Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 77/2024 du 23 août 2024

Objet: Demande d'avis concernant un projet de loi *concernant la résilience des entités critiques* (CO-A-2024-205)

Mots-clés : Entités critiques – OCAM – autorités sectorielles – communication de données – vérification de sécurité - SICAD

Version originale

Introduction

L'avis concerne un projet de loi transposant la Directive (UE) 2022/2557 du Parlement et du Conseil relative à la résilience des entités critiques.

L'Autorité relève principalement l'utilisation de notions imprécises telles que « *informations utiles* » ou de « *toute autre autorité* » ou encore l'absence d'éléments objectifs permettant de déterminer quelles personnes sont susceptibles de faire l'objet d'une vérification de sécurité ou quand des données peuvent valablement être communiquées à une entité fédérée.

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité »),

Présent.e.s : Mesdames Juline Deschuyteneer, Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Gert Vermeulen;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu l'article 43 du règlement d'ordre intérieur selon lequel les décisions du Service d'Autorisation et d'Avis sont adoptées à la majorité des voix;

Vu le 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* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu la demande d'avis de Madame Annelies Verlinden, Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique (ci-après « la demanderesse »), reçue le 6 juin 2024;

Vu les informations complémentaires reçues le 19 juin 2024 ;

Émet, le 23 août 2024, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le demanderesse a sollicité l'avis de l'Autorité concernant un projet de loi concernant la résilience des entités critiques (ci-après « le projet ») et plus particulièrement les art. 8, 16, 19, 20, 23, 24 et 63.

2. L'exposé des motifs précise que le projet entend transposer la Directive (UE) 2022/2557 du Parlement et du Conseil relative à la résilience des entités critiques[1].

II. EXAMEN DU PROJET

1) Analyse de la menace par l'OCAM (art. 8) et échange d'informations (art. 23)

3. L'art. 8 en projet impose à l'OCAM de réaliser, au plus tard tous les 4 ans, une évaluation stratégique commune[2] (ci-après « *analyse de la menace* ») pour les secteurs et sous-secteurs énumérés en annexe du projet. Pour ce faire, l'art. 8, §3 en projet impose à l'autorité désignée « *Point de Contact Central National pour la résilience des entités critiques* » par le Roi, aux autorités sectorielles[3] (telles que l'IBPT, la Banque nationale ou l'Agence fédérale des médicaments et de produits de santé), aux

[1] Pour une analyse historique de la législation relative aux infrastructures critiques et en particulier de la directive dite « CER », que le projet entend transposer, voy. Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*, *8*(sup1), 85–101. https://doi.org/10.1080/23789689.2022.2128562

[2] Visée à l'art. 8, al. 1er, 1° de la loi du 10 juillet 2006 relative à l'analyse de la menace (MB 20.07.2006)

[3] Enumérées dans l'annexe au projet (et, le cas échéant, devant encore faire l'objet d'une désignation par AR)

services de renseignement et de sécurité, aux services de police, à l'Administration des Douanes et Accises, au service public fédéral Mobilité et Transports, à l'Office des Etrangers, au SPF Affaires étrangères, à la Direction Générale Centre de Crise, à la direction générale Etablissements pénitentiaires, au Service des Cultes et de la Laïcité, à l'administration générale de la Trésorerie et aux services publics désignés par le Roi, sur la proposition du Conseil national de sécurité[4] de communiquer les « *informations utiles* » à l'OCAM.

4. En ce qui concerne les mesures ayant un impact sur la protection des données, le projet a principalement deux effets :

   1) Il ajoute de nouveaux types de menaces aux missions de l'OCAM[5] et par conséquent de nouvelles finalités de communication et de traitements de données ; et
   2) il étend la liste des services, autres que les services d'appui, qui sont astreint à une obligation de communication des « informations utiles ».

Communication d'informations utiles à l'OCAM

5. L'Autorité relève tout d'abord que les **services publics susceptibles d'être désignés par le Roi doivent à tout le moins être déterminables** sur base de leurs missions légales. Il convient donc de reformuler l'art. 8 en ce sens et de démontrer le caractère nécessaire et proportionné de l'intégration de ces services d'appui supplémentaires.

6. Ensuite, l'Autorité observe que, la notion d' « *informations utiles* » figurant à l'art. 8, §3 est remplacée, dans le commentaire de cette disposition, par celle d' « *informations pertinentes* ». Le commentaire de l'art. 8 se contente de préciser que ces informations « *peuvent comprendre des rapports d'incidents émis par des entités critiques* ».

7. A cet égard, il y a lieu de rappeler que l'OCAM n'a pas été créé pour être un service de renseignement. En d'autres termes, l'OCAM n'a pas vocation à collecter directement des informations. Les informations lui sont communiquées par ses services d'appui. La fonction d'analyse de la menace est apparue suite à un attentat contre la synagogue de Bruxelles, en 1982 et était alors confiée au Groupe Interforce Antiterroriste (G.I.A.) intégré aux services de la gendarmerie[6] (l'idée, un instant évoquée, que ce

[4] En d'autres termes, aux services d'appui de l'OCAM énumérés à l'art. 2, al. 1er, 2° de la loi relative à l'analyse de la menace précitée

[5] Poursuivant ainsi la tendance initiée par la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (MB 15 juillet 2011)

[6] T. Coosemans, « Les dispositifs de sécurité avant et après le 11 septembre 2001 », *Courrier hebdomadaire*, CRISP, n° 1762-1763, 2002, p. 32

service soit actif sur le terrain fut « rapidement abandonnée »[7]). Cependant, le GIA souffrait de problèmes de circulation des informations[8].

8. Suite aux attentats du 11 septembre 2001, de nouvelles structures de coordination sont mises en places partout dans le monde[9]. C'est dans cette optique que, « *le 10 novembre 2004, le Comité ministériel du renseignement et de la sécurité a décidé que le G.I.A. allait être transformé en un organe où toutes les informations pertinentes pour une évaluation de la menace devraient être regroupées et où ces données pourraient être analysées et traitées* »[10]. Cette décision fut traduite par l'adoption de la loi du 10 juillet 2006 relative à l'analyse de la menace[11].

9. La Commission de la protection de la vie privée (CPVP), prédécesseur en droit de l'APD, a rendu l'avis 8/2005[12] au sujet de ce projet de loi. A cette occasion la CPVP relevait déjà - tout comme la section de législation du Conseil d'Etat[13] – que :

- *la* ***notion de « pertinence » n'est pas définie*** *dans le texte*[14] ;
- *le* ***risque d'imposer à des responsables de traitement des obligations qui n'entrent pas dans le cadre de leurs missions premières***[15] ;
- *la Commission s'interroge en particulier sur la* ***détermination des critères*** *sur base desquels les services partenaires estimeront qu'une information est pertinente*[16] ;
- *à défaut de* ***directives précises****, l'on risque d'aboutir à une communication particulièrement large d'informations, dans la mesure où un service préférera transmettre trop que trop peu sous peine d'être sanctionné, ce qui conduirait à une* ***transgression, notamment du principe de proportionnalité*** *tel que prévu par la loi relative à la protection de la vie privée*[17] ;

---

[7] W. Van LAETHEM, « L'Organe de coordination pour l'analyse de la menace : une analyse ponctuelle », Vigiles, 2007/4, p. 110, note 6

[8] T. Coosemans, « Les dispositifs de sécurité avant et après le 11 septembre 2001 », *op. cit.*, p. 31 ; K. Lasoen, « Indications and Warning in Belgium: Brussels is not Delphi », *Journal of Strategic Studies*, volume 40, n° 7, 2017, p. 932.

[9] Voy. W. Van LAETHEM, « L'Organe de coordination pour l'analyse de la menace », *op. cit.*, p. 111

[10] *Ibidem.*, p. 112

[11] MB 20.07.2006

[12] Avis du 25 mai 2005, Doc. parl. Ch., 17 octobre 2005, 51-2032/001, p. 90 (https://www.lachambre.be/FLWB/pdf/51/2032/51K2032001.pdf)

[13] Avis n° 38.782/2/V donné le 11 août 2005, Doc. parl. Ch., 17 octobre 2005, 51-2032/001, p. 63

[14] Point 10, p. 94

[15] Avis n°33 du 13 décembre 1999 concernant des projets de loi relatifs à la criminalité informatique, p. 9 et 10; avis d'initiative n°44/2001 du 12 novembre 2001 concernant la compatibilité et la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications, p. 6 ; L'avis 8/2005 (point 11, p. 94) précise en outre que « *s'il entre dans les missions légales des services de renseignements et de police de rechercher, d'analyser et de traiter des informations en vue d'assurer la sécurité de l'État, de ses citoyens et le maintien de l'ordre public, il n'en est pas de même des autres membres de l'OCAM (les «services partenaires») dont les missions légales sont d'un tout autre ordre. Or, l'avant-projet exige de ces services une première analyse de l'information au regard de la menace qui existe ou pourrait exister sur la sécurité de l'État* ».

[16] *Op. cit.*, point 12

[17] *Ibidem.*, point 12

- *l'OCAM devrait déterminer de la façon la plus précise possible les traitements qu'il entend effectuer afin que les services partenaires disposent de* ***lignes directrices claires*** *quant à la pertinence des informations qu'ils sont supposés transmettre*[18] ;
- *il est essentiel que le projet prévoie le traçage de l'information (de qui provient-elle, à qui a-t-elle été communiquée, etc.) et qu'un contrôle a posteriori notamment quant à la pertinence de la communication de cette information soit prévu à l'égard de toutes les autorités membres de l'OCAM*[19].

10. En réponse à ces avis, les travaux parlementaires de la loi de 2006 précisent que le gouvernement ne partage pas l'observation relative au manque de précision entrainant un risque de voir la disposition considérée comme disproportionnée. « *Il souhaite insister sur la circonstance qu'****il s'agit ici «uniquement» d'un transfert de données déjà récoltées légalement par d'autres autorités publiques****. De plus,* ***le transfert ne concerne souvent pas des données personnelles*** *mais principalement des évènements. Il est important à cet égard de souligner que ces données ne sont pas utilisées par l'OCAM pour prendre des décisions individuelles de nature administrative ou judiciaire, par exemple, à l'égard de personnes concrètes mais bien de réaliser des analyses de la menace* ».

11. Cette précision - qui gagnerait à être rappelée dans les travaux préparatoires du projet - confirme que l'OCAM n'a pas vocation à collecter directement des informations (et encore moins des données à caractère personnel). En effet, Les services bénéficiant du statut de service d'appui sont soumis à une obligation légale de communication de renseignements. A noter que cette obligation a été qualifiée d'inédite, car les homologues européens de l'OCAM n'en bénéficient pas[20].

Extension des autorités à qui une obligation de communication d'information est imposée

12. En visant dans une même disposition relative à l'obligation de communication[21], à la fois les services de police et de renseignement, les autres services d'appui et les autorités sectorielles auxquelles l'obligation de communication est étendue, les auteurs du projet engendrent un risque de confusion quant à l'étendue de l'obligation pesant sur les uns et les autres.

---

[18] *Ibidem.*, point 13

[19] *Ibidem.*, point 13, p. 96

[20] C. THOMAS, « L'organisation fédérale de la lutte antiterroriste en Belgique », Courrier hebdomadaire du CRISP 2020/18-19 (n° 2463-2464), p. 79

[21] A savoir l'art. 8, §3 du projet

13. En effet, l'obligation de communication pesant sur les services d'appui est de nature tant proactive que réactive (sous réserve d'embargo)[22] et elle est susceptible de viser des catégories particulières de données[23]. En revanche, les autorités sectorielles (telles que l'IBPT, la Banque nationale ou l'Agence fédérale des médicaments et de produits de santé) n'ont pas vocation à collecter auprès des entités concernées des données à caractère personnel pour une finalité liée à la lutte contre les menaces terroristes et encore moins des catégories particulières de données au sens de l'art. 9.2. du RGPD.

14. Il en résulte la nécessité de mentionner dans le projet que l'obligation de communication pesant sur les autorités sectorielles (et en particulier en ce qui concerne les données à caractère personnel) se limite à une **communication des données expressément demandées par l'OCAM et dont elles disposent déjà en vertu de leurs missions**. L'Autorité estime par ailleurs qu'il convient de préciser dans le commentaire de l'article concerné que toute velléité d'une autorité sectorielle de se muer en service d'enquête ou de communiquer spontanément à l'OCAM[24] des données à caractère personnel relatives à une éventuelle suspicion, serait nécessairement considéré comme un traitement de données disproportionné et, par conséquent, illicite.

Informations « utiles » mais données à caractère personnel « nécessaires »

15. Enfin, en ce qui concerne les données à caractère personnel dont la communication peut être demandée par l'OCAM, l'Autorité rappelle son avis 34/2024[25], soulignant que c'est au critère de nécessité qu'il convient d'avoir égard pour déterminer la possibilité de traiter des données. « *Et la nécessité de traiter des données sera in concreto appréciée compte-tenu de la finalité du traitement et de la phase d'exercice de la mission concernée (la nécessité d'une donnée pourra varier selon le cycle du renseignement ; notamment, ce n'est pas parce qu'une donnée ne s'avère plus nécessaire dans une phase ultérieure d'exercice de la mission concernée, qu'elle ne l'était pas dans sa phase initiale)* ».

16. L'Autorité estime donc que, comme le prévoient d'ailleurs déjà les dispositions les plus actuelles applicables aux services de renseignement[26], l'art. 8, §3 en projet doit être modifié afin de prévoir qu' « *en ce qui concerne les données à caractère personnel, l'obligation de communication à l'OCAM*

---

[22] Voy. les art. 6 et le CHAPITRE IV de la loi de 2006; Le fait d'appliquer un même régime aux services de police et de renseignement qu'aux autres services d'appui, dépasse la saisine de l'Autorité dans le cadre du présent avis ; pour une critique du libellé de cette disposition voy. l'avis n° 184/2021 du 4 octobre 2021, points 40 et sv. (https://www.autoriteprotectiondonnees.be/publications/avis-n-184-2021.pdf) et W. Van LAETHEM, « L'Organe de coordination pour l'analyse de la menace », *op. cit.,* pp. 116 et sv.

[23] Art. 142 LTD

[24] Plutôt qu'au parquet ou aux services de police

[25] Rendu le 15 avril 2024 au sujet de la Proposition de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour, point 28 (

[26] Telles que l'art. 108 LTD

porte exclusivement sur les données nécessaires à la réalisation d'une analyse de la menace par l'OCAM » (et non les informations utiles ou pertinentes).

17. La même remarque vaut pour l'échange de « *toute information utile pour la prise de mesures externes de protection des entités critiques* » visé à l'art. 23 en projet.

2) Communication de l'analyse de la menace par l'OCAM aux autorités sectorielles (art. 8, §4)

18. L'art. 8, §4 dispose que l'OCAM communique l'évaluation de la menace aux autorités sectorielles. Cette communication a pour finalité de permettre aux autorités sectorielles d'intégrer ces conclusions dans l'analyse de risque qu'elles sont tenues d'effectuer.

19. L'Autorité présume que ces conclusions communiquées par l'OCAM **ne comprennent pas de données à caractère personnel**, concernant des auteurs ou des suspects, provenant des services d'appui[27]. Le cas échéant, il convient de le préciser.

20. **Si des données à caractère personnel devaient malgré tout figurer dans les conclusions communiquées**, il conviendrait de revoir fondamentalement le projet en veillant à démontrer le caractère nécessaire et proportionné d'une telle communication et à déterminer les éléments essentiels de l'enregistrement de ces données par les autorités sectorielles. Cette détermination devrait intervenir dans les différentes lois organiques de ces autorités sectorielles, mais il conviendrait de mentionner une référence à ces dispositions dans les travaux préparatoires du présent projet. Dans un tel cas de figure, il conviendrait en outre de préciser que sauf cas exceptionnel dûment motivé, seule une version pseudonymisée des conclusions sera communiquée aux autorités sectorielles.

3) Point de contact de l'entité critique (art. 16)

21. L'art. 16, §1er, al. 2 en projet dispose que le point de contact de l'entité critique remplit la fonction de point de contact vis-à-vis d'une série de d'autorités énumérées ainsi que « *de toute autorité ou service public compétent pour toute question liée à la résilience de l'entité et de son infrastructure* ».

22. L'Autorité rappelle que, sauf à exclure la communication de données à caractère personnel des auteurs ou suspects connus des services d'appui et de l'OCAM du rôle de point de contact, le nombre de destinataires potentiels de ces données a un impact très important sur l'ingérence dans les droits et

[27] En effet, pour autant que besoin, la communication de données à caractère personnel à la direction d'une entité critique interviendrait par le biais du parquet ou des services de police et non de l'OCAM

libertés des personnes concernées. **Il est donc essentiel que la liste des destinataires et les finalités de communications soient déterminées de manière suffisamment précise pour permettre à un responsable du traitement d'évaluer si une (demande de) communication de telles catégories de données à tel bourgmestre ou à telle autre autorité est bien légalement fondée et nécessaire**.

23. Par conséquent, il y a lieu de modifier l'art. 16 en projet en vue de préciser, **soit** que des données à caractère personnel des auteurs ou suspect connus des services d'appui et de l'OCAM ne seront en aucun cas communiquées au point de contact, **soit** quelles catégories de données à caractère personnel sont susceptibles d'être communiquées, par qui, pour quelle finalité, moyennant quelle durée de conservation maximale, etc. En d'autres termes, dans cette seconde hypothèse, outre le caractère nécessaire et proportionné du traitement, l'ensemble des éléments essentiels relatifs à ce traitement doivent être déterminés dans le projet.

4) Initiation d'une vérification de sécurité par les entités critiques (art. 19)

24. L'art. 19 en projet permet à une entité critique de demander une vérification des antécédents[28] pour l'exercice d'une profession, d'une fonction, d'une mission ou d'un mandat ou pour l'accès à ses locaux, bâtiments ou terrains.

25. Le commentaire relatif à cette disposition précise que « *le risque existe que les collaborateurs des entités critiques ou leurs contractants abusent par exemple de leurs droits d'accès pour causer des dommages au sein de l'organisation de l'entité critique* ».

26. Si la finalité de ce traitement doit être considérée comme suffisamment spécifique, déterminée et légitime, il n'en demeure pas moins que le **champ d'application personnel** n'est pas défini de manière suffisamment précise pour permettre à un responsable du traitement de déterminer envers quelles catégories de personnes une telle vérification est nécessaire et proportionnée et dans quels cas une demande ne pourrait en aucun cas être autorisée.

27. L'Autorité rappelle par ailleurs qu'en prévoyant une « *possibilité* » de demande de vérification, un responsable du traitement ne pourrait voir sa responsabilité engagée que si une telle demande était formulée alors qu'un tel traitement ne serait pas nécessaire et proportionné au regard des finalités visées. En revanche, rien ne pourrait être reproché au responsable du traitement qui s'abstiendrait de

[28] Visée à l'art. 22quinquies de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé (MB 7.05.1999)

réclamer une telle vérification. Afin de soumettre ce traitement au régime de l'obligation légale[29], il conviendra de veiller, lors de la reformulation de l'art. 19, à prévoir qu'une telle vérification « *doit* » être demandée.

28. L'Autorité estime par conséquent que l'art. 19 en projet doit être reformulé de manière à **déterminer de manière objective les catégories de personnes** (en fonction de leurs tâches ou d'autres éléments qu'il convient de décrire) pouvant faire l'objet d'une vérification de sécurité ainsi que le **moment auquel cette demande peut être formulée** (avant l'entrée en service, périodiquement, à la suite d'un événement devant être déterminable à la lecture du projet et du commentaire concerné ?)[30].

5) Obligation d'information lorsque survient un événement (art. 20)

29. L'art. 20 en projet impose aux entités critiques d'**informer** trois autorités, dont le Service d'information et de communication de la police fédérale au niveau de l'arrondissement judiciaire[31] (ci-après **le « SICAD »),** lors de la survenance d'un événement.

30. Sans préjudice des éventuelles observations du COC à ce sujet, l'Autorité estime que la **désignation du SICAD en lieu et place d'une autorité de police administrative territorialement compétente doit être dûment justifiée** dans le commentaire de la disposition concernée. L'Autorité en profite pour rappeler que si, par hypothèse, le libellé de l'art. 20 avait été retenu pour répondre à une réalité technique (par exemple parce que les services placés sous la responsabilité des gouverneurs de Province ne disposent pas d'une infrastructure comparable), il conviendrait d'adapter la technique aux normes relatives à la détermination des compétences des autorités et non d'adapter les normes à une solution technique existante.

6) Echange d'informations avec les entités fédérées (art. 24, §2)

31. L'art. 24, §2 en projet dispose que l'autorité sectorielle[32] (telles que l'IBPT, la Banque nationale ou l'Agence fédérale des médicaments et de produits de santé), l'autorité désignée « *Point de Contact Central National pour la résilience des entités critiques* » par le Roi et l'entité critique « *peuvent, le cas*

[29] A toutes fins utiles, l'Autorité précise qu'une obligation légale n'implique pas qu'une modalisation soit inconcevable.

[30] Sur cette question voy. également les observations formelles du CEPD relatives à la proposition de directive sur la résilience des entités critiques, formulées le 11 août 2021, p. 3 (https://www.edps.europa.eu/system/files/2021-08/21-08-11_edps_comments_critical_entities_fr.pdf)

[31] Tel que visé par la loi du 7 décembre 1998 organisant un service de police intégré, structuré a deux niveaux

[32] Enumérées dans l'annexe au projet (et, le cas échéant, devant encore faire l'objet d'une désignation par AR)

échéant, échanger des informations avec les entités fédérées, pour les entités critiques relevant de leur compétence ».

32. Pour autant que ces échanges comportent des données à caractère personnel, l'Autorité estime qu'il convient de faire preuve d'une précision bien plus grande dans le libellé d'une disposition susceptible de fonder une communication à des entités fédérées.

33. En tout état de cause, la seule présence d'une entité critique (telle que le siège d'une banque ou une entreprise agro-alimentaire) sur le territoire d'une Région ne peut justifier la communication de données à caractères personnelles aux autorités régionales. Par ailleurs, si l'entité fédérée est responsable du traitement de l'entité critique, il n'est pas à proprement parler question de communication de données, au sens du RGPD, entre l'entité critique et l'entité fédérée.

34. Par conséquent, pour autant que l'échange d'information implique une communication de données à caractère personnel, l'art. 24, §4 doit être reformulé de manière à **encadrer plus précisément cette communication et à permettre d'identifier les hypothèses dans lesquelles une communication de données devrait être considérée comme illicite**. A noter que si l'échange d'information devait être obligatoire et ou réciproque, un tel échange ne pourrait être effectué de manière licite qu'après la conclusion d'une accord de coopération.

7) Modification de la loi du 10 juillet 2006 relative à l'analyse de la menace (art. 63)

35. L'art. 63 insère dans la loi du 10 juillet 2006 relative à l'analyse de la menace, une obligation de communication, par les services d'appui de l'OCAM[33], des catégories particulières de données[34] et les renseignements dont ils disposent dans le cadre de leurs missions légales et qui s'avèrent pertinents en vue d'atteindre les finalités de l'analyse de la menace visée à l'art. 8, §2 (commenté *supra*).

36. L'Autorité estime que la référence à l'art. 142 LTD est ici insuffisante. Il convient en revanche d'**encadrer la banque de données** dans laquelle les données seront enregistrées. S'il s'agit de la banque de données commune, il convient de se référer aux dispositions pertinentes et de préciser quelles seront les mesures mises en place pour éviter la communication de données non pertinentes

[33] A savoir aux services de renseignement et de sécurité, aux services de police, à l'Administration des Douanes et Accises, au service public fédéral Mobilité et Transports, à l'Office des Etrangers, au SPF Affaires étrangères, à la Direction Générale Centre de Crise, à la direction générale Etablissements pénitentiaires, au Service des Cultes et de la Laïcité, à l'administration générale de la Trésorerie

[34] Plus particulièrement « *les données à caractère personnel de toute nature, en ce compris celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, les données qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes* »

aux autres services partenaires. En d'autres termes, il convient de prévoir des mesures permettant d'éviter, par exemple, que les convictions religieuses communiquées par le Service des Cultes soient rendues accessibles à la CTIF. Si la communication intervient par le biais d'une autre banque de données, il convient d'encadrer ce traitement sur le même modèle que la banque de données commune. Le cas échéant, il y a lieu de tenir compte de son avis 97/2023[35], lors de la rédaction des dispositions encadrant l'échange de renseignements entre les services d'appui et l'OCAM.

PAR CES MOTIFS,
L'Autorité
estime que :

- l'art. 8 doit être reformulé de manière à ce que les services publics susceptibles d'être désignés par le Roi soient déterminables sur base de leurs missions légales et le caractère nécessaire et proportionné de l'intégration de ces services d'appui supplémentaires doit être démontré dans le commentaire (point 5) ;
- la circonstance qu'il s'agit uniquement d'un transfert de données déjà récoltées légalement par d'autres autorités publiques et que ce transfert ne concerne souvent pas des données personnelles doit être rappelée dans le commentaire des art. 8 et 23 (points 10 et 17) ;
- il convient d'indiquer dans le projet que « l'obligation de communication pesant sur les autorités sectorielles (en ce qui concerne les données à caractère personnel) se limite à une communication des données expressément demandées par l'OCAM et dont elles disposent déjà en vertu de leurs missions » et de préciser dans le commentaire de l'article concerné que toute velléité d'une autorité sectorielle de se muer en service d'enquête ou de communiquer spontanément à l'OCAM des données à caractère personnel relatives à une éventuelle suspicion, serait nécessairement considéré comme un traitement de données disproportionné et, par conséquent, illicite (points 14 et 17) ;
- les art. 8, §3 et 23 en projet doivent être modifiés afin de prévoir qu' « *en ce qui concerne les données à caractère personnel, l'obligation de communication à l'OCAM porte exclusivement sur les données nécessaires à la réalisation d'une analyse de la menace par l'OCAM* » (points 16 et 17) ;
- l'art. 8, §4 doit être reformulé (points 18 à 20) ;
- la liste des destinataires et les finalités de communications doivent être déterminées de manière plus précise (points 22 et 23) ;

[35] Avis du 16 juin 2023 relatif à un avant-projet de loi portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » 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'art. 19 doit être reformulé de manière à déterminer de manière objective les catégories de personnes pouvant faire l'objet d'une vérification de sécurité ainsi que le moment auquel cette demande peut être formulée (point 27 et 28) ;
- désignation du SICAD doit être dûment justifiée (point 30) ;
- l'art. 24, §4 doit être reformulé de manière à encadrer plus précisément cette communication (points 32 à 34) ;
- il convient d'encadrer la banque de données dans laquelle les données seront enregistrées (point 36).

Pour le Service d'Autorisation et d'Avis,
(sé.) Cédrine Morlière, Directrice