Avis n° 57/2015 du 16 décembre 2015

Objet: Avant-projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme (CO-A-2015-063)

La Commission de la protection de la vie privée (ci-après la « Commission ») ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la « LVP »), en particulier l'article 29 ;

Vu la demande d'avis du Ministre de l'Intérieur et du Ministre de la Justice, reçue le 16/12/2015 ;

Vu le rapport de Monsieur Frank Schuermans et Monsieur Gert Vermeulen ;

Émet, le 16 décembre 2015, l'avis suivant :

A. Objet et contexte de la demande

1. Une circulaire ministérielle du Ministre de l'Intérieur et du Ministre de la Justice relative à l'échange d'informations et au suivi des foreign terrorist fighters en provenance de Belgique a été prise le 21 août 2015 (ci-après, la « circulaire FTF »). Elle remplace une précédente circulaire du 25 septembre 2014. L'essence de cette circulaire dont le contenu précis revêt un caractère confidentiel se trouve dans l'accord de Gouvernement[1].

2. La circulaire prévoit une analyse personnalisée de la menace pour chaque « Foreign Terrorist Fighter »[2] (FTF) sur base d'informations provenant des différents services, rassemblées dans une base de données unique, avec un paquet de mesures personnalisées et de mesures spécifiques d'accompagnement au niveau local. La base de données sera alimentée par les services de police et de renseignement, ainsi que tout autre partenaire pertinent.

3. L'avant-projet de loi relatif à des mesures de complémentaires en matière de lutte contre le terrorisme (ci-après l'« avant-projet ») soumis pour avis vise à la mise sur pied de cette banque de données commune.

4. Le demandeur a fait le choix d'insérer le cadre juridique relatif à cette banque de données commune dans la loi du 5 août 1992 *sur la fonction de police* (ci-après la « LFP »).

5. Le texte de l'avant-projet va plus loin que l'objet initial de la circulaire en prévoyant la possibilité de créer des (multiples) banques de données communes dans le cadre de la prévention et du suivi du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme.

6. Le texte aborde également deux autres mesures annoncées par le Premier Ministre le 19 novembre 2015 en matière de lutte contre le terrorisme :

- la possibilité de procéder à des perquisitions 24 heures sur 24 ;
- la révision de la législation relative aux écoutes téléphoniques (article 90*ter* du code d'instruction criminelle).

7. Les trois objets de l'avant-projet touchant la matière de la protection des données à caractère personnel et/ou de la vie privée au sens large, la Commission les aborde dans le présent avis à travers une analyse chronologique des différents articles pertinents.

---

[1] http://www.koengeens.be/fr/news/2015/08/27/nouvelle-circulaire-foreign-terrorist-fighters.

[2] Combattant terroriste étranger.

B. Examen de l'avant-projet

B.1. Examen du chapitre 2 de l'avant-projet (articles 2 à 4) – modifications de la loi du 7 juin 1969 *fixant le temps pendant lequel il peut être procédé à des perquisitions ou visites domiciliaires*

8. L'avant-projet ajoute l'interdiction d'effectuer une privation de liberté dans un lieu non accessible au public de nuit (entre neuf heures du soir et cinq heures du matin) à l'interdiction de procéder à des perquisitions et des visites domiciliaires nocturnes dans un lieu non accessible au public prévue actuellement dans la loi du 7 juin 1969 *fixant le temps pendant lequel il peut être procédé à des perquisitions ou visites domiciliaires*.

9. L'objectif poursuivi par le demandeur est de renforcer la sécurité juridique sur ce point. La Commission prend note des explications du demandeur présentées dans l'exposé des motifs à cet égard.

10. L'avant-projet ajoute ensuite une double exception à l'interdiction d'effectuer une perquisition, une privation de liberté ou une visite domiciliaire de nuit dans un lieu non accessible au public, en cas d'infraction terroriste[3] ou d'infraction dans le cadre d'une association de malfaiteurs ou une organisation criminelle[4] pour autant qu'il existe des indices sérieux de possession d'armes prohibées, d'explosifs ou de substances dangereuses.

11. Le demandeur tend par cet ajout à offrir aux autorités des moyens supplémentaires dans la lutte contre les infractions terroristes et la criminalité grave avec usage d'armes à feu, d'explosifs et de substances dangereuses, lorsqu'il doit être procédé à une perquisition, une capture ou une arrestation d'individus dangereux ou susceptibles d'opposer une résistance, avec tous les moyens à leur disposition, y compris des armes à feu ou des explosifs, etc. La Commission n'a pas de remarques concernant l'insertion envisagée.

B.2. Examen du chapitre 3 de l'avant-projet (article 5) – modifications de l'article 90*ter* du code d'instruction criminelle

12. Le demandeur vise à étendre la liste limitative des infractions pour lesquelles des écoutes peuvent être ordonnées, en y insérant notamment le trafic d'armes et certaines infractions à la loi sur les armes.

---

[3] Infraction visée au livre II, titre I*ter* du code pénal.

[4] Infraction visée au livre II, titre VII, chapitre Ier du code pénal.

13. Comme la Commission a pu l'indiquer récemment[5], l'examen d'un tel élargissement doit tenir compte des contraintes déduites de l'article 8, § 2, de la Convention européenne des droits de l'homme et appliquées à de multiples reprises par la Cour européenne des droits de l'Homme[6]. Suivant cette jurisprudence, il importe que la limitation du droit au respect de la vie privée et familiale, du domicile et de la correspondance soit inspirée par un intérêt public, qu'elle soit proportionnée, et que l'étendue et le mode d'exercice du pouvoir octroyé aux autorités publiques soient définis avec suffisamment de précision.

14. Étant donné le caractère intrusif important de cette mesure de surveillance, ce n'est dès lors que lorsqu'il s'agit d'infractions considérées comme étant graves que ce moyen peut être utilisé. Ainsi que le mentionne le demandeur, selon l'exposé des motifs de la loi du 30 juin 1994[7] ayant introduit le mécanisme des écoutes, il s'agit d'une exception strictement réglementée à l'interdiction absolue d'intercepter des communications : pour se conformer au principe du respect fondamental de la vie privée du citoyen tel qu'il est formulé dans l'article 8 de la Convention européenne des droits de l'homme, les faits punissables pour lesquels cette mesure d'instruction est possible doivent être limités à des formes de criminalités graves correspondant notamment à ce qu'il est convenu d'appeler terrorisme, grand banditisme ou crime organisé (Doc. Sénat, 843-1, 1992-1993, p. 11).

15. La Commission prie dès lors le demandeur de tenir compte des exigences précitées en ce qui concerne l'ajout à la liste limitative précitée de certaines infractions à la loi du sur les armes[8]. Elle se demande particulièrement quelle est la pertinence de permettre une mesure de surveillance aussi invasive à l'égard de toutes personnes soupçonnées de port d'une arme en vente libre sans motif légitime.

16. Elle invite en tout état de cause le demandeur à fournir une motivation détaillée quant à l'adéquation de l'extension de la possibilité de recourir à des écoutes par rapport à ces infractions, qu'elle est bien en mal de trouver dans l'actuel exposé des motifs.

B.3. **Examen du chapitre 4 de l'avant-projet** – modifications de la LFP

---

[5] Voir l'avis n° 05/2015 du 24 février 2015 relatif à un projet de loi visant à renforcer la lutte contre le terrorisme, https://www.privacycommission.be/sites/privacycommission/files/documents/avis_05_2015.pdf, ayant précédé la loi du 20 juillet 2015 *visant à renforcer la lutte contre le terrorisme* qui étend la possibilité des écoutes aux infractions terroristes introduites dans le code pénal par la loi du 18 février 2013 *modifiant le livre II, titre Ier ter du code pénal* et par ladite loi du 20 juillet 2015.

[6] Voir notamment les affaires Sunday Times, Klass, Malone et Kruslin.

[7] Relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées.

[8] Loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes, aussi appelée « loi sur les armes ».

I. Analyse de l'article 6 de l'avant-projet – modifications apportées à l'article 44/2 de la LFP

1. Présentation des modifications

17. L'article 44/2 de la LFP prévoit actuellement la création de 3 catégories de banques de données policières opérationnelles permettant la structuration de données nécessaire à l'exercice des missions de police administrative et de police judiciaire suivant les finalités propres à chaque catégorie de banques de données :

- la banque de données nationale générale (BNG) ayant pour finalité notamment d'identifier les suspects, la coordination et le croisement des données, la vérification des antécédents, l'indication de mesures à prendre et l'appui à la politique policière ;
- les banques de données de base ayant pour finalité de permettre le compte-rendu aux autorités compétentes de l'exercice des missions de police ;
- les banques de données particulières créées dans des circonstances exceptionnelles pour des besoins policiers particuliers et ne pouvant figurer en BNG en raison de la classification des données, pour des raisons de nature technique ou fonctionnelle ou en raison du caractère excessif d'une centralisation.

18. L'avant-projet envisage d'ajouter un paragraphe complémentaire à cet article afin de permettre la possibilité de créer une ou plusieurs banques de données communes dans le cadre de la prévention et du suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme. Ce paragraphe stipule à cet effet que « *lorsque l'exercice conjoint, par tout ou partie des autorités, organes, organismes, services, directions ou commission visés à l'article 44/11/3 ter [en projet], des missions de prévention et de suivi du terrorisme au sens de l'article 8, 1°, b) de loi du 30 novembre 1998 organique des services de renseignement et de sécurité ou de l'extrémisme au sens de l'article 8, 1° c) de la même loi, lorsqu'il peut mener au terrorisme, nécessite que ceux-ci structurent les données à caractère personnel et les informations relatives à ces missions de sorte qu'elles puissent être directement retrouvées, celles-ci sont traitées dans une ou plusieurs banques de données communes* ».

19. Le demandeur fait valoir qu'il est primordial que les différents services dont les missions concernent directement ou indirectement la lutte contre le terrorisme et l'extrémisme soient guidés dans leurs actions quotidiennes et dans leurs prises de décisions sur des données mises en commun. Cette mise en commun va en effet permettre d'augmenter la qualité des données et de décider d'agir/ne pas agir plus rapidement/opportunément, à l'heure du « *real time intelligence* ».

20. L'exposé des motifs fournit l'explication succincte suivante quant à l'encadrement de ces banques de données communes dans la LFP : « *La police intégrée sera toujours concernée de près par les banques de données communes car elle devra, sur la base des directives émises par les autorités administratives et judiciaires, assurer le volet opérationnel du traitement de données et pouvoir agir concrètement sur le terrain pour contrer les phénomènes de terrorisme et de radicalisme pouvant conduire au terrorisme sur la base des principes décrits dans la loi sur la fonction de police* ».

21. D'après le demandeur, la référence aux définitions de terrorisme et d'extrémisme de la loi du 30 novembre 1998 *organique des services de renseignement et de sécurité* (ci-après, la « loi du 30 novembre 1998 ») a pour but de de trouver le plus grand commun dénominateur aux acteurs, qui interviennent directement ou indirectement en matière de sécurité.

2. Analyse des modifications

22. La Commission prend note des explications fournies par le demandeur pour expliquer la création d'une nouvelle catégorie de banque de données au sein de la LFP.

23. Elle se demande néanmoins d'où vient la nécessité de la mise en place d'une ou plusieurs nouvelles banques de données et de créer un nouveau cadre juridique à côté de ce qui existe déjà. En effet, la banque de données et les fichiers de travail de l'OCAM semblent suffisants pour rencontrer les finalités poursuivies moyennent des adaptations visant à permettre un échange de données optimal entre les différents partenaires de la chaîne pénale, policière et de sécurité. En effet, le système d'information de l'OCAM, tel que prévu à l'article 9 de la loi du 10 juillet 2006 *relative à l'analyse de la menace* (ci-après la « loi OCAM ») et dans l'arrêté d'exécution du 28 novembre 2006 *portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace* (les articles 3 à 6 inclus), semble déjà constituer une base juridique assez solide pour la (les) banque(s) de données « intégrée(s) » et « mixte(s) » qui est (sont) envisagée(s). L'intégration de cette banque de données commune dans la LFP, et plus particulièrement dans la section 1*bis* (« De la gestion des informations ») du Chapitre 4 (« Missions des services de police »), qui vise et traite exclusivement du fonctionnement des services de police apparaît pour le moins très étrange. La très brève explication dans l'exposé des motifs (cf. point 20) ne justifie pas vraiment la raison pour laquelle le fondement juridique de cette banque de données mixte et commune, qui sera alimentée, utilisée et consultée par divers services non policiers, doit quand même se trouver dans la loi organique qui fixe les principes fondamentaux de la LFP. On ne précise pas non plus le rapport entre cette (ces) nouvelle(s) banque(s) de données intégrée(s) et commune(s) liée(s) au terrorisme et le système d'information de l'OCAM. S'agit-il des mêmes données et informations ? Ou précisément pas ? Y a-t-il un risque de doubles saisies et donc de

contradictions lorsque les mêmes informations sont saisies à plusieurs reprises (par exemple à la fois dans la BNG, et dans une banque de données policière particulière, et dans la banque de données de l'OCAM, et dans cette nouvelle banque de données commune) ?

24. L'OCAM est par essence la plate-forme où les données en relation avec le radicalisme et le terrorisme qui proviennent de différents services (services d'appui) devraient être réunies en vue de l'analyse de la menace. Sur cette base, les décisions aussi bien au niveau stratégique, tactique qu'opérationnel pourraient ensuite être prises pour autant que ses possibilités de communication et de coopération avec les autres acteurs de la chaîne pénale, policière et de sécurité soient étendues. C'est d'ailleurs ce qui ressort des déclarations du Ministre de l'Intérieur dans le cadre de l'adoption de la circulaire FTF : « *Dès à présent, chaque Foreign Terrorist Fighter sera passé à la loupe et évalué individuellement par l'OCAM. Sur cette base, les autorités locales sauront quel suivi ils doivent opérer. Leur travail sur le terrain sera plus efficace au bénéfice de notre sécurité à tous* »[9].

25. La référence aux définitions de la loi du 30 novembre 1998 en tant que commun dénominateur montre d'ailleurs qu'il est davantage question d'un traitement qui relève plutôt du renseignement que d'un traitement policier pur et dur.

26. La Commission reconnaît que le cadre actuel ne permet pas un échange d'informations optimal, notamment en ce qui concerne la collaboration entre le bourgmestre et les autres services communaux. Néanmoins, le cadre actuel de la loi OCAM et de son arrêté d'exécution permet déjà beaucoup de choses (on peut ainsi par exemple se référer à l'article 10, § 3 de la loi OCAM qui permet le cas échéant de partager les analyses et évaluations opérationnelles (ponctuelles) avec d'autres personnes ou services que les personnes ou services opérationnels, par exemple aussi à un bourgmestre), mais n'empêche bien entendu pas de prévoir un transfert et un échange d'informations plus larges et de meilleure qualité avec d'autres autorités que celles prévues actuellement de manière limitative. Un réel accès direct, destiné par exemple à un bourgmestre ou à un CPAS, à la banque de données envisagée (et aux informations qui y sont reprises et qui proviennent principalement de services de sécurité et de police) est quoi qu'il en soit inadmissible. Les bourgmestres ne devraient recevoir que les informations qui sont importantes du point de vue du maintien de l'ordre public. En ce qui concerne par exemple les CPAS ou d'éventuels autres services communaux (population, etc.), tout au plus semble-t-il important que les informations dont ils disposent au sujet de certaines personnes reprises dans la banque de données puissent être transmises aux services compétents (police, services de renseignement) afin qu'elles puissent également être intégrées à celle-ci. Des « droits d'écriture » directs pour eux semblent également

[9] http://www.koengeens.be/fr/news/2015/08/27/nouvelle-circulaire-foreign-terrorist-fighters.

inadmissibles étant donné qu'il est préférable de prévoir une validation par les services compétents. Un simple système de « flagging » (habituel dans le contexte de banques de données internationales telles que le SIS), leur permettant uniquement de voir dans la banque de données les personnes pour lesquelles la police et/ou les services de renseignement estiment nécessaire que les informations dont ils disposent soient fournies, permettrait de réaliser la finalité. Si l'on détermine légalement qu'un « flag » implique pour eux qu'ils doivent fournir d'éventuelles informations disponibles, cela résout également les problèmes qui se posent aujourd'hui au sujet du refus de transmettre des informations en vertu du secret professionnel.

27. Par ailleurs, dès lors que l'objectif du demandeur est de prévenir et lutter contre le terrorisme et le radicalisme pouvant conduire au terrorisme, la Commission se demande s'il ne serait pas préférable de renvoyer (aussi) aux dispositions du Code pénal spécifique à ces phénomènes figurant dans le livre 2, Titre I*ter*. Par ailleurs, on ne sait pas très clairement ce que l'on entend par les termes « *et* ***de suivi*** *du terrorisme …* » à l'article 44/2, § 2 en projet de la LFP. La Commission suppose qu'il faut également entendre par là (outre le suivi plus stratégique et le suivi dans le cadre du travail des services de renseignement) les missions de police judiciaire ainsi que la recherche et les poursuites pénales. En d'autres termes, cette nouvelle banque de données commune servira également à accomplir les missions précitées de police judiciaire. C'est ce qui ressort notamment de l'article 44/11/3*bis*, §2, b) en projet qui dispose que cette banque de données est créée dans le but de prendre notamment des décisions par les autorités de police judiciaire (à savoir un procureur, un juge d'instruction, etc.). Il est recommandé de mentionner cela en toutes lettres à l'article 44/2, § 2, à défaut de quoi cela resterait un point d'interrogation. Enfin, le dernier alinéa de l'article 44/2, § 2 en projet n'est pas très clair quand il évoque le « *traitement de ces banques de données* ». On veut peut-être dire par là « *la création et le traitement de données à caractère personnel et d'informations dans ces banques de données* ».

28. La Commission émet également des réserves quant à l'utilisation de la notion d'« *extrémisme, lorsqu'il peut mener au terrorisme* ». Elle a déjà eu l'occasion de le mentionner précédemment[10] mais il est important de souligner que l'extrémisme au sens de la loi du 30 novembre 1998 n'est actuellement pas une infraction/un fait punissable (sauf l'extrémisme sous la forme de racisme et de xénophobie). Si la notion d'« *extrémisme, lorsqu'il peut mener au terrorisme* » est séduisante en théorie, son utilisation commune par différents services risque de s'avérer délicate dans la pratique. La Commission se demande si le responsable opérationnel d'une banque de donnée commune aura suffisamment d'autorité pour en juger surtout s'il n'est pas issu des services de renseignement.

---

[10] Avis 30/2013 du 17 juillet 2013 concernant le projet de loi complétant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, en vue d'élargir la compétence de contrôle de la Cellule de traitement des informations financières en ce qui concerne l'extrémisme, https://www.privacycommission.be/sites/privacycommission/files/documents/avis_30_2013.pdf.

29. Autre élément tout aussi imprécis à l'heure actuelle : quel service ou entité aura la responsabilité opérationnelle de cette banque de données intégrée et commune (le(s)dit(s) gestionnaire(s), voir l'article 44/11/3*bis*, § 3 en projet). Les responsables du traitement sont bien désignés clairement en les personnes du Ministre de l'Intérieur et du Ministre de la Justice, mais on ne sait pas clairement qui sera ou est le sous-traitant/gestionnaire à proprement parler. C'est assez essentiel, non seulement pour permettre une gestion efficace de la (des) banque(s) de données (l'unité de commandement est également importante à cet égard), mais aussi pour que les organes de contrôle sachent clairement à qui ils doivent s'adresser en pratique. Du point de vue de la protection de la vie privée, il est essentiel de ne pas avoir trop de capitaines sur le navire, mais au contraire de savoir de manière extrêmement claire qui est (sont) le(s) responsable(s) opérationnel(s). Plus ils sont nombreux, plus cela devient problématique en termes d'efficacité, tant du point de vue opérationnel que de celui de la protection de la vie privée. L'article 44/11/3*bis*, § 3 en projet délègue cette compétence aux deux ministres. La Commission n'a dès lors à ce jour aucune indication quant au fonctionnement concret de la (des) banque(s) de données commune(s) envisagée(s). L'identité du gestionnaire sera transmise dans la déclaration qui sera faite par les deux ministres aux organes de contrôle (cf. l'article 44/11/3*bis*, § 3 en projet). La Commission préfère que cette désignation se fasse soit dans la loi, soit dans un arrêté d'exécution.

30. L'exposé des motifs indique enfin aussi que cette (ces) banque(s) de données ne veulent « *bien entendu pas dire que d'office l'ensemble de ces acteurs auront accès à une banque de données commune, mais, que sur la base de la finalité propre à la DB commune, de leur compétence légale et en fonction de leur besoin d'en connaître, tout ou partie de ceux-ci pourront avoir accès* » La Commission adhère à cette thèse mais aimerait aussi que cela soit inscrit dans la loi. Celle-ci devrait préciser (le cas échéant dans un arrêté d'exécution) le droit d'accès (aussi bien en lecture qu'en écriture) maximal de chaque acteur dans les banques de données communes et les finalités précises pour lesquelles leur accès est nécessaire.

II. Analyse de l'article 7 de l'avant-projet – modifications apportées à l'article 44/3 de la LFP

1. Présentation des modifications

31. L'avant-projet prévoit la désignation d'un conseiller en sécurité et en protection de la vie privée pour les données traitées dans le cadre des banques de données communes, en ajoutant un paragraphe 3 à l'article 44/3 de la LFP. Il est chargé pour ces banques de données des mêmes missions confiées aux conseillers désignés par les différents services de police ainsi que des contacts avec les organes en charge du contrôle des données incluses dans les banques de

données communes. Il exerce ses fonctions en toutes indépendance par rapport aux acteurs ayant directement accès aux banques de données communes et rend compte directement aux ministres de l'Intérieur et de la Justice.

2. Analyse des modifications

32. La Commission prend note de la désignation envisagée d'un conseiller en sécurité en charge notamment de la politique de sécurisation et de protection des données à caractère personnel des banques de données communes.

33. Cette désignation fait suite à l'introduction par la loi du 18 mars 2014 *relative à la gestion de l'information policière* de la figure du conseiller en sécurité et en protection de la vie privée au niveau des services de police. La Commission avait salué l'initiative dans son avis relatif à l'avant-projet de cette loi[11]. Il en va évidemment de même concernant la désignation envisagée de ce nouveau conseiller pour les banques de données communes.

34. La Commission remarque cependant que rien n'est précisé sur les modalités de désignation du conseiller, ni sur l'autorité ou l'instance qui le désigne. Elle invite le demandeur à préciser à tout le moins qui va désigner ce conseiller. On peut supposer que cela se fera peut-être par le responsable du traitement et donc par les deux ministres de tutelle.

35. La Commission se demande pourquoi la disposition relative à la constitution de la plate-forme chargée de veiller à la réalisation coordonnée du travail des conseillers se retrouve à présent entre le paragraphe relatif à la désignation des conseillers pour les banques de données originaires et la disposition relative aux conseillers en charge des banques de données communes. Il serait utile de mettre cette dernière disposition en dernier lieu dans l'article 44/3 dès lors que les conseillers en charge des banques de données communes devraient également participer à l'initiative de la plate-forme commune.

III. Analyse de l'article 9 de l'avant-projet – modifications apportées à l'article 44/6 de la LFP

1. Présentation des modifications

36. Cet article instaure le contrôle des données incluses dans les banques de données communes par l'introduction d'un alinéa 2 à l'article 44/6 de la LFP, qui prévoit actuellement le contrôle des

[11] https://www.privacycommission.be/sites/privacycommission/files/documents/avis_47_2013.pdf.

données traitées notamment dans les 3 catégories originaires de banques de données policières par l'Organe de contrôle de l'information policière (en abrégé, COC).

37. L'avant-projet introduit en l'occurrence un contrôle conjoint des données au sein des banques de données communes par le COC, le Comité permanent de contrôle des services de renseignement et de sécurité (Comité R) et le Comité permanent de contrôle des services de police (Comité P), dès lors que ces banques de données vont être alimentées et/ou exploitées notamment par l'OCAM, les services de police et les services de renseignement.

2. Analyse des modifications

38. La Commission ne voit pas d'obstacles à ce que des synergies soient créées au niveau du contrôle de ces banques de données communes afin d'en assurer tous les aspects.

39. Cela étant, associer à cette tâche pas moins de trois organes conjointement ne paraît pas praticable. La Commission a toujours souligné qu'un contrôle doit aussi être efficace dans la pratique et qu'il doit y avoir une cohésion de l'équipe en charge du contrôle à cet égard. Impliquer trois organes parlementaires qui connaissent eux-mêmes une structure et un processus décisionnel de type collégial à cet exercice risque de poser des problèmes d'efficacité. La logique semble dès lors d'associer uniquement le COC et le Comité R à ce contrôle conjoint, afin de ne pas complexifier inutilement le contrôle. En effet, impliquer le COC et le Comité P paraît redondant et le COC est l'organe en première ligne en ce qui concerne le traitement de l'information policière.

IV. Analyse de l'article 11 de l'avant-projet – insertion des articles 44/11/3*bis* à 44/11/3*quater* de la LFP

Le demandeur prévoit l'insertion d'une sous-section 7*bis* intitulée « Des banques de données communes » dans le chapitre IV, section 1re*bis* de la LFP et l'introduction au sein de cette sous-section des articles 44/11/3*bis* à 44/11/3*quater*.

1. Présentation du nouvel article 44/11/3bis de la LFP

40. Cet article édicte les conditions de création et de traitement des banques de données communes.

41. Il désigne tout d'abord les responsables du traitement des banques de données communes, à savoir le Ministre de l'Intérieur et le Ministre de la Justice qui peuvent conjointement créer des banques de données communes (§ 1er).

42. Cet article énonce ensuite les deux finalités distinctes de création d'une banque de données commune (§ 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 différents acteurs concernés en matière de prévention et de suivi du terrorisme et de l'extrémisme pouvant mener au terrorisme ;
- l'aide à la prise de décisions par les autorités administratives, de police administrative ou de police judiciaire, en matière de prévention et de suivi du terrorisme et de l'extrémisme pouvant mener au terrorisme.

43. Le demandeur introduit également une disposition permettant la transparence de la création effective de ces banques de données communes. Il est ainsi prévu que les responsables du traitement doivent faire une déclaration préalable de la création d'une banque de données commune, du gestionnaire qu'ils désignent et des modalités de traitement, dont l'enregistrement des données, au COC, au Comité R et au Comité P qui émettent conjointement un avis dans les 30 jours à partir de la réception de la déclaration (voir toutefois les remarques de la Commission au point 39) (§ 3).

44. En ce qui concerne le type de données à caractère personnel qui pourront être traitées dans ces banques de données communes, l'avant-projet prévoit la possibilité de traiter différentes catégories de données à caractère personnel relatives notamment aux personnes, aux groupements, aux organisations et aux phénomènes liés aux missions de prévention et de suivi du terrorisme et de l'extrémisme pouvant mener au terrorisme (§ 4).

45. Le demandeur précise que ces données et informations relatives à différentes catégories de données peuvent ou non être des données à caractère personnel et informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

46. Au niveau de la durée de conservation des données à caractère personnel, il est énoncé qu'elles sont supprimées dès que les finalités ayant présidé à leur création disparaissent, et au maximum 30 ans après le dernier traitement. Il est examiné au minimum tous les 3 ans après le dernier traitement si la finalité pour laquelle les données à caractère personnel et les informations sont traitées dans la banque de données commune est toujours présente (§ 5).

47. Le demandeur justifie une telle durée en arguant du fait que les phénomènes de terrorisme et d'extrémisme pouvant conduire au terrorisme ne peuvent en effet pas être traités utilement sur

des courtes périodes vu que les réponses opérationnelles à apporter sont tributaires d'une compréhension historique, anthropologique et sociétale de ceux-ci.

48. L'avant-projet prévoit par ailleurs une journalisation de tous les traitements réalisés par les directions, services, organes, organismes, autorités ou commissions, dans les banques de données communes, conservée pendant 30 ans à partir du traitement réalisé (§ 6).

49. L'exposé des motifs précise que cette journalisation doit permettre de vérifier la conformité des traitements réalisés et peut aussi être utilisée à des fins opérationnelles, par exemple pour contacter directement le service et/ou la personne qui a alimenté ou consulté la banque de données commune afin notamment d'obtenir de plus amples renseignements.

50. Le dernier paragraphe stipule enfin que des modalités complémentaires de gestion des banques de données communes peuvent être déterminées par un arrêté royal délibéré en Conseil des ministres (§ 7).

2. Analyse du nouvel article 44/11/3bis de la LFP

- *Quant à la responsabilité du traitement des banques de données communes*

51. La Commission prend note de la désignation en qualité de responsables du traitement des ministres de l'Intérieur et de la Justice. Ces derniers sont déjà responsables pour la BNG et les banques de données de base de la police en fonction de la nature judiciaire ou administrative des données concernées. S'agissant de traitements impliquant différents acteurs de la chaîne pénale, policière et de sécurité dépendant pour la plupart de ces ministres, leur responsabilité finale en ce qui concerne ces banques de données communes tombe sous le sens. Il paraît à cet égard difficile de mettre en place un système de responsabilité générale au niveau des acteurs opérationnels comme c'est le cas pour les banques de données particulières.

52. Cela étant, des responsabilités spécifiques (opérationnelles) doivent être dégagées pour chaque banque de données commune, sous peine de voir se dégrader rapidement la qualité des données en leur sein. Ainsi, le demandeur a prévu la désignation d'un gestionnaire pour chaque banque de données commune. Sa responsabilité quant à la qualité et la pertinence des données devrait être précisée. La Commission songe notamment à la nécessité de disposer d'un interlocuteur dans le cadre du contrôle qu'elle sera amenée à exercer dans le cadre des demandes d'accès indirect aux informations qui seront traitées dans ces banques de données communes sur base de l'article 13 de la LVP (cf. chapitre 5 de l'avant-projet analysé infra). Par ailleurs, pour les organes de contrôle qui seront finalement retenus (COC et/ou Comité P et Comité R), il est essentiel, comme

indiqué, qu'ils puissent s'adresser à un responsable opérationnel. La Commission renvoie à cet égard à nouveau vers sa remarque formulée au point 29.

- *Quant aux finalités spécifiques des banques de données communes*

53. La Commission fait remarquer que la création d'une banque de données communes ne devrait intervenir que dans des circonstances spécifiques qui nécessitent une mise en commun de données, en l'espèce dans le cadre des finalités générales de la prévention et du suivi du terrorisme (voir ci-avant le point 27 relatif à la signification du terme « *suivi* ») et de l'extrémisme pouvant mener au terrorisme (voir ci-avant le point 28 relatif à cette notion), dès lors que la gestion séparée de données ne permet pas de remplir adéquatement ces finalités générales.

54. La Commission souhaite faire remarquer que des finalités stratégiques, tactiques et opérationnelles sont ou peuvent quand même être très différentes de sorte que l'on se demande si cette (ces) banque(s) de données intégrée(s) et commune(s) contiendra(contiendront) conjointement ces trois types de données. Dans l'affirmative, il faudra installer des systèmes (assurément complexes) d'accès différencié selon le principe « need to know ». On ne voit ainsi pas directement pourquoi la Commission permanente de la police locale ou la Direction générale Sécurité et Prévention du SPF Intérieur devraient avoir accès à des données à caractère personnel et informations tactiques et opérationnelles. La Commission estime donc qu'il convient au minimum que les informations stratégiques d'une part, et les informations tactiques/opérationnelles d'autre part, soient intégrées dans des banques de données distinctes avec des accès et des profils adaptés ou au moins que ces profils d'accès soient établis lorsque les trois types d'informations sont intégrés dans une seule banque de données. En réalité, la Commission souhaite que les finalités stratégiques, tactiques et opérationnelles soient distinguées les unes des autres et décrites précisément dans la loi ou un arrêté d'exécution. A partir de là, un accès différencié des différents acteurs selon la finalité poursuivie doit être prévu dans la loi ou un arrêté d'exécution.

- *Quant aux catégories de données à caractère personnel traitées*

55. Il est fait référence au lien que les catégories de données doivent présenter avec les missions de prévention et de suivi du terrorisme et de l'extrémisme pouvant mener au terrorisme. La Commission invite le demandeur à préciser dans le texte légal que ces catégories de données doivent être adéquates, pertinentes et non excessives au regard non seulement de ces missions mais également des finalités visées au § 2 de l'article 44/11/3*bis* en projet.

56. S'agissant de la qualité des données, le demandeur précise qu'il appartiendra aux gestionnaires des banques de données communes à veiller à travers la mise en place de procédures adéquates de ces principes de bonne gestion. La Commission s'interroge aussi quelque peu quant au fait que des informations classifiées soient reprises avec des informations non classifiées dans une seule banque de données commune. Cela signifie en effet que cette banque de données ne peut être consultée que par des personnes disposant d'une habilitation de sécurité correcte, à moins que l'on puisse techniquement scinder les deux types d'informations afin d'empêcher qu'un fonctionnaire ne disposant pas d'habilitation de sécurité consulte quand même des informations classifiées. La toute grande majorité des magistrats de parquet ne disposent par exemple pas d'une habilitation de sécurité de sorte que soit ils devront la demander, soit ils ne pourront obtenir qu'un accès limité à la ou aux banques de données communes et ne pourront consulter que les informations non classifiées. Si dans l'exposé des motifs on affirme que « *Même si le Ministère Public n'est pas un service qui fournit directement les banques de données communes, il a bien besoin d'un accès direct dans le cadre de l'exercice de ses missions légales* », la Commission attire l'attention à cet égard sur cette problématique complexe, qui se pose peut-être aussi pour de nombreuses autres personnes faisant partie d'un des organes prévus à l'article 44/11/3*ter* en projet.

57. La Commission rappelle qu'elle souhaiterait que l'organe ou l'entité qui sera gestionnaire, le rôle et la responsabilité de ces gestionnaires soient définis dans le texte légal, ou, au moins délégué au Roi (cf. points 29 et 52).

- *Quant à la déclaration préalable de la création d'une banque de données commune*

58. La Commission réitère ses commentaires formulés au point 39 quant à l'association de trois organes parlementaires collégiaux dans le cadre de l'avis préalable à la création d'une banque de données commune. Elle estime que l'association du COC et du Comité R à l'exercice présentent des garanties minimales d'un contrôle préalable à la fois exhaustif et efficace.

59. Le demandeur mentionne dans l'exposé des motifs relatif au contrôle à posteriori des banques de données communes que les organes en charge de ce contrôle pourront lors des contrôles vérifier que leurs recommandations émises à l'occasion de la déclaration préalable ont bien été suivies. La Commission invite le demandeur à préciser directement dans le texte légal que les organes chargé du contrôle peuvent émettre des recommandations au travers des avis qu'ils rendent dans le cadre de la déclaration préalable. Il semble d'ailleurs évident que les organes de contrôle désignés doivent pouvoir faire des recommandations à tout moment et pas uniquement à l'occasion de la déclaration.

60. Le demandeur précise qu'au cas par cas, pour chaque banque de données, les catégories de données à caractère personnel traitées devront notamment être précisées dans la déclaration commune. La Commission invite à faire figurer cette obligation spécifique en ce qui concerne la déclaration des catégories de données à caractère personnel traitées directement dans le texte de l'avant-projet.

- *Quant au délai de conservation des données traitées*

61. La Commission constate qu'un délai de conservation maximal de 30 ans est prévu. Le projet s'inspire ainsi du règlement tel qu'applicable à l'OCAM où les données et informations de la banque de données de l'OCAM sont conservées durant un délai de 30 ans[12].

62. La Commission estime qu'il s'agit d'un délai acceptable.

63. La Commission renvoie aussi le demandeur à la solution retenue pour la BNG avec un mécanisme d'archivage des données passé un délai raisonnable. Elle rappelle qu'il s'agit en tout état de cause d'un délai maximal qui ne peut justifier la conservation de données inadéquates, non pertinentes ou excessives au regard de la finalité spécifique de la banque de données commune ou de données ne présentant pas ou plus la qualité requise, notamment au regard des règles d'enregistrement.

64. Le demandeur précise dans l'exposé des motifs que l'examen d'office tous les 3 ans a été prévu afin que des données à caractère personnel et des informations qui ne répondent plus à l'une des finalités poursuivies en créant les bases de données communes ne restent pas dans l'attente de l'effacement au terme du délai maximal prévu.

65. La Commission estime que le texte de l'avant-projet ne reflète pas tout à fait cette intention et invite le demandeur à préciser le texte de l'avant-projet. La Commission constate que ce délai de révision de 3 ans est plus court que celui prévu pour le système d'information de l'OCAM dans l'arrêté d'exécution de l'OCAM (art. 5, § 2, 2e alinéa) et estime dès lors que ce délai plus court est positif.

- *Quant à la journalisation des traitements réalisés dans les banques de données communes*

[12] Article 5, § 1er de l'arrêté royal du 28 novembre 2006 *portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace*.

66. La Commission apprécie que la journalisation soit prévue dans le texte légal dès lors que ce procédé technique devrait permettre de responsabiliser les acteurs dans leur alimentation des banques de données communes et de dépister les éventuels abus du système.

67. Elle prend acte du délai de conservation des données de journalisation retenu qui coïncide avec la durée actuellement retenue de conservation des données au sein des banques de donnés communes.

- *Quant aux modalités complémentaires de gestion des banques de données communes*

68. L'avant-projet prévoit qu'un arrêté royal délibéré en Conseil des Ministres peut venir déterminer des modalités complémentaires de gestion des banques de données communes.

69. La Commission souhaiterait qu'un tel arrêté royal lui soit soumis préalablement pour avis, vu sa potentielle influence sur les traitements de données à caractère personnel au sein des banques de données communes.

3. Présentation du nouvel article 44/11/3ter de la LFP

70. Cet article détermine les différents acteurs qui alimentent et accèdent aux banques de données communes.

71. Tout ou partie des données sont « *directement accessibles* », « *sur la base du besoin d'en connaître* » aux directions ou services des acteurs suivants énumérés dans le nouvel article 44/11/3*ter* de la LFP :

- l'Organe pour la coordination de l'analyse de la menace (OCAM)
- la police intégrée
- la Commission permanente de la police locale
- la Direction générale Centre de Crise
- la Direction générale Sécurité et Prévention du Service public Fédéral Intérieur
- la Direction générale des Établissements pénitentiaires et les établissements pénitentiaires
- le Service Public Fédéral Affaires étrangères, Direction générale Affaires consulaires
- le Ministère public
- la Sûreté de l'État
- le Service général du renseignement et de la sécurité des forces armées (SGRS)
- la Cellule de traitement de l'information financière (CTIF)
- l'Office des étrangers
- les services d'enquête et recherche de l'administration générale des douanes et accises

72. Le demandeur précise dans ses explications relatives à la possibilité de créer des banques de données communes qu'une gestion commune ne veut pas dire que l'ensemble des acteurs concernées auront d'office accès à une banque de données commune, mais, que sur la base de la finalité propre à la banque de données commune, de leur compétence et en fonction de leur besoin d'en connaître, tout ou partie de ceux-ci pourront avoir accès. Il s'agira de déterminer au cas par cas, sur la base des besoins tactiques, stratégiques et opérationnels et des finalités quels organes participent ou non à l'alimentation et/ou la consultation d'une telle banque de données.

73. L'avant-projet ajoute que d'autres autorités publiques belges, organes ou organismes publics ou d'intérêt public chargés par la loi de l'application de la loi pénale ou qui ont des missions légales de sécurité publique, peuvent être autorisées par arrêté royal à accéder directement en tout ou partie aux banques de données communes.

74. Une obligation de principe d'alimenter les banques de données communes est édictée, tandis que des règles plus précises d'enregistrement doivent être déterminées par les ministres de l'Intérieur et de la Justice, où l'on tient notamment compte de l'avis que doit émettre l'organe de contrôle. On prévoit enfin une procédure d'embargo similaire à celle existant déjà à l'article 44/8 de la LFP au sujet de l'alimentation de la BNG.

4. Analyse du nouvel article 44/11/3ter de la LFP

75. La Commission constate que les acteurs ayant un accès direct à la banque de données commune font partie de ce que l'on peut appeler la chaîne pénale, policière et de sécurité.

76. La Commission constate et regrette cependant qu'une gradation dans l'accès ne soit pas mise en place comme c'est le cas pour la BNG, pour laquelle trois possibilités d'accéder aux données et informations policières par les partenaires de la chaîne pénale, policière et de sécurité sont prévues, à savoir la « *communication* », l'« *interrogation directe* » (comparable à un « système hit/no hit ») et l'« *accès direct* ». Dans ce cadre, la LFP stipule en outre qu'un arrêté royal doit venir préciser les modalités d'accès et d'interrogation directs par les partenaires et ajoute que ces modalités portent au moins sur le besoin d'en connaître, les catégories de membres du personnel qui disposent d'un accès, les traitements automatisés impliqués, l'obligation du respect du secret professionnel et les mesures de sécurité minimales.

77. Il n'est pas proportionnel de prévoir un accès direct à cette (ces) banque(s) de données commune(s) pour tous les organes prévus à l'article 44/11/3*ter* en projet. On ne comprend ainsi pas pourquoi la Commission permanente de la police locale devrait disposer d'un tel accès. Les

mêmes questions se posent au sujet de la Direction générale Sécurité et Prévention du SPF Intérieur, de la Direction générale des Établissements pénitentiaires et de (tous les) établissements pénitentiaires et « du » Ministère public (MP). En ce qui concerne le MP, on ne sait pas clairement qui ou quelle fonction est visé(e) par « le » MP. S'agit-il de chaque magistrat de parquet ? S'agit-il également du personnel de soutien ? L'Organe Central pour la Saisie et la Confiscation fait également partie du MP. Y a-t-il également un accès direct pour l'OCSC ? Il semble qu'il faille au minimum préciser qu'il doit s'agir de magistrats de parquet chargés de cette matière. Des questions similaires peuvent se poser pour les Douanes et Accises, ainsi que pour la CTIF. De quelles informations au maximum ont-ils besoin, et pour quelle finalité légitime précisément ? Que peut bien faire la CTIF d'informations sur l'extrémisme ? Jusqu'à nouvel ordre, il ne s'agit pas d'une infraction (voir avis n° 30/2013 du 17 juillet 2013[13]), et les enquêtes de la CTIF ont essentiellement pour finalité de fournir des informations au MP en vue par exemple de poursuivre éventuellement le financement du terrorisme (pas de l'extrémisme). Il convient donc d'inscrire dans la loi ou un arrêté d'exécution, pour chaque service, quel type d'accès est l'accès maximal du point de vue de la proportionnalité, et pour quelle finalité légitime précise un tel accès peut être nécessaire.

78. La Commission invite dès lors le demandeur à mettre en place un système similaire d'accès différencié notamment en fonction de la finalité spécifique de la banque de données commune.

79. En tout état de cause, le principe théorique du « besoin d'en connaître » ou « need to know » et l'application de ce principe dans la pratique doit être clarifié notamment quant à son implémentation technique.

80. Par ailleurs, on a vu que les banques de données communes peuvent contenir des données classifiées. Le demandeur ne peut dès lors faire l'économie d'un système d'accès graduel et personnalisé dès lors que l'accès à de telles données nécessite une habilitation de sécurité dans le chef de celui qui les consulte.

81. La Commission note également que le demandeur a prévu la déclaration préalable aux instances de contrôle du gestionnaire de la banque de données commune (voir toutefois le point 43). Cela étant, son rôle devrait être défini dans le cadre des règles d'accès aux banques de données communes, notamment quant à son rôle de 'dirigeant' de la banque de données commune et quant à la validation des données.

---

[13] demande d'avis concernant le projet de loi complétant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, en vue d'élargir la compétence de contrôle de la Cellule de traitement des informations financières en ce qui concerne l'extrémisme: https://www.privacycommission.be/sites/privacycommission/files/documents/avis_30_2013.pdf.

82. L'exposé des motifs fait valoir que deux niveaux existent concernant la validation des données à caractère personnel et des informations : le premier qui prévoit que l'alimentation des banques de données communes se fait en concertation entre les services de renseignement et de sécurité, l'OCAM et la police fédérale et le second prévoyant l'alimentation selon les règles de validation internes, propres à chaque service.

83. La Commission ne voit pas où se traduisent ces deux niveaux de validation dans le texte légal et invite le demandeur à corriger le texte de l'avant-projet sur ce point très important. En effet, la question de savoir qui valide les données à caractère personnel et informations à reprendre dans les banques de données précitées et qui en prend la responsabilité est essentielle. La Commission souligne qu'une possibilité directe d'alimentation et de validation par d'autres services que les services de renseignement et de sécurité, l'OCAM ou la police fédérale implique de grands risques pour la qualité et la fiabilité des informations introduites. Il faudrait au minimum confier au responsable opérationnel de la (des) banque(s) de données commune(s) la validation d'informations fournies par des services autres que les services précités, en mentionnant explicitement tant la fiabilité des informations proprement dites que leur source[14].

84. Enfin, la Commission accueille favorablement la prévision de règles précises d'enregistrement à déterminer par les ministres de l'Intérieur et de la Justice. La Commission juge en effet qu'il est nécessaire de fixer des critères d'enregistrement objectifs précisés à tout le moins dans une circulaire, à l'instar de ce qui se passe dans le cadre de la BNG via la Circulaire MFO-3[15] (circulaire qu'il convient d'ailleurs à son tour de moderniser, vu le cadre légal qui a été substantiellement modifié entre-temps). La Commission invite à cet égard le demandeur à préciser que les règles doivent être non seulement précises mais également objectives. À défaut de telles règles, la pertinence des données à caractère personnel enregistrées sera difficile à justifier.

5. Présentation du nouvel article 44/11/3quater de la LFP

85. Cet article prévoit la possibilité de communiquer les données extraites d'une des banques de données communes à une autorité ou entité tierce selon les modalités déterminées conjointement par les ministres de l'Intérieur et de la Justice, en concertation avec le Collège des Procureurs généraux, après évaluation par ceux des services qui ont livré tout ou partie de ces données ou informations.

---

[14] En utilisant par exemple la "4x4 intelligence-matrix" telle qu'utilisée au niveau d'Europol et dans le cadre de la collaboration quotidienne avec Europol, où tant la fiabilité des informations que leur source sont classées sur une échelle de 4.

[15] Directive commune MFO-3 des Ministres de l'Intérieur et de la Justice du 14 juin 2002 *relative à la gestion de l'information de police judiciaire et de police administrative*, dont le contenu est à portée confidentielle.

6. Analyse du nouvel article 44/11/3quater de la LFP

86. La Commission constate que la LFP fait une distinction entre la communication des données de la BNG à des partenaires nationaux et des partenaires internationaux et prévoit des règles relatives à une communication récurrente ou volumineuse.

87. La Commission recommande d'en faire de même ici.

88. En ce qui concerne des acteurs privés ou des acteurs publics en dehors de la chaîne pénale et de sécurité, La Commission considère que ces règles devraient être fixées par arrêté royal (délibéré ou non en Conseil des ministres) soumis préalablement à son avis, créant ainsi au moins davantage de transparence quant à la question de savoir à quels tiers privés ces données extrêmement sensibles sont communiquées et selon quelles règles cela se fait. Cette disposition déroge en effet au principe général consacré jusqu'à présent et depuis la création en 1992 de la LFP, à savoir qu'aucune information policière ne peut être communiquée à des tiers privés. Les actuels articles 44/11/4 à 44/11/13 inclus (l'ensemble de la sous-section 8 : « *La communication des données et l'accès à la B.N.G.* ») ne permettent pas le transfert d'informations policières au départ des banques de données policières à des tiers privés. Pour la première fois, on déroge toutefois à ce principe, de sorte qu'il convient de prévoir plusieurs garanties importantes à cet effet. Enfin, la notion d'« *entité* » tierce n'est pas très claire. Peut-être vise-t-on des parties tierces privées ? Il est recommandé de le mentionner également dans le texte de la loi ou au moins dans l'arrêté royal nommé ci-dessus, soumis préalablement à l'avis de la Commission.

B.4. Examen du chapitre 5 de l'avant-projet – modification de la LVP

89. Les banques de données communes pouvant contenir des données issues de la Sûreté de l'État, du SGRS ou de l'OCAM, des exceptions aux obligations de la LVP similaires à celles qui existent pour les traitements propres de ces services sont prévues pour les traitements au sein des banques de données communes.

90. La Commission reconnaît qu'il est préférable d'étendre le champ d'application de l'article 3, § 4 pour y inclure les traitements au sein des banques de données communes, afin de ne laisser aucun doute quant à l'exclusion des traitements qui y sont opérés à certaines obligations de la LVP, notamment en ce qui concerne les droits d'accès des personnes concernées.

91. À cet égard, il est nécessaire pour la Commission de disposer de personnes de contact afin de pouvoir contrôler les traitements opérés dans le cadre de l'accès indirect prévu à l'article 13 de la LVP, dès lors qu'il y a une volonté d'écarter l'application des droits d'accès au sens large prévus

aux articles 10 à 12 de la LVP. Ces personnes pourraient être les gestionnaires désignés des banques de données communes. Il est en tout cas nécessaire pour la Commission (et pour les autres organes de contrôle chargés de contrôler la banque de données commune) de disposer d'interlocuteurs susceptibles d'entreprendre des actions sur les traitements effectués (accès, correction, suppression) au sein des banques de données communes.

PAR CES MOTIFS,

Au vu des observations formulées dans le présent avis, la Commission émet :

- un avis favorable sur le chapitre 2 de l'avant-projet ;
- un avis favorable sur le chapitre 3 de l'avant-projet, moyennant la prise en compte de ses remarques formulées aux points 15 et 16 ;
- un avis favorable en ce qui concerne les points suivants du chapitre 4 de l'avant-projet :
  - la désignation d'un conseiller en sécurité et en protection de la vie privée pour les données traitées dans le cadre des banques de données commune, moyennant la prise en compte de ses remarques formulées aux points 34 et 35 ;
  - la mise en place d'un contrôle conjoint des banques de données communes par des organes parlementaires indépendants, moyennant la prise en compte de sa remarque formulée aux points 39 et 58 ;
  - la responsabilité générale des Ministres de l'Intérieur et de la Justice du traitement des données à caractère personnel au sein des banques de données communes ;
  - la finalité générale de création des banques de données communes, moyennant la prise en compte de ses remarques formulées aux points 27 et 28 ;
  - le type de données à caractère personnel traitées dans les banques de données communes, moyennant la prise en considération de ses remarques formulées aux points 55, 56 et 60 ;
  - la déclaration préalable de la création d'une banque de données communes aux organes de contrôle, moyennant la prise en compte de ses remarques formulées aux points 59 et 60 ;
  - les délais de conservation et de révision des données à caractère personnel traitées dans les banques de données commune ;
  - la journalisation des traitements réalisés dans les banques de données communes ;
  - la possibilité de déterminer par arrêté royal des modalités complémentaires de gestion des banques de données communes, moyennant la prise en compte de sa remarque formulée au point 69 ;
  - la prévision de règles précises d'enregistrement à déterminer par les ministres de l'Intérieur et de la Justice ;
- un avis défavorable en ce qui concerne les points suivants du chapitre 4 de l'avant-projet :

- la création de nouvelles banques de données sans examen sérieux de la possibilité d'améliorer le système d'information de l'OCAM et du risque de chevauchement avec les banques de données et fichiers de travail existants (voir points 23 à 26) ;
- l'absence de désignation d'un responsable opérationnel pour chaque banque de données commune (voir points 29, 52, 57 et 81) ;
- le manque de précision dans la détermination des finalités spécifiques de création des banques de données communes (voir point 54) ;
- l'absence de mise en place dans le texte légal d'un accès différencié selon les finalités précises poursuivies par les différents acteurs et la difficulté de l'implémentation pratique du concept théorique du « besoin d'en connaître » (voir points 30 et 76 à 80) ;
- l'absence d'un mécanisme de validation des données traitées au sein des banques de données communes (voir points 82 et 83) ;
- l'encadrement faible de la communication des données à caractère personnel extraites des banques de données communes à des entités tierces (voir points 26 et 86 à 88) ;

- un avis favorable sur le chapitre 5 de l'avant-projet, moyennant la prise en compte de sa remarque formulée au point 91.

L'Administrateur f.f., Le Président

(sé) An Machtens (sé) Willem Debeuckelaere