Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 108/2025 du 17 octobre 2025

Objet : Avis concernant un projet d'arrêté royal établissant un cadre de référence pour la consultation des données ETIAS à des fins répressives (CO-A-2025-161).

Mots-clés : ETIAS – European Travel Information and Authorisation System ; accès à des données des voyageurs ; finalité répressive ; autorités compétentes.

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

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 la Justice, chargée de la Mer du Nord, et de Monsieur Bernard Quintin, ministre de la Sécurité et de l'Intérieur, chargé de Beliris, reçue le 16 septembre 2025 ;

Vu la demande d'informations complémentaires adressée au demandeur le 30 septembre 2025 ;

Vu les réponses communiquées par le demandeur le 7 octobre 2025 ;

Vu la demande d'informations complémentaires adressée au demandeur le 8 octobre 2025 ;

Vu les réponses communiquées par le demandeur le 13 octobre 2025 ;

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») émet, le 17 octobre 2025, l'avis suivant :

L'Autorité ne publie en français et en néerlandais que les avis concernant les projets ou propositions de textes de rang de loi émanant de l'Autorité fédérale, de la Région de Bruxelles-Capitale ou de la Commission Communautaire Commune. La « Version originale » est la version qui a été validée.

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le demandeur a introduit auprès de l'Autorité une demande d'avis concernant un projet d'arrêté royal *établissant un cadre de référence pour la consultation des données ETIAS à des fins répressives* (ci-après, « **le Projet** »). Le Projet établit la liste des infractions visées à l'article 13, § 2, al. 2, de la loi du 29 mars 2024 *relative à la création et à l'organisation des missions de l'Unité nationale ETIAS* (ci-après, « l'U.N.E. » et la « **Loi ETIAS** »).

2. La Loi ETIAS exécute certaines dispositions du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 *portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) no 1077/2011, (UE) no 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226* (ci-après, « **le Règlement ETIAS** »). L'Autorité s'est prononcée au sujet de l'avant-projet de cette loi dans son Avis n° 121/2023 du 18 juillet 2023 *concernant un avant-projet de loi relatif à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) (CO-A-2023-236) et un avant-projet de loi modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) (CO-A-2023-237)* (ci-après, « **l'Avis de 2023 de l'Autorité** ») auquel il est renvoyé à des fins de contextualisation.

3. Sauf indication explicite dans le sens contraire, **l'Autorité n'aborde pas dans le présent avis les suites qui ont été réservée à son Avis de 2023 dans la Loi ETIAS.**

II. EXAMEN DU PROJET

II.1. Compétence de l'Autorité

4. Selon les traitements de données à caractère personnel concernés dans le contexte normatif du « European Travel Information and Autorisation System » (ci-après, « **ETIAS** »), le Règlement ETIAS prévoit l'application du RGPD, de la **Directive 2016/680**[1] ou du Règlement 2018/1725[2]. Le Projet s'inscrit plus précisément dans le cadre de la **consultation** des données du système ETIAS **à des fins**

[1] 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.*

[2] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE*.

Pour être exhaustif, dès lors qu'Europol est impliquée, encore convient-il d'évoquer le Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 *relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI*.

répressives[3]. A ce sujet, il se dégage des articles 1, 2.[4], et 56, 3., du Règlement ETIAS que **cette consultation à des fins répressives est soumise à la Directive 2016/680**[5], qui en droit belge, est transposée dans le **Titre 2 de la LTD**. L'article **66, 3., du Règlement ETIAS** dispose quant à lui que « [l]*'autorité de contrôle* ***instituée conformément à l'article 41, paragraphe 1, de la directive (UE) 2016/680***[6] *contrôle la licéité de l'accès aux données à caractère personnel par les États membres* » (mis en gras par l'Autorité) s'agissant de la consultation du système ETIAS à des fins répressives.

5. En droit belge, les **autorités compétentes** pour demander de tels accès aux fins d'une telle consultation sont l'Office des étrangers (ci-après, « **l'OE** ») ainsi que les « *services* » visés à l'article 6, 2°, a), c), d), e), de la Loi ETIAS, soit les Services de police, la Sûreté de l'Etat (ci-après, « **la VSSE** »), le Service Général du Renseignement et de la Sécurité des Forces armées (ci-après, « **le SGRS** »), et l'Administration générale des Douanes et Accises (ci-après, « **l'AGD&A** »).

6. Le Règlement ETIAS lui-même, les articles 30 et 31 de la Loi ETIAS et la LTD déterminent les règles de protection des données applicables à ces traitements de données ainsi que les autorités de contrôle compétentes en la matière.

7. L'Autorité dispose en l'occurrence en droit positif d'une compétence limitée aux autorités publiques compétentes (pour consulter les données ETIAS à des fins répressives) suivantes. S'agissant de **l'AGD&A**, au considérant n° 113 de son **Avis de 2023**, l'Autorité avait souligné ce qui suit : « *L'Autorité attire l'attention du demandeur sur le fait que même lorsqu'elle agit dans le cadre du titre 2 de la LTD, l'AGD&A demeure soumise au contrôle de l'Autorité de Protection des Données*[…]*. Or l'article 34 du Projet, concernant l'accès à ETIAS à des fins répressives*[…]*, ne modifie que l'article 281 de la loi du 18 juillet 1977 générale sur les douanes et accises*[…]*. La compétence octroyée au COC à l'égard de l'AGD&A dans le cadre du fonctionnement de l'UIP a nécessité une modification de l'article 71 de la*

---

[3] Articles 50-52 du Règlement ETIAS.

[4] « *2. Le présent règlement fixe les conditions dans lesquelles les autorités désignées des États membres et Europol peuvent consulter les données conservées dans le système central ETIAS aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves relevant de leur compétence, ainsi qu'aux fins des enquêtes en la matière* ».

[5] « *La directive (UE) 2016/680 s'applique au traitement de données à caractère personnel par les autorités désignées des États membres aux fins de l'article 1er, paragraphe 2, du présent règlement* ».

[6] Selon lequel:

« *1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application de la présente directive, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union (ci-après dénommées «autorité de contrôle»).*

2. Chaque autorité de contrôle contribue à l'application cohérente de la présente directive dans l'ensemble de l'Union. À cette fin, les autorités de contrôle coopèrent entre elles et avec la Commission conformément au chapitre VII.

3. Les États membres peuvent prévoir qu'une autorité de contrôle instituée au titre du règlement (UE) 2016/679 est l'autorité de contrôle visée dans la présente directive et prend en charge les missions de l'autorité de contrôle devant être instituée en vertu du paragraphe 1 du présent article.

4. Lorsqu'un État membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité visé à l'article 51 ».

LTD[7]*. Dans la logique du Projet, le COC devrait également être désigné, pour l'accès à ETIAS aux fins répressives, par l'AGD&A, via une modification de l'article 71 de la LTD* » (mise en gras enlevée dans le présent avis). **L'Autorité constate qu'en droit positif, elle est** toujours **compétente pour l'application du Titre 2 de la LTD à l'AGD&A** dans le cadre de la consultation à des fins répressives des données ETIAS.

8. Ensuite, en ce qui concerne **l'OE**, l'Autorité avait exprimé ce qui suit aux considérants nos 87 et 88 de son Avis de 2023 : « *L'Autorité relève au passage que l'article 41 du Projet fait désormais de l'OE une autorité compétente au sens du titre 2 de la LTD, en modifiant l'article 26, 7°, de la LTD, lorsque celui-ci exerce ses compétences répressives en vertu de l'article 81 de la loi du 15 décembre 1980*[…]*. Cette modification a une portée qui dépasse les objectifs du Projet. L'exposé des motifs du Projet se borne à préciser que cette intégration a lieu « compte tenu des compétences répressives » de l'OE*[…]*. L'Autorité prend acte de cette modification et du fait que l'Autorité de Protection des Données reste l'autorité de contrôle de l'OE* » (mise en gras enlevée dans le présent avis). Ce constat demeure, **l'Autorité est compétente pour appliquer le titre 2 de la LTD dans le cadre de la consultation à des fins répressives des données ETIAS, lorsque l'OE « *exerce ses compétences répressives en vertu de l'article 81 de la loi du 15 décembre 1980* »**[8].

9. Enfin, s'agissant du **SGRS** et de la **VSSE**, l'Autorité réitère la position exprimée au considérant n° 31 de son Avis de 2023 selon laquelle notamment, **le Règlement ETIAS n'apparaît pas laisser de marge de manœuvre pour rendre applicables et compétente des règles et une autorité de contrôle autres que celles découlant de la mise en œuvre de la Directive 2016/680** (ou du RGPD).

10. L'Autorité prend acte des raisons évoquées dans le commentaire des articles pertinents de la Loi ETIAS[9] qui en substance, recommandent les considérations suivantes. Ce commentaire précise notamment que « *Seul le législateur national est compétent en matière de sécurité nationale. Si le législateur souhaite inclure les services de renseignement et de sécurité, il peut très bien prévoir que la directive 2016/680 ne s'applique pas* ». **Cependant**, « *conformément à la jurisprudence constante de la Cour* [de justice], *bien qu'il appartienne aux États membres de définir leurs intérêts essentiels de sécurité et d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure,* ***le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale ne saurait***

---

[7] Voir l'article 13 de la loi du 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers, selon lequel :

« *L'article 71, § 1er, de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, est complété par un alinéa rédigé comme suit:*

"Elle est également, vis-à-vis de l'autorité compétente visée à l'article 26, § 1er, 7°, e), chargée de surveiller l'application de l'article 281, § 4, de la loi générale sur les douanes et accises du 18 juillet 1977" » (souligné par l'Autorité).

[8] Article 26, 7°, i), de la LTD.

[9] *Doc. Parl.*, Ch. des Repr., n° 55-3886/001, pp. 27-28.

entraîner l'inapplicabilité du droit de l'Union et dispenser les États membres du respect nécessaire de ce droit *[voir, en ce sens, arrêts du 4 juin 2013, ZZ, C-300/11, EU:C:2013:363, point 38 et jurisprudence citée ; du 20 mars 2018, Commission/Autriche (Imprimerie d'État), C-187/16, EU:C:2018:194, points 75 et 76, ainsi que du 2 avril 2020, Commission/Pologne, Hongrie et République tchèque (Mécanisme temporaire de relocalisation de demandeurs de protection internationale), C-715/17, C-718/17 et C-719/17, EU:C:2020:257, points 143 et 170]* » (mis en gras par l'Autorité)[10].

11. La consultation du système ETIAS à des fins répressives par le SGRS et la VSSE devrait par conséquent être soumise à des règles conformes à la Directive 2016/680 et relever de la compétence d'une autorité de protection des données désignée conformément à l'article 41 de cette directive et rencontrant les exigences consacrées dans les articles 42-47 de cette dernière. C'est à l'aune de ces considérations qu'**il appartient au demandeur de vérifier si le législateur pouvait soumettre la consultation d'ETIAS à des fins répressives par la VSSE et le SGRS au sous-titre 1er du titre 3 la LTD et à la compétence du Comité R** en tant qu'autorité de protection des données. Dans la négative, il convient d'adapter le cadre normatif applicable afin de garantir la sécurité juridique dans l'intérêt des activités des responsables du traitement et des personnes concernées.

12. Le commentaire des articles précise encore que « *La consultation des données ETIAS par les services de renseignement et de sécurité, telle que prévue aux articles 13 et 14 du projet de loi, ne peut se faire que dans le cadre de l'exécution des missions légales contenues dans les articles 7 et 11 de la loi du 30 novembre 1998 pour autant qu'elles se recoupent avec les finalités répressives telles que définies par le Règlement ETIAS. Si le titre 2 devenait applicable au traitement dans le cadre d'ETIAS, il en résulterait que des régimes de protection différents devraient être appliqués dans le cadre d'un seul fichier. Ceci est pratiquement irréalisable. Le titre 2 de la loi du 30 juillet 2018 ne s'applique qu'aux autorités visées à l'article 26 de la loi du 30 juillet 2018, qui poursuivent des fins répressives. Il n'inclut pas les services de renseignement et de sécurité* ».

13. Cette complexité découle des choix des législateurs européen et belge qui, tous deux, ont cherché à garantir le meilleur équilibre entre les droits et libertés des personnes concernées et l'action efficace des différentes autorités concernées. L'argument de l'impossibilité pratique d'appliquer des régimes de protection des données distincts *à un même fichier* ne semble pas décisif. En effet, des fichiers/traitements distincts, aux finalités distinctes, peuvent être mis en place, selon que l'autorité compétente concernée agit ou pas, comme une autorité « *compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces*

[10] C.J.U.E. (Gr. Ch.), arrêt du 6 octobre 2020, Privacy International, aff. C-623/17, considérant n° 44.

»[11]. La Cour de justice a elle-même par exemple reconnu que « *le caractère exhaustif des finalités visées à l'article 1er, paragraphe 2, de la directive PNR implique également que les données PNR* ***ne sauraient être conservées dans une base de données unique pouvant être consultée aux fins de la poursuite tant de ces finalités*** **[(visées par la Directive PNR)]** ***que d'autres finalités****. En effet, la conservation de ces données dans une telle base de données comporterait le risque que lesdites données soient utilisées à des fins autres que celles visées à cet article 1er, paragraphe 2* »[12] (mis en gras par l'Autorité). D'ailleurs, l'applicabilité de différents régimes de protection des données (Directive 2016/680 et RGPD) à une même autorité est une hypothèse déjà existante en droits belge et européen, compte-tenu des critères d'applicabilité matériel (finalité du traitement) et organique (autorité concernée) de la protection des données retenus dans ces droits. L'Autorité doute sur ce point que le régime juridique consacré dans la Directive 2016/680 – applicable à la Police et aux autorités judiciaires dans le domaine pénal – soit à ce point incompatible avec les activités des services de renseignement et de sécurité s'inscrivant dans le champ d'application de cette directive.

II.2. Criminalité grave et liste d'infractions

14. L'Autorité réitère tout d'abord la position qu'elle avait exprimée dans son **Avis de 2023, aux considérants nos 92-93**, auxquels elle se réfère à titre préliminaire, y compris quant à leur motivation : **la liste des infractions concernées devrait se trouver dans la Loi ETIAS**.

15. **Sans compter** les « *Infractions terroristes listées aux articles 3 à 14 de la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil* » (que le Projet ne liste pas) et le « Livre 2, Titre I*ter*, du CP » (cette catégorie est-elle d'ailleurs équivalente à la catégorie juste citée ?), le Projet vise, en comptant les dispositions se référant au nouveau Code pénal, **près de 330 dispositions du droit belge**.

16. L'Autorité **ne passe pas en revue toutes ces dispositions** et se limite à souligner que ne peuvent justifier la consultation à des fins répressives du système ETIAS, que les **infractions terroristes** (« *une infraction qui correspond ou est équivalente à l'une des infractions visées dans la directive (UE) 2017/541* ») et les **infractions pénales graves** (« *une infraction qui correspond ou est équivalente à l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI, si elle est passible, en droit national, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée*

[11] Article 3, 7., a), de la Directive 2016/680.

[12] C.J.U.E. (Gr. Ch.), 21 juin 2022 (Ligue des droits humains c/ Conseil des ministres), aff. C-817/19, considérant n° 235.

maximale d'au moins trois ans »)[13], conformément à l'interprétation à suivre imposée par la Cour de justice et la Cour constitutionnelle dans le contexte du traitement des données passagers[14].

17. L'Autorité relève néanmoins que la Loi ETIAS/le Projet **doit lister les dispositions de droit belge qui consacrent les** « *Infractions terroristes listées aux articles 3 à 14 de la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil* ».

18. Ensuite, c'est **l'article 2 du Projet**, et non la Loi ETIAS elle-même, qui précise que les services concernés « *doivent effectuer **au cas par cas** une appréciation relative à la gravité de l'infraction en cause* » (mis en gras par l'Autorité), et que « *L'appréciation de la gravité de l'infraction implique une vérification que **le seuil de gravité requis** pourrait être atteint au regard des circonstances en cause et, si nécessaire, une **évaluation complémentaire quant au caractère grave** de l'infraction* » (mis en gras par l'Autorité). Cette disposition appelle les commentaires suivants.

19. Premièrement, sans préjudice du commentaire suivant, l'Autorité est d'avis que **les obligations précitées devraient être consacrées dans la Loi ETIAS** elle-même.

20. Deuxièmement, **concrètement, cette disposition ne fixe pas de seuil de gravité ou des critères à appliquer** pour identifier dans quels cas une infraction est susceptible de constituer une infraction pénale grave (au-delà des infractions que la Cour de justice a considéré comme revêtant « *par leur nature, un niveau de gravité incontestablement élevé* »[15]). Il convient de souligner à ce sujet que **la Cour de justice n'a pas rejeté une approche qui se réfèrerait au *minimum* de la peine applicable** (plutôt qu'à son maximum)[16]. L'Autorité a interrogé le demandeur à ce sujet et celui-ci a notamment répondu ce qui suit :

> « […] *En droit pénal belge, il est généralement considéré que les infractions reprises à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle sont des infractions considérées comme graves et qui peuvent donc justifier une ingérence grave dans les droits fondamentaux, comme celle induite par les traitements des données PNR/ETIAS. La référence à cet article*

---

[13] Article 3, 15. et 16. du Règlement ETIAS.

[14] C.J.U.E. (Gr. Ch.), 21 juin 2022 (Ligue des droits humains c/ Conseil des ministres), aff. C-817/19 et C. Const., arrêt n° 131/2023 du 12 octobre 2023. Voir également l'Avis de 2023 de l'Autorité et les considérants nos 92-94.

[15] C.J.U.E. (Gr. Ch.), 21 juin 2022 (Ligue des droits humains c/ Conseil des ministres), aff. C-817/19, considérant n° 149

[16] C.J.U.E. (Gr. Ch.), 21 juin 2022 (Ligue des droits humains c/ Conseil des ministres), aff. C-817/19, considérant n° 151 :

«…***dans la mesure où l'article 3, point 9, de la directive PNR se réfère non pas à la peine minimale applicable, mais à la peine maximale applicable****, il n'est pas exclu que des données PNR puissent faire l'objet d'un traitement à des fins de lutte contre des infractions qui, bien qu'elles remplissent le critère prévu par cette disposition relatif au seuil de gravité, relèvent, compte tenu des spécificités du système pénal national, non pas des formes graves de criminalité, mais de la criminalité ordinaire* » (mis en gras par l'Autorité).

est dès lors mentionnée pour justifier que cette appréciation supplémentaire n'est pas requise lorsque l'infraction n'a pas été citée par la Cour de justice de l'Union européenne comme étant incontestablement grave (voir le point 149 de l'arrêt précité). On ne peut en effet déterminer à l'avance toutes les infractions qui seront suffisamment graves et (pour PNR) qui présenteront un lien direct ou indirect avec le transport international. Pour certaines infractions, ces éléments ne pourront être appréciés qu'au cas par cas en fonction des circonstances en cause (ex : une infraction qui ne peut atteindre le seuil de gravité que s'il s'agit d'une récidive, infractions pour lesquelles le lien avec le transport international est indirect) ».

21. Réinterrogé à ce propos[17], le demandeur a répondu ce qui suit :

« *Voor inbreuken die onder artikel 90ter, §§2 tot 4 van het Wetboek van Strafvordering (Code d'instruction criminelle) vallen,* ***is inderdaad <u>in principe</u> geen aanvullende beoordeling van de ernst van de inbreuk nodig omdat deze inbreuken over het algemeen beschouwd worden als ernstig****, étant entendu que le seuil de gravité requis par la directive PNR ou le règlement ETIAS (passible, en droit national, d'une* ***peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans****) doit toujours pouvoir être atteint* » (mis en gras par l'Autorité).

« ***Niet alle inbreuken die in de KB's vermeld worden zijn 'incontestablement graves' of vallen onder artikel 90ter, §§2 tot 4*** *van het Wetboek van Strafvordering. Le seuil de gravité requis est toujours le même pour ces infractions mais il faudra vérifier qu'il est bien atteint au regard des circonstances du cas - l'infraction n'est pas grave par nature mais* ***dans certaines circonstances****, elle le devient (récidive, mobile discriminatoire, usage de la violence,...). Voor deze inbreuken is dus een aanvullende beoordeling van de ernst nodig.* ***Om te beslissen of iets al dan niet ernstig is, moet men zich baseren op bestaande rechtspraak en rechtsleer die betrekking hebben op deze inbreuk en hoe de ernst van deze inbreuk beoordeeld kan worden*** » (mise en gras et souligné par l'Autorité).

22. Ces réponses appellent les commentaires suivants. Premièrement, l'Autorité prend acte du fait que sont « *en principe* » considérées comme atteignant le seul de gravité requis les infractions visées à **l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle,** pour autant qu'elles soient passibles

[17] Pour ce qui concerne les infractions qui ne sont pas par nature graves conformément à la jurisprudence de la Cour de justice, le critère de seuil de gravité est-il automatiquement rempli si l'infraction appartient à la liste des infractions reprises dans l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle (sans prise en considération de niveaux de peine) ? Y a-t-il des infractions citées dans les projets qui ne sont ni des infractions incontestablement graves visées par la Cour de justice, ni des infractions reprises dans l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle ? Dans l'affirmative, quel est alors le critère de seuil de gravité retenu pour ces infractions ?

d'une **peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans**, compte-tenu de la finalité de cette disposition du Code d'instruction criminelle en droit belge. Cela étant précisé, il convient de clarifier dans quels cas ce principe ne pourrait pas être suivi (si cette hypothèse peut se présenter), et de préciser alors quel(s) critère(s) supplémentaire(s) devrai(en)t être rempli(s).

23. Deuxièmement, **l'auteur du Projet doit préciser quel(s) critère(s) supplémentaire(s) clairs doi(ven)t être rempli(s), au-delà de la peine maximale d'au moins trois ans**, pour les **infractions visées par le Projet qui ne sont ni des infractions graves par nature** au sens de la jurisprudence de la Cour de Justice, **ni des infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle**. Une référence à la doctrine ou à la jurisprudence quant à la manière dont serait appréciée la gravité de ces faits ne constitue pas un/des critères sur la base desquels il est considéré qu'un seuil de gravité est atteint, n'est pas suffisamment déterminé et peut même constituer une source de discrimination (quelle jurisprudence ? ; quelle doctrine ? ; au choix de qui ?). Il convient de fixer à cet égard, **dans le cadre normatif**, des critères, le cas échéant issus de la jurisprudence (par exemple, un critère basé sur la peine qui serait susceptible d'être prononcée *in concreto* à l'aune des faits concernés ; de nouveau, un critère basé sur le niveau du minimum de la peine prononçable ; d'autres critères à identifier).

24. Troisièmement, l'Autorité est d'avis que ces critères et clarifications doivent être intégrés **dans le dispositif de la Loi ETIAS elle-même. Si le demandeur ne suivait pas l'Avis de l'Autorité sur ce point,** ces critères et clarifications devraient impérativement être intégrés **à tout le moins au dispositif du Projet**.

PAR CES MOTIFS,
L'Autorité est d'avis que :

1. Elle est compétente s'agissant de la consultation des données du système ETIAS à des fins répressives par l'Office des étrangers et l'Administration générale des Douanes et Accises (**considérants nos 4-8**) ;

2. La consultation à des fins répressives des données ETIAS par la Sûreté de l'Etat et le Service Général du Renseignement et de la Sécurité des Forces armées devrait relever de dispositions du droit belge conformes à la Directive 2016/680 et relever de la compétence d'une autorité de contrôle désignée conformément à cette même directive. Le Règlement ETIAS n'apparaît pas laisser de marge de manœuvre à cet égard. Il appartient au demandeur de vérifier, à l'aune de ces considérations, si le législateur pouvait soumettre la consultation d'ETIAS à des

fins répressives par ces services au sous-titre 1er du titre 3 la LTD et à la compétence du Comité R en tant qu'autorité de protection des données (**considérants nos 9-13**) ;

3. La liste des infractions concernées par la consultation du système ETIAS à des fins répressives devrait être reprise dans la loi ETIAS elle-même (**considérant n° 14**) ;

4. Ne peuvent justifier la consultation à des fins répressives du système ETIAS que les infractions terroristes et les infractions pénales graves conformément à l'interprétation donnée par la Cour de justice et la Cour constitutionnelle dans le contexte du traitement des données des passagers. L'Autorité n'est pas en mesure de passer en revue les nombreuses dispositions légales citées dans le Projet. Sans préjudice du point n° 3 précédent, le Projet doit également lister les dispositions de droit belge consacrant les infractions terroristes « *listées aux articles 3 à 14 de la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil* » (**considérants nos 15-17**) ;

5. Les obligations relatives à l'appréciation du seuil de gravité des infractions pouvant fonder la consultation du système ETIAS à des fins répressives devraient être consacrées dans la Loi ETIAS elle-même (**considérants nos 18-19**). Les critères applicables à ce seuil de gravité doivent être clarifiés dans le dispositif de la Loi ETIAS/du Projet (**considérants nos 20-22**).

Pour le Service d'Autorisation et d'Avis,
(sé) Alexandra Jaspar, Directrice