet te bepalen dat persoonsgegevens van minderjarigen door de politiediensten kunnen worden verwerkt teneinde die diensten toe te laten hun wettelijke opdrachten te vervullen. Die opdrachten, die onder meer betrekking hebben op de handhaving van de openbare orde, de bescherming van personen en goederen en het voorkomen en het opsporen van misdrijven, houden, uit hun aard, niet uitsluitend verband met handelingen en gedragingen van meerderjarigen.

Niettemin dient de wetgever, bij het bepalen van de omstandigheden waarin persoonsgegevens door de politiediensten kunnen worden verwerkt, rekening te houden met de bijzondere situatie van de minderjarigen, onder meer op het vlak van hun persoonlijkheid en hun maturiteitsgraad.”³⁷

Over de keuze van de leeftijd vanaf wanneer een natuurlijke persoon kan worden geregistreerd in de gemeenschappelijke gegevensbank T.E.R. staat in de bespreking van artikel 2 het volgende:

“Dit wetsontwerp schept tevens meer duidelijkheid rond de criteria van de opname in de gegevensbank T.E.R. met betrekking tot de leeftijd van een natuurlijke persoon: meerderjarige natuurlijke personen en minderjarige natuurlijke personen vanaf twaalf jaar kunnen in de gemeenschappelijke gegevensbank T.E.R. worden opgenomen als ze voldoen aan de opnamecriteria. Minderjarigen jonger dan twaalf jaar worden dus niet als entiteit in de gemeenschappelijke gegevensbank T.E.R. opgenomen. Voor minderjarigen van twaalf tot en met achttien jaar wordt er bovendien in extra beschermingsmaatregelen voorzien. Zo bedraagt de maximale bewaringstermijn in de gemeenschappelijke gegevensbank T.E.R. na de laatste verwerking niet dertig maar vijftien jaar en moet de operationeel verantwoordelijke de noodzakelijkheid om de gegevens te archiveren die op hem betrekking hebben, minimaal om de drie jaar en niet om de vijf jaar evalueren. Tot slot is het zo dat bij de evaluatie vóór de mededeling van gegevens via een informatiekaart rekening moet worden gehouden met het statuut van minderjarige om te beoordelen of het noodzakelijk is om die mededeling te doen.

³⁷ GwH 14 juli 2016, nr. 108/2016, B.148.1 en B.149. Zie eveneens GwH 23 april 2015, nr. 44/2015, B.51.3.

Er werd geopteerd voor de ondergrens van twaalf jaar omdat dit een spilleeftijd die in verschillende wetgevingen wordt gehanteerd.

Vanaf die leeftijd kunnen immers maatregelen worden genomen ten aanzien van minderjarigen die verdacht worden van het plegen van een als misdrijf omschreven feit. Vóór die leeftijd wordt de voorkeur gegeven aan doorverwijzing naar hulpverlening aan minderjarigen in gevaar, en kan men het kind alleszins niet plaatsen op grond van het als misdrijf omschreven feit (art. 37, §2, van de wet van 8 april 1965 betreffende de jeugdbescherming, het ten laste nemen van minderjarigen die een als misdrijf omschreven feit hebben gepleegd en het herstel van de door dit feit veroorzaakte schade).

Overigens geldt twaalf jaar als de leeftijd vanaf wanneer een kind kan betrokken worden bij diverse procedures die het aanbelangen. Zo moet het kind bijvoorbeeld toestemmen in zijn adoptie (art. 348-1 van het Burgerlijk Wetboek), het moet gedagvaard worden om te verschijnen voor de jeugdrechtbank ingeval van procedure van minderjarige in gevaar of van minderjarige die wordt vervolgd wegens een als misdrijf omschreven feit (art. 46 van de wet van 8 april 1965 betreffende de jeugdbescherming, het ten laste nemen van minderjarigen die een als misdrijf omschreven feit hebben gepleegd en het herstel van de door dit feit veroorzaakte schade), en ook moet het kind ingelicht worden over zijn recht om gehoord te worden door de familierechtbank in de procedures aangaande het ouderlijk gezag (art. 1004/1 van het Gerechtelijk Wetboek).

Op internationaal niveau is het Comité voor de rechten van het kind (dat belast is met het toezicht op de toepassing van het Internationaal Verdrag inzake de Rechten van het Kind vanwege de Staten) zeer stellig geweest in zijn opmerkingen nr.10 (2017) betreffende de rechten van het kind binnen het rechtssysteem voor minderjarigen.

Het preciseert het volgende (nr. 32, bladzijde 54): ‘Rule 4 of the Beijing Rules recommends that the beginning of MACR [minimum age of criminal responsibility] shall not be fixed at too low an age level, bearing in mind the facts of emotional, mental and intellectual maturity. In line with this rule the Committee has recommended States parties not to set a MACR at a too low level and to increase the existing low MACR to an internationally acceptable level. From these recommendations, it can be concluded that a minimum age of criminal responsibility below the age of 12 years is considered by the Committee not to be internationally acceptable. States parties are encouraged to increase their lower MACR to the age of 12 years as the absolute minimum age and to continue to increase it to a higher age level’.

Het verschil in behandeling tussen de minderjarigen onderling naargelang ze al dan niet de leeftijd van twaalf jaar hebben bereikt, lijkt *in casu* ten aanzien van de rechtspraak van het Grondwettelijk Hof redelijkerwijze verantwoord, aangezien de wetgever bij het vaststellen van de minimumleeftijd van personen wier persoonsgegevens mogen worden verwerkt in een instrument zoals de gemeenschappelijke gegevensbank T.E.R., zich in principe kan laten leiden door de leeftijd van twaalf jaar die in de voornoemde wetten wordt vastgesteld.³⁸

³⁸ GwH 14 juli 2016, nr. 108/2016, B.145 tot B.156.

Artikel 6

1. Paragraaf 2, 1°, 1), a), ii., vermeldt als een van de categorieën van gegevens die mogen worden verwerkt, “indien van toepassing, het identificatienummer van het Rijksregister van de natuurlijke personen”.

De vraag rijst of niet eveneens dient te worden voorzien in een identificatie die gekoppeld is aan andere registers, zoals bijvoorbeeld het vreemdelingenregister.

Op een vraag daarover heeft de gemachtigde van de minister geantwoord dat ook het nummer van het vreemdelingenregister een unieke identificatie mogelijk maakt en dat die identificatie aan de lijst moet worden toegevoegd.

Artikel 6 moet dienovereenkomstig worden aangevuld. Hetzelfde geldt voor de bespreking, waarin de toevoeging van dat extra gegeven moet worden verantwoord.

2. In artikel 6, § 2, eerste lid, 1°, 1), c), worden de gegevens opgesomd betreffende de bijzondere categorieën van persoonsgegevens, waaronder de gegevens over de gezondheid (v.). Wat die laatste gegevens betreft, bepaalt artikel 6, § 2, tweede lid, binnen welke grenzen die zogeheten “gevoelige” gegevens mogen worden verzameld en bepaalt artikel 6, § 2, derde lid, in welk geval ze mogen worden meegedeeld.

Die gegevens maken deel uit van de gegevens die worden bedoeld in artikel 9, lid 1 en 2, van de AVG en in artikel 10 van de voornoemde richtlijn (EU) 2016/680.³⁹

Artikel 10 van die richtlijn luidt:

“(…) verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over gezondheid (...) [is] slechts toegelaten wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkene, en:

- a) bij het Unierecht of het lidstatelijke recht is toegestaan;
- b) noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
- c) die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.”⁴⁰

³⁹ Wat het toepassingsgebied van de AVG en van de voornoemde richtlijn (EU) 2016/680 betreft, wordt verwezen naar algemene opmerking II, B, 2.6.

⁴⁰ Zie ook artikel 34, § 1, van de voornoemde wet van 30 juli 2018, waarbij artikel 10 van de richtlijn wordt omgezet. Artikel 34 van de wet bevat eveneens een paragraaf 2, die als volgt luidt:

“§ 2. De passende waarborgen zoals bedoeld in paragraaf 1 voorzien ten minste in dat de bevoegde overheid of de verwerkingsverantwoordelijke een lijst van de categorieën van personen die toegang hebben tot de persoonsgegevens opstelt, met een beschrijving van hun hoedanigheid ten opzichte van de verwerking van de beoogde gegevens. Deze lijst wordt ter beschikking gehouden van de bevoegde toezichthoudende autoriteit.

De bevoegde overheid waakt erover dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.”

In de AVG wordt datzelfde onderwerp geregeld bij artikel 9: in lid 1 vermeldt – en verbiedt – het dezelfde verwerkingen als die welke in artikel 10 van richtlijn (EU) 2016/680 worden opgegeven en in lid 2 somt het vervolgens een reeks gevallen op waarin dat verbod niet van toepassing is, onder meer wanneer:

“i) de verwerking (...) noodzakelijk [is] om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim.”

In de bespreking van artikel 6 van het voorontwerp staat het volgende:

“Voor de verwerking van alle bovengenoemde bijzondere categorieën van persoonsgegevens gelden de passende, bij de gegevensbeschermingswet opgelegde waarborgen. De gegevens in de gemeenschappelijke gegevensbank T.E.R. zijn namelijk toegankelijk op basis van verschillende toegangsrechten die de Koning de in de wet opgesomde diensten zal verlenen op basis van het principe van de behoefte om te kennen in het kader van de uitoefening van hun opdrachten bedoeld in artikel 3 en overeenkomstig de doeleinden van artikel 5, tweede lid. Voorts zal elke dienst moeten identificeren welke van zijn personeelsleden gemachtigd zijn om de toegangsrechten tot de gemeenschappelijke gegevensbank T.E.R. uit te oefenen en een lijst van die personen moeten bezorgen aan de beheerder van de toegangen. Die lijst kan, in voorkomend geval, ter beschikking worden gesteld van de functionaris voor gegevensbescherming en van de operationeel verantwoordelijke in het kader van hun respectieve opdrachten. Er wordt ook gepreciseerd dat de personeelsleden houder moeten zijn van een veiligheidsmachtiging van het niveau ‘geheim’ om toegang te kunnen krijgen tot de gemeenschappelijke gegevensbank T.E.R.”

Bij de tenuitvoerlegging van de machtiging die artikel 6, § 2, vijfde lid, aan de Koning verleent om, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de toezichthoudende overheden, de maatregelen te bepalen die nodig zijn met het oog op het beheer en de veiligheid van de persoonsgegevens en de informatie die worden verwerkt in de gemeenschappelijk gegevensbank T.E.R., zal, wat de zogeheten “gevoelige” gegevens betreft, rekening dienen te worden gehouden met de verplichtingen opgelegd bij artikel 10 van richtlijn 2016/680 en bij artikel 9 van de AVG, in het bijzonder lid 2, i), van die laatste bepaling. Dat brengt met zich mee dat, voor de verwerkingen die in het toepassingsgebied van de richtlijn vallen, wordt voorzien in “passende waarborgen voor de rechten en vrijheden van de betrokkene” en dat, voor de verwerkingen die onder de AVG vallen, wordt voorzien in “passende en specifieke maatregelen (...) ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim”, eveneens rekening houdend met artikel 34, § 2, van de voornoemde wet van 30 juli 2018.

Artikel 13

1. Artikel 13, § 2, bepaalt dat de operationeel verantwoordelijke hetzij de vermelde personen of organismen in kennis stelt van de zich voordoende “inbreuken op de beveiliging” van de gemeenschappelijke gegevensbank T.E.R. (eerste en tweede lid), hetzij die inbreuken aan die personen of organismen meldt (derde lid). In artikel 13, § 3, wordt voorts de inhoud beschreven van “de in paragraaf 2, tweede en derde lid bedoelde melding”.

In het tweede lid van paragraaf 2 wordt echter de uitdrukking “in kennis stellen” gebruikt, en is er geen sprake van het begrip “melding”. Ook zou de “melding” waarnaar artikel 13, § 3, verwijst, dus niet slaan op het eerste lid van paragraaf 2.

Naar aanleiding van een vraag daarover heeft de gemachtigde van de minister voorgesteld om de paragrafen 2 en 3 met elkaar in overeenstemming te brengen door alleen gebruik te maken van het begrip “melding”.

Artikel 13 moet dienovereenkomstig worden herzien.

2. Aangezien in paragraaf 2, derde lid, wordt bepaald dat in geval van een inbreuk op de beveiliging die aanleiding kan vormen tot een hoog risico voor de rechten en vrijheden van natuurlijke personen, de operationeel verantwoordelijke deze inbreuk zo snel mogelijk moet melden aan de toezichthoudende overheden, heeft het geen zin om nog eens te specificeren dat dat moet gebeuren “indien mogelijk (...) 72 uur nadat” de operationeel verantwoordelijke er kennis van heeft genomen. Zoals dat zinsstuk gesteld is, zou men het bovendien zo kunnen interpreteren dat die melding ten vroegste 72 uur na de kennisneming hoort te worden gedaan, wat geen steek zou houden.

De woorden “en indien mogelijk, 72 uur nadat hij er kennis van heeft genomen” moeten worden weggelaten.

Artikel 16

Bij artikel 16 van het voorontwerp wordt aan de toezichthoudende overheden uitsluitend een leesrecht met betrekking tot de actieve gemeenschappelijke gegevensbank en de archieven verleend.

Er wordt in de memorie van toelichting evenwel meermaals uitgelegd dat het leesrecht altijd verbonden is aan het schrijfrecht.⁴¹

⁴¹ Zie bijvoorbeeld de inleidende bespreking van afdeling 5 van hoofdstuk 2 (“het leesrecht [gaat samen] met het schrijfrecht/de schrijfplicht”) en de bespreking van artikel 17 (“de lees- en schrijfrechten [zijn] onlosmakelijk met elkaar verbonden”).

De gemachtigde van de minister heeft beaamd dat dit niet het geval is in het kader van artikel 16, dat dus een uitzondering vormt aangezien het paar “leesrecht/schrijfrecht” niet geldt voor de toezichthoudende organen, wier controlefunctie immers geen schrijfrecht vereist maar enkel een leesrecht.

De memorie van toelichting en de bespreking moeten dienovereenkomstig duidelijker worden geformuleerd.

Artikel 19

1. Doordat het zinsdeel “die een leesrecht en een schrijfrecht hebben” tussen komma’s staat, moet het eerste lid zo worden gelezen dat niet alleen de basisdiensten maar ook de partnerdiensten noodzakelijkerwijze over die rechten beschikken.

Luidens artikel 17 komen die diensten echter pas in het bezit van die rechten als de Koning hun die verleent.

Om alle dubbelzinnigheid in de tekst te voorkomen, moeten die komma’s dus worden weggelaten, en dit, *mutatis mutandis*, naar het voorbeeld van de redactie van artikel 23, eerste lid, van het voorontwerp in verband met het vraagrecht dat door de Koning aan de partnerdiensten zou zijn verleend.

2. Er wordt bepaald dat de basisdiensten en de partnerdiensten die met betrekking tot de gemeenschappelijke gegevensbank T.E.R. over een schrijfrecht en een leesrecht beschikken, verplicht zijn de gegevensbank te raadplegen en ambtshalve daarin hun eigen persoonsgegevens en relevante informatie in te voeren, die “worden afgeleid uit de persoonsgegevens en informatie waarover [ze] beschikken in het kader van hun respectieve opdrachten en de daarmee verband houdende doeleinden”.

Uit artikel 18 volgt echter dat alleen een basisdienst over een recht beschikt om een “entiteit” in de gemeenschappelijke gegevensbank T.E.R. te creëren.

Rekening houdend met het feit dat de partnerdiensten verplicht zijn om de persoonsgegevens en de informatie waarover ze beschikken, in de gegevensbank in te voeren, dienen de nadere regels te worden gespecificeerd op basis waarvan die diensten worden geïnformeerd zodra een “entiteit” in de gegevensbank wordt gecreëerd. Zo niet zouden de betrokken diensten zich verplicht zien op eigen initiatief op de hoogte te blijven van de eventuele creatie van een “entiteit” waarover ze gegevens en informatie zouden hebben, wat praktisch gezien maar moeilijk denkbaar zou zijn.

Artikel 30

De bespreking van artikel 30 bevat geen uitleg over de strekking van paragraaf 4, die de volgende nieuwe machtiging aan de Koning verleent:

“De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, andere regels bepalen inzake de verantwoordelijkheid op het gebied van de bescherming van persoonsgegevens van de basisdiensten en de partnerdiensten die deze gegevens verwerken.”

Naar aanleiding van een vraag daarover heeft de gemachtigde van de minister de volgende preciseringen gegeven:

“Un premier contrôle de qualité est opéré au sein même du service qui transmet une donnée ou une information à la [banque de données commune (BDC)] T.E.R. Les services disposant d'un droit de lecture et d'écriture dans la BDC doivent mettre en place un système de validation interne de leurs propres données afin d'avoir des données adéquates, pertinentes et non excessives au regard des missions et des finalités de la BDC (art. 14). L'article 15 prévoit qu'un service partenaire peut ajouter des données à propos d'une entité déjà enregistrée sans modifier/supprimer celles qui existent déjà. Seul le service qui a enregistré une donnée peut la modifier, la rectifier et la supprimer. Si un autre service estime qu'une donnée doit être modifiée, rectifiée ou supprimée, il en informe le service qui l'a enregistrée en vue de procéder le cas échéant aux adaptations nécessaires. En cas de désaccord, le responsable opérationnel prend la décision finale.”

Het verdient aanbeveling die toelichtingen in de bespreking van de bepaling op te nemen.

Artikelen 31 en 32

1. Luidens artikel 31 van het voorontwerp

“(…) worden er persoonsgegevens en informatie uit de gemeenschappelijke gegevensbank T.E.R., alsook andere persoonsgegevens en relevante informatie, waaronder geclassificeerde informatie in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, uitgewisseld binnen een of meer overlegplatformen die bij elk gerechtelijk arrondissement zijn opgericht, onder de naam ‘Lokale task force’ (hierna ‘LTF’), tenzij die uitwisseling een onderzoek, de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kan brengen.”

In artikel 32, § 1, vierde lid, van het voorontwerp wordt bepaald dat de voorzitter van die lokale taskforce in overleg met zijn “deelnemers”, te weten de inlichtingen- en veiligheidsdiensten, het Coördinatieorgaan voor de dreigingsanalyse, de federale politie, de lokale politie, de Algemene Directie Dienst Vreemdelingenzaken van de Federale overheidsdienst Binnenlandse Zaken en het Openbaar Ministerie,

“andere diensten, organen of instanties [kan] uitnodigen wegens de bijdrage die ze door hun functie of bevoegdheden kunnen leveren aan een gerichte en geïndividualiseerde opvolging van de entiteit.”

De artikelen 31 en 32 van het voorontwerp zijn ondergebracht in een hoofdstuk 3 met als opschrift “Verrijking van gegevens over entiteiten en opvolging van een in de gemeenschappelijke gegevensbank T.E.R. gevalideerde entiteit”.

2. Uit de redactie van het begin van artikel 31 kan worden opgemaakt dat de uitwisseling van gegevens binnen de lokale taskforce het volgende doel zou dienen:

“de verrijking van persoonsgegevens en informatie over entiteiten en de opvolging en het nemen van maatregelen ten aanzien van de in de gemeenschappelijke gegevensbank T.E.R.”

Naar aanleiding van een vraag daarover heeft de gemachtigde van de minister het volgende gesteld over de uitwisseling van gegevens of informatie binnen de lokale taskforce en over wat dient te worden verstaan onder het begrip “verrijking van gegevens”:

“L’avant-projet de loi utilise en effet à plusieurs reprises la notion d’enrichissement des données/informations. Cette notion doit être comprise d’une part comme une contextualisation des données et d’autre part comme la mise à jour de l’information déjà enregistrée et/ou l’ajout des informations nouvelles.

Pourquoi faut-il contextualiser ?

La [banque de données 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 T.E.R.] ne reprend pas, par exemple, le contenu *in extenso* des procès-verbaux) et la contextualisation permet donc de donner tout le contexte relatif à la donnée enregistrée dans la [banque de données T.E.R.] (personne, véhicule, ...).

Pourquoi faut-il mettre à jour ?

Lors de la [Task force locale] et de la discussion avec les différents services présents, il peut ressortir qu’il y ait des nouvelles données à enregistrer et qu’il faille donc ‘enrichir’ la banque de données ou qu’il soit nécessaire de mettre de l’information déjà enregistrées à jour.

Telles qu’elles sont définies à l’article 2, 5° et 6°, de l’avant-projet, les données à caractère personnel et les informations qui peuvent être insérées dans la banque de données commune T.E.R. sont des données et des informations non classifiées.

(...)

Comme l’article 2, points [5]° et [6]°, le prévoit, la [banque de données T.E.R.] ne contient pas de données classifiées. Utiliser une banque de données qui peut contenir des données classifiées a des implications majeures en termes de développement, sécurité de la banque de données, ce qui n’est pas le cas de la banque de données commune T.E.R.

Lors des réunions des [Task forces locales], dans le cadre de l’enrichissement des données, entre partenaires qui disposent d’une habilitation de sécurité et du besoin d’en connaître, des informations classifiées sur une personne enregistrée dans la banque de données T.E.R. peuvent être échangées.”

Uit die toelichtingen blijkt dat de gegevensuitwisseling binnen de lokale taskforce kan leiden tot een precisering van persoonsgegevens of informatie die al in de gemeenschappelijke gegevensbank T.E.R. zitten, tot een update van die gegevens of tot de invoering van nieuwe gegevens.

Gelet op de definities in de punten 5° en 6° van artikel 2 van het voorontwerp, mag, teneinde de samenhang van het hele dispositief te bewaren, artikel 31 van het voorontwerp evenwel niet aldus worden geïnterpreteerd dat geclassificeerde gegevens of geclassificeerde informatie in de gemeenschappelijke gegevensbank T.E.R. kunnen worden geregistreerd. Die gegevens en informatie mogen hoogstens tijdens vergaderingen van de lokale taskforce worden uitgewisseld.

Onder voorbehoud van die interpretatie is artikel 31 van het voorontwerp toelaatbaar.

3. Naar aanleiding van een vraag over de strekking van het ontworpen artikel 32, § 1, vierde lid, heeft de gemachtigde van de minister ook de volgende preciseringen gegeven:

“Lors des réunions de la [Task Force locale], les principes de base (chapitre 2 sections 5 et 7) contenus dans le projet de loi en matière d'accès ou de communication de données sont respectés.

Chaque membre présent travaille sur la base du principe du besoin d'en connaître.

Si un membre externe est invité, il est présent dans le but exclusif de fournir des données, éclairer un point précis par son expertise et pas pour recevoir des données. Il est présent pour ‘son point’ et quitte ensuite la réunion après son exposé.”

Uit die toelichtingen volgt dat het ontworpen artikel 32, § 1, vierde lid, zo moet worden geïnterpreteerd dat “andere diensten, organen of instanties” die zijn uitgenodigd om deel te nemen aan de vergaderingen van de lokale taskforce, gegevens of informatie die ze in het kader van hun opdracht bezitten, kunnen meedelen om de gegevens of de informatie die al in de gegevensbank zitten, te verrijken. Ze zouden daarentegen geen gegevens of informatie kunnen ontvangen die de andere leden van de lokale taskforce zouden bezitten.

Onder voorbehoud van die interpretatie is ook artikel 32 van het voorontwerp toelaatbaar.

Artikel 32

Artikel 32, § 1, regelt de samenstelling van de lokale taskforce, die LTF wordt genoemd.

Er wordt echter niets bepaald in verband met het aantal leden per categorie, noch in verband met de nadere regels voor de werkwijze van die LTF.

Op een vraag daarover heeft de gemachtigde van de minister het volgende geantwoord:

“Le texte va être réexaminé pour prévoir éventuellement la présence au minimum d'une personne par autorité présente à la TLF. Le texte va être réexaminé pour prévoir éventuellement un nombre minimum de réunion par an.”

Artikelen 34 tot 49

Zoals de gemachtigde van de minister heeft beaamd, moeten de memorie van toelichting en de bespreking worden aangevuld met een artikelsgewijze uitleg van de ontworpen bepalingen, zodat de wijzigingen die in de wet van 30 juli 2018 worden aangebracht, worden toegelicht.

Artikel 46

Artikel 46 strekt ertoe artikel 162 van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’ aan te vullen met twee nieuwe leden, die het derde en het vierde lid worden.

Uit het ontworpen derde lid vloeit voort dat, in afwijking van het huidige eerste lid van artikel 162, de operationeel verantwoordelijke van de gegevensbank na overleg met de basisdiensten kan toestaan dat een verantwoordelijke voor verdere verwerking persoonsgegevens betreffende entiteiten die in de gemeenschappelijke gegevensbank T.E.R. geregistreerd staan, raadpleegt voor historische, wetenschappelijke of statistische doeleinden.

De vraag rijst waarom in een dergelijke afwijking van artikel 162, eerste lid, van de voornoemde wet wordt voorzien, zonder dat ten aanzien van de toestemming tot raadpleging een voorbehoud wordt gemaakt voor het geval dat die raadpleging de uitoefening van de strafvordering, de veiligheid van een persoon of de relatie met een rechtshandhavingsautoriteit van een buitenlandse Staat in het gedrang zou brengen. Dat voorbehoud wordt overigens ook in artikel 20 van het voorontwerp gemaakt.

Als er dienaangaande geen verantwoording kan worden gegeven, moet het dispositief worden aangevuld zodat in dat geval wordt voorzien.

In de Nederlandse tekst van het derde lid dient overigens het woord “toestaan” ingevoegd te worden tussen het woord “entiteiten” en de woorden “door de operationeel verantwoordelijke”.

Artikel 54

Zoals de gemachtigde van de minister heeft beaamd, dient het tweede lid, *in fine*, te worden aangevuld zodat bepaald wordt dat de Koning de bestaande verwijzingen in de wetten naar de bepalingen van de opgeheven koninklijke besluiten kan vervangen door verwijzingen naar de ermee overeenstemmende bepalingen “van deze wet of van de besluiten tot uitvoering ervan”.

Artikel 56

Artikel 56 is als volgt geredigeerd:

“Deze wet treedt in werking op de datum bepaald door de Koning en uiterlijk op xxx.”

Naar aanleiding van een vraag over het feit dat het voorontwerp de uiterste inwerkingtredingsdatum onvermeld laat, heeft de gemachtigde van de minister het volgende gesteld:

“Il était en effet important que la loi et l'arrêté royal portant exécution de celle-ci entrent en vigueur en même temps, et ce, pour permettre une application complète de la législation en matière de la [banque de données communes] T.E.R. Le but est que le projet de loi et d'arrêté royal entrent en vigueur encore sous cette législature. Nous proposons donc de prendre une date ultime (et au plus tard) fin 2024.”

Overeenkomstig de desbetreffende regels van de wetgevingstechniek dient de datum in artikel 56 te worden aangevuld.⁴² Dientengevolge moet de keuze van die datum van inwerkingtreding in de bespreking van het artikel worden toegelicht.

SLOTOPMERKINGEN

Het voorontwerp moet op de volgende punten worden herzien:

– in artikel 2, 5°, dient het volledige opschrift te worden vermeld van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 ‘betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)’; ook dient te worden vermeld dat dat opschrift wordt afgekort als “AVG” en dient die afkorting in het vervolg van het voorontwerp te worden gebruikt;

– Evenzo moet in de Franse tekst van artikel 33, § 2, 6°, het juiste opschrift van de wet van 18 september 2017 ‘relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces’ worden opgegeven ;

– in de Franse tekst van artikel 2, 15°, moet de eerste vermelding van het woord “organique” worden geschrapt;

– in de Franse tekst van artikel 6, §2, eerste lid, 1°, 1), c), i., dient het woord “de” te worden weggelaten;

⁴² *Beginselen van de wetgevingstechniek – Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbevelingen 154.1 en 154.1.2 en formule F 4-5-2-4.

– ten slotte dienen de verwijzingen naar artikelen te worden gecontroleerd of gepreciseerd, zoals bijvoorbeeld in de artikelen 7, § 2, derde lid, 4°, 11, tweede lid, 5°, 16, 39, 44 en 50; hetzelfde geldt voor artikel 32, § 1, derde lid, dat een verkeerde verwijzing bevat aangezien daarin dient te worden verwezen naar artikel 4, derde lid, van de wet van 11 december 1998 ‘betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst’, en voor artikel 32, § 2, eerste lid, 1°, dat naar artikel 31 en niet naar artikel 32 van het voorontwerp moet verwijzen.

LE GREFFIER – DE GRIFFIER

LE PRÉSIDENT – DE VOORZITTER

Esther CONTI

Pierre VANDERNOOT