Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 121/2023 du 18 juillet 2023

Objet:
Demande d'avis 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)
Demande d'avis concernant 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)

Version originale

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye et Bart Preneel;

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 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances 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 les demandes d'avis de la ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique, Madame Annelies Verlinden (ci-après « la ministre » ou « le demandeur »), reçues le 8 juin 2023;

Émet, le 18 juillet 2023, l'avis suivant :

I. Objet et contexte de la demande d'avis

1. La ministre a introduit auprès de l'Autorité une demande d'avis 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) (ci-après, « **le Projet** »), et une demande d'avis concernant 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, « **le Projet modificatif** »).

2. Ces projets exécutent certaines dispositions du Règlement (UE) 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** »). Ce dispositif, s'inscrivant dans un contexte normatif complexe, concerne les ressortissants d'Etats tiers qui, dispensés de l'obligation d'obtenir un visa, souhaitent voyager dans l'Union. A sa genèse, ETIAS est inspiré de l'ESTA américain, de l'AVE du canadien et de l'eVisitor australien.

3. Le Contrôleur Européen de la Protection des Données (ci-après, « **CEPD** ») a rendu un avis au sujet de la proposition de Règlement ETIAS auquel l'Autorité renvoie à titre informatif[1].

[1] Celui-ci a toutefois souligné « *qu'en l'absence d'une analyse d'impact relative à la protection des données, qui constitue une condition sine qua non essentielle, il est impossible de procéder à une évaluation exhaustive de la nécessité et de la proportionnalité de l'ETIAS tel qu'il est proposé actuellement* » **CEPD, avis 3/2017** *sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)*, 6 mars 2017 (ci-après « **avis CEPD ETIAS** »). Ultérieurement, voir CEPD, avis sur l'AIPD de l'ETIAS, Dossier 2021-0640, disponible sur https://edps.europa.eu/system/files/2022-03/22_03_27_formal_consultation_etias_dpia_fr.pdf, dernièrement consulté le 05/07/2023.

II. Examen

4. L'examen des Projets est structuré comme suit :

5. **Sur le plan de la protection des données**, ETIAS se situe à la fois dans le champ d'application du **RGPD**, dans celui de la Directive **2016/680**[2] et dans celui du **Règlement 2018/1725**[3]. L'article 31 du Projet découpe le Projet selon les règles de protection des données belges applicables. Conformément à la LTD, l'Autorité rappelle qu'elle ne se prononce pas sur le traitement de données à caractère personnel par les autorités compétentes (dont les services de police) visées au titre 2 de la LTD, compétence relevant de l'Organe de Contrôle de l'information policière (ci-après, « **COC** »), ou par les services de renseignement et de sécurité visés au titre 3 de la LTD, pour lesquels le Comité permanent de contrôle des services de renseignement et de sécurité est compétent. Ces autorités ont été saisies par le demandeur dans leurs compétences respectives.

6. Le **Règlement ETIAS** lui-même contient une série de **dispositions spécifiquement relatives au traitement de données à caractère personnel et en particulier** : son article 13 (accès aux données conservées dans ETIAS) ; son Chapitre XI (articles 54 et 55) (conservation[4] et modification des données) ; son Chapitre XII (protection des données), dont l'article 56 ventile l'application du RGPD et de la Directive 2016/680, l'article 57 identifie un responsable du traitement des données et l'article 58 désigne un sous-traitant, l'article 59 vise la sécurité des traitements, l'article 60 concerne les incidents de sécurité, l'article 61 porte sur l'autocontrôle, l'article 62 exige des sanctions, l'article 63 a trait à la responsabilité (civile – droit à réparation), l'article 64 vise le droit d'accès, l'article 65 limite les communications de données à caractère personnel à des Etats tiers ou des entités privées, les articles 66 à 68 visent le contrôle par les autorités de contrôle et leur coopération, et les articles 69 et 70 prévoient la tenue de registres.

7. En résumé, les Projets soumis pour avis s'inscrivent entre autres dans des logiques institutionnelles (création de l'Unité nationale ETIAS belge, répartition des tâches, etc.) et procédurales (organisation des accès, organisation d'une voie de recours dans le Projet de modification, etc.).

8. Le Règlement ETIAS et le Projet impliquent clairement une **ingérence particulièrement importante** dans les droits et libertés des personnes concernées. En ce sens notamment : les

---

[2] 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.*

[3] 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*.

[4] Le dossier de demande est conservé pendant la durée de validité de l'autorisation de voyage ou pendant cinq ans à compter de la dernière décision de refus, d'annulation ou de révocation (sous réserve de suppression anticipée, voir l'article 54, 1., b), du Règlement ETIAS). Le demandeur peut également consentir à ce que son dossier demeure conserver afin de faciliter une nouvelle demande (article 54, 2., du Règlement ETIAS). Le dossier de demande est automatiquement effacé du système central ETIAS à l'expiration de la période de conservation.

traitements prévus sont à grande échelle[5], ils ont un impact direct sur la liberté des personnes concernées de se rendre dans l'Union[6], ils impliquent des données pouvant se révéler sensibles et présentant un risque de discrimination[7], ils entraînent d'une manière ou d'une autre, une certaine surveillance continue des personnes concernées[8], ils conduisent au croisement de plusieurs systèmes d'information répondant à des finalités distinctes[9], et ils reposent sur des traitements automatisés de données (un *screening*) également basés sur le profilage[10].

II.1. ETIAS, SES FINALITÉS ET LES RÈGLES DE PROTECTION DES DONNÉES APPLICABLES

9. Le Règlement ETIAS crée un système européen d'information et d'autorisation concernant les voyages (ci-après, « **ETIAS** », pour « *European Travel Information and Authorisation System* »[11]). Lorsqu'il entrera en vigueur, les nationaux d'une soixantaine de pays tiers[12] ne devant pas disposer de visa pour entrer dans trente pays européens[13], devront obtenir une autorisation de voyage via ETIAS, accessible à partir d'un site Internet et d'une application mobile, et délivrée au terme d'un *screening* automatisé organisé par le Règlement et reposant en partie, sur les Etats membres.

[5] Voir les considérants nos 9-10.

[6] Voir notamment les considérants nos 9-13.

[7] Voir notamment le considérant n° 50.

[8] Voir les considérants nos 79-81.

[9] Notamment, au considérant n° 15 de son avis, le CEPD « *souhaite insister sur le fait que, bien qu'il existe des interactions entre la migration et la sécurité intérieure, il s'agit de deux domaines de l'ordre public différents dont les objectifs et les acteurs principaux sont distincts* ». Voir également les considérants nos 35 et s.

[10] Voir les considérants nos 35 et s.

[11] Voir https://travel-europe.europa.eu/etias/what-etias_en, dernièrement consulté le 27/06/2023.

[12] Voir https://travel-europe.europa.eu/etias/who-should-apply_en#who-needs-an-etias-travel-authorisation,

dernièrement consulté le 27/06/2023. L'article 2 du Règlement ETIAS définit les catégories de ressortissants de pays tiers auxquelles il s'applique et auxquelles il ne s'applique pas.

[13] Soit les 27 Etats Membres, la Suisse, le Lichtenstein et la Norvège,

voir https://travel-europe.europa.eu/etias/who-should-apply_en#ETIAS-countries, dernièrement consulté le 27/06/2023.

10. Le Règlement ETIAS[14] fixe dans le détail le cadre normatif de fonctionnement d'ETIAS (et du système d'information ETIAS[15]) de telle sorte qu'en la matière, la **marge de manœuvre de l'Etat belge est réduite**. Au niveau européen, ETIAS est développé et géré techniquement par l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (ci-après, « **eu-LISA** »)[16]. L'**unité centrale ETIAS** (soit une entité administrative) est quant à elle créée au sein de **l'Agence européenne de garde-frontières et de garde-côtes**[17]. Cette dernière Agence et eu-LISA se voient en outre attribuer par le Règlement ETIAS des responsabilités de responsable du traitement[18].

11. Dans le contexte du *screening* et des autorisations de voyage, les **unités nationales ETIAS** (ci-après, « **U.N.E.** »)[19] sont sollicitées dans certaines hypothèses, lorsque le *screening* automatisé nécessite un

[14] Confiant également à la Commission le pouvoir d'adopter des actes délégués et d'exécution. Peuvent être cités les textes suivants. Voir notamment :

Décision déléguée (UE) 2019/969 de la Commission du 22 février 2019 *relative à l'outil permettant aux demandeurs de donner ou de retirer leur consentement à la conservation de leur dossier de demande pour une période supplémentaire, en application de l'article 54, paragraphe 2, du règlement (UE) 2018/1240 du Parlement européen et du Conseil* ;

Décision d'exécution (UE) 2021/627 de la Commission du 15 avril 2021 *établissant des règles relatives à la tenue des registres et à l'accès à ceux-ci dans le système européen d'information et d'autorisation concernant les voyages (ETIAS) conformément au règlement (UE) 2018/1240 du Parlement européen et du Conseil* ;

Règlement délégué (UE) 2021/916 de la Commission du 12 mars 2021 *complétant le règlement (UE) 2018/1240 du Parlement européen et du Conseil portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) en ce qui concerne la liste préétablie de groupes d'emplois utilisée dans le formulaire de demande* ;

Décision d'exécution (UE) 2021/1028 de la Commission du 21 juin 2021 *portant adoption de mesures d'application du règlement (UE) 2018/1240 du Parlement européen et du Conseil en ce qui concerne la modification, l'effacement et l'effacement anticipé des données ainsi que l'accès à ces dernières dans le système central ETIAS* ;

Règlement d'exécution (UE) 2022/1380 de la Commission du 8 août 2022 *établissant les règles et conditions applicables aux interrogations de vérification lancées par les transporteurs, les dispositions relatives à la protection et à la sécurité des données pour le dispositif d'authentification des transporteurs, ainsi que les procédures de secours en cas d'impossibilité technique et abrogeant le règlement d'exécution (UE) 2021/1217* ;

Décision d'exécution (UE) 2022/102 de la Commission du 25 janvier 2022 *établissant des formulaires de refus, d'annulation ou de révocation d'une autorisation de voyage*, ci-après, la « **décision d'exécution 2022/102** » ;

Décision déléguée (UE) 2022/1612 de la Commission du 16 février 2022 *précisant le contenu et la forme de la liste préétablie d'options devant être utilisée aux fins d'une demande d'informations ou de documents supplémentaires conformément à l'article 27, paragraphe 3, du règlement (UE) 2018/1240 du Parlement européen et du Conseil* ;

Commission Delegated Decision of 10.12.2020 *supplementing Regulation (EU) 2018/1240 of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) as regards flagging* ;

Commission Delegated Decision of 23.11.2021 *on further defining security, illegal immigration or high epidemic risk*, C(2021) 4981 final ;

Commission Delegated Decision of 27.3.2023 *supplementing Regulation (EU) 2018/1240 of the European Parliament and of the Council, as regards specifying the conditions for the correspondence between the data present in a record, alert or file of the other EU information systems consulted and an ETIAS application file,* C(2023) 950 final ;

[15] Voir les articles 5 et 6 du Règlement ETIAS qui définissent ce qu'est ETIAS ainsi que l'architecture technique du système d'information ETIAS. Notamment, ETIAS comprend « *une interface uniforme nationale (**IUN**) dans chaque État membre, basée sur des spécifications techniques communes et identiques pour tous les États membres, qui permet au système central ETIAS de se connecter de manière sécurisée aux infrastructures frontalières nationales et aux points d'accès centraux des États membres visés à l'article 50, paragraphe 2* » (gras ajouté par l'Autorité) (article 6, 2., b), du Règlement ETIAS).

[16] Voir l'article 6 du Règlement ETIAS. Voir encore les responsabilités définies aux articles 73 et 74 du Règlement ETIAS.

[17] Voir l'article 7 du Règlement ETIAS. Voir encore les responsabilités définies à l'article 75 du Règlement ETIAS.

[18] Voir l'article 57 du Règlement ETIAS. Voir les considérants nos 102 et s.

[19] Article 8 du Règlement ETIAS.

traitement « manuel »[20]. Le Projet crée l'U.N.E belge **au sein du Centre de Crise National** (ci-après, « **CCN** »)[21].

12. ETIAS poursuit plusieurs objectifs[22] qui peuvent être regroupés, en simplifiant, sous trois grands groupes de finalités, dont les deux premiers retiendront l'essentiel des commentaires émis dans le présent avis.

II.1.1. Finalité prévention de risques

13. Tout d'abord, ETIAS à pour objectif de prévenir certains risques liés à l'entrée des personnes concernées sur le territoire européen : un risque en matière de **SÉCURITÉ**[23] ; un risque en matière **d'IMMIGRATION ILLÉGALE**[24] ; et un **RISQUE ÉPIDÉMIQUE ÉLEVÉ**[25]. Il s'agit d'une finalité de prévention de risques.

14. Le **RGPD** s'applique aux traitements par les **unités nationales ETIAS** « *qui **évaluent** les demandes* »[26] (gras ajouté et souligné par l'Autorité) d'autorisation de voyage des personnes concernées.

15. Cependant, « [l]*orsque le traitement de données à caractère personnel par les unités nationales ETIAS est effectué par les **autorités compétentes** qui **évaluent** les demandes aux fins de la **prévention** ou de la détection des **infractions terroristes ou d'autres infractions pénales graves**, ou des enquêtes en la matière, la **directive (UE) 2016/680** s'applique* »[27] (gras ajouté et souligné par l'Autorité).

16. « *Lorsque l'Unité nationale ETIAS **décide** de délivrer, de refuser, de révoquer ou d'annuler une autorisation de voyage* » (gras ajouté et souligné par l'Autorité), le **RGPD** s'applique[28].

---

[20] L'article 76 du Règlement ETIAS détermine des responsabilités incombant aux Etats membres.

[21] Article 4 du Projet.

[22] L'article 4 du Règlement ETIAS définit plus précisément les objectifs du Règlement.

[23] Défini à l'article 3, 1., 6., du Règlement ETIAS, comme « *un risque de menace pour l'ordre public, la sécurité intérieure ou les relations internationales de l'un des Etats membres* ».

[24] Défini à l'article 3, 1., 7., du Règlement ETIAS, comme « *le risque qu'un ressortissant de pays tiers ne remplisse as les conditions d'entrée et de séjour énoncées à l'article 6 du Règlement (UE) 2016/399* ».

[25] Défini à l'article 3, 1., 8., du Règlement ETIAS, comme « *toute maladie à potentiel épidémique au sens de la définition qu'en donne le règlement sanitaire internationale de l'Organisation mondiale de la santé (OMS) ou le Centre européen de prévention et de contrôle des maladies (ECDC), et d'autres maladies infectieuses ou parasitaires contagieuses, pour autant qu'elles fassent l'objet de dispositions de protection applicables aux ressortissants des Etats membres* ».

[26] Article 56, 2., al. 1er, du RGPD.

[27] Article 56, 2., al. 2, du RGPD.

[28] Article 56, 2., al. 3, du RGPD.

17. Et s'agissant de **l'autorité de contrôle**, le Règlement prévoit de manière générale que chaque Etat membre « *veille à ce que l'autorité de contrôle instituée conformément à l'article 51, paragraphe 1, du règlement (UE) 2016/679 contrôle en toute indépendance la licéité du traitement des données à caractère personnel effectué par l'État membre concerné en vertu du présent règlement, y compris de leur transmission à partir d'ETIAS et vers celui-ci* » (souligné par l'Autorité)[29]. Le Règlement ETIAS ne se réfère à l'autorité de contrôle visée à l'article 41 de la Directive 2016/680 que dans son article 65 (relatif à la communication des données à des pays tiers[30]) et concernant l'utilisation d'ETIAS à des fins répressives[31]. Autrement dit, **l'Autorité en conclut que l'Autorité de contrôle désignée en exécution du RGPD devrait également être compétente à l'égard de l'évaluation de risques, bien que cette évaluation soit soumise à la Directive 2016/680[32]**.

18. Le Projet alloue les compétences, dans la finalité de prévention des risques poursuivie par ETIAS, entre deux sections différentes de l'U.N.E. belge[33] :

    - La **section de l'Office des Etrangers** (ci-après, « **Section OE** »)[34], qui est compétente à l'égard des risques d'immigration illégale ;

    - Et la **section du Centre National de Crise** (ci-après, « **Section CCN** »)[35], qui est compétente pour les autres risques (à savoir, le risque de sécurité et le risque épidémique élevé)[36].

19. Compte-tenu de ce qui vient d'être précisé, l'article 31, § 2, du Projet peut prévoir l'application du titre 2 de la LTD à « *l'évaluation des risques sécuritaires* », **pour autant que l'Autorité de Protection des Données sera l'autorité de contrôle compétente dans ce contexte**, **sauf pour ce qui concerne la compétence du COC à l'égard des services de police**, dès lors que celui-ci a aussi été désigné comme autorité de contrôle en exécution du RGPD[37].

---

[29] Article 66, 1., du Règlement ETIAS.

[30] Voir à ce sujet, les considérants nos 116-117.

[31] Considérants nos 28 et s.

[32] Ce qui peut être mis en perspective avec la possibilité ouverte aux Etats membres, par l'article 41, 3., de la Directive 2016/680, de désigner une autorité de contrôle instituée au titre du RGPD, comme autorité de contrôle dans le cadre de cette directive.

[33] Il s'agit plus exactement du traitement des « *réponses positives* », voir les considérants nos 42-58 à ce sujet. Article 5, § 1er, du Projet.

[34] L'article 26 du Projet détermine sa composition.

[35] Les articles 6 à 10 du Projet détermine sa composition et son fonctionnement.

[36] Celle-ci comporte un officier de liaison de l'Office des Etranger, article 6, 3°, du Projet, qui est sous l'autorité du fonctionnaire dirigeant de la Section O.E. de l'U.N.E. Sa mission est définie à l'article 30 du Projet.

[37] L'article 4, § 2, al. 4, de la LCA, prévoit que :

« *A l'égard des services de police au sens de l'article 2,2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle de l'information policière visé à l'article 44/6, § 1er, de la loi du 5 août 1992 sur la fonction de police* ».

20. Il convient encore de souligner que s'inscrit dans la finalité de la prévention des risques, l'établissement de la **liste de surveillance ETIAS**[38]. Il s'agit d'une liste comportant des informations introduites par Europol ou par les Etats Membres[39], sur la base d'informations relatives à des **infractions terroristes ou à d'autres infractions pénales graves** – sont visées des personnes soupçonnées[40]. Cette liste sera l'objet d'un traitement automatisé dans le cadre du *screening* mis en place en vertu du Règlement ETIAS[41].

21. **A ce sujet, l'article 21 du Projet doit être adapté en ce qu'il se réfère aux finalités répressives d'ETIAS plutôt qu'à la finalité de prévention du risque de sécurité**. Si le Règlement ETIAS n'est pas limpide à ce propos[42], l'Autorité est d'avis que le demandeur pourrait considérer de manière générale que la contribution à la liste de surveillance ETIAS participe à l'évaluation des demandes au regard du risque de sécurité et partant, peut être soumise aux règles transposant la Directive 2016/680[43], étant entendu que comme cela vient d'être souligné, l'Autorité de Protection des Données est l'autorité de contrôle visée par le Règlement ETIAS, sauf pour les services de police. Autrement dit, **l'article 21 du Projet peut prévoir l'application du titre 2 de la LTD « *aux fins de la gestion de la liste de surveillance ETIAS* » pour autant que l'Autorité de Protection des Données soit l'autorité de contrôle compétente, sauf pour les services de police**.

22. Enfin, si l'Autorité n'est en principe pas compétente en droit positif belge pour se prononcer sur les règles qui régissent les traitements de données dont sont responsables les **services de renseignements et de sécurité**, force est de constater que le Projet entend intégrer ces services au dispositif du Règlement ETIAS, en leur attribuant une compétence de procéder à l'évaluation des demandes au regard du risque de sécurité. **Sans adaptation du droit belge, l'Autorité de Protection des Données serait compétente, sur la base de sa compétence résiduaire[44], à l'égard des membres détachés des services de renseignement et de sécurité dans le cadre de l'analyse de risques** à réaliser (en exécution des règles de protection des données du titre 2 de la LTD).

---

[38] Voir l'article 20, 4., du Règlement ETIAS.

[39] Article 34, 3., du Règlement ETIAS. Les articles 34, 3., et 35, du Règlement ETIAS déterminent les **responsabilités des Etats membres** (et d'Europol) en la matière.

[40] Voir l'article 34, 2., du Règlement ETIAS et la note de bas de page n° 52. L'article 34, 4., du Règlement ETIAS précise les données reprises dans la liste (le nom, les autres noms tels que les éventuels pseudonymes, l'adresse électronique, l'adresse IP, les prénoms, la nationalité, etc.).

[41] Voir le considérant nos 45 et s.

[42] L'article 56, 2., ne vise pas directement la contribution à la liste de surveillance.

[43] Voir l'article 31, § 2, du Projet, rendant applicable le titre 2 de la LTD.

[44] Voir l'article 4, § 2, al. 2, de la LCA.

23. **A ce sujet, l'Autorité doute que le Règlement ETIAS permette de soumettre une partie des traitements de données qu'il encadre à une autorité de contrôle qui ne serait pas désignée en exécution du RGPD ou en transposition de la Directive 2016/680**, soit une autorité ne relevant pas de la sphère d'application du droit européen. Le Projet entend permettre l'intervention des services de renseignements et de sécurité dans les matières relevant des autorités compétentes au sens du titre 2 de la LTD et de la Directive 2016/680 – soit une finalité *autre* que celle justifiant leur exclusion du droit européen en général[45]. Or l'article 42 du Projet qui insère un nouveau sous-titre 5*bis* intitulé « *De la protection des personnes physiques à l'égard de certains traitements de données à caractère personnel par la section du Centre de Crise National de l'Unité nationale ETIAS* » au titre 3 de la LTD, attribue une compétence au Comité permanent R visé à l'article 95 de la LTD, une autorité qui n'est pas désignée en droit belge en vertu des règles européennes de protection des données précitées.

24. Dans ces conditions, **l'Autorité semble pouvoir conclure qu'il découle juridiquement de ce qui précède** (notamment au sujet de l'autorité de contrôle désignée par le Règlement ETIAS[46]) **que l'Autorité de Protection des Données doit être désignée comme autorité de contrôle** en la matière (évaluation des risques, y compris la liste de surveillance ETIAS) – sans préjudice des commentaires ultérieurs concernant les finalités poursuivies par les services de renseignement et de sécurité[47]. Et ceci, **à moins que le législateur belge**, à la manière dont il a procédé pour les services de police, **ne désigne le Comité R comme autorité compétente belge en exécution du RGPD, pour les services de renseignements et de sécurité** (compétence relevant à ce jour, de l'Autorité de Protection des Données)**, lorsque leurs traitements de données relèvent du RGPD[48]**.

25. Les **règles auxquelles seraient soumis les services de renseignements et de sécurité dans ce domaine en vertu du Projet posent également question**. Selon l'article 184/2 en projet de la LTD (tel qu'introduit par l'article 42 du Projet), celui-ci s'applique « *au traitement de données à caractère personnel effectué par les détachés de la* [VSSE] *et du* [SGRS] *au sein de la section du Centre de Crise National de l'U.N.E.* » dans le cadre des finalités visées à l'article 14, § 1er, 3°, du Projet, à savoir la consultation d'ETIAS *à des fins répressives*. L'Autorité observe d'emblée que l'article 31, § 3, du Projet et l'article 184/2 de la LTD en Projet doivent être reformulés afin que soient également

[45] Le Projet entend même aller plus loin, de manière contestable, voir les considérants nos 95 et s.

[46] Voir le considérant n° 17.

[47] Voir les considérants nos 95-97.

[48] Pour rappel bien entendu, l'article 73 de la LTD dispose que : « *Le présent sous-titre s'applique à tout traitement de données à caractère personnel par les services de renseignement et de sécurité et leurs sous-traitants effectués dans le cadre des missions desdits services visés aux articles 7 et 11 de la loi du 30 novembre 1998 ainsi que par ou en vertu de lois particulières* ». En substance, dans l'exercice de leurs missions relevant de la sécurité nationale, les services de renseignements et de sécurité sont soumis à des règles de protection des données belges ne découlant pas du droit de l'Union européenne. Et dans ce cadre, le Comité R est l'autorité de contrôle compétente, conformément à l'article 95 de la LTD.

encadrées sans aucun doute les activités de traitement par les membres détachés des services de renseignements et de sécurité *lorsqu'ils réalisent des évaluations de risques* pour la Section CCN.

26. Mais plus fondamentalement, compte-tenu de ce qui vient d'être évoqué[49] et de l'article 66, 2., du Règlement ETIAS[50], l'Autorité est d'avis que **ce serait en principe le titre 2 de la LTD qui devrait s'appliquer *mutatis mutandis,* et non un autre titre prévoyant des règles *sui generis* réduites concernant le traitement des données à caractère personnel**. Il se dégage clairement du Règlement ETIAS que les traitements de données réalisés en exécution de celui-ci doivent soit être conformes au RGPD soit à la Directive 2016/680. S'agissant de l'évaluation du risque de sécurité, c'est cette dernière qui s'applique conformément à l'article 56, 2., al. 2, du Règlement ETIAS.

27. **En conclusion, les développements précédents peuvent être synthétisés comme suit, s'agissant des services de renseignements et de sécurité.** Si l'Etat belge entend étendre le dispositif européen ETIAS à ses services de renseignements et de sécurité lorsque ceux-ci agissent dans le cadre des finalités de ce dernier, il doit soumettre ceux-ci, à ces fins, aux règles européennes de protection des données applicables, dès lors que dans ce cas, ils agissent comme des autorités compétentes au sens de la Directive 2016/680. D'une part, dès lors que l'évaluation du risque (y compris la contribution à la liste de surveillance) est soumise à la Directive 2016/680 lorsqu'elle est effectuée par les autorités compétentes, l'activité des services de renseignement en la matière doit être soumise *mutatis mutandis* aux règles de droit belge transposant cette directive (titre 2 de la LTD). S'agissant de l'autorité de contrôle compétente, d'autre part, le Règlement ETIAS exigeant qu'il s'agisse de l'autorité désignée en exécution du RGPD, cela ne peut être, pour ces services, que l'Autorité de Protection des Données. A moins que le législateur belge, à la manière dont il a procédé pour les services de police, ne désigne le Comité R comme autorité compétente belge en exécution du RGPD pour les services de renseignements et de sécurité, lorsque leurs traitements de données relèvent du RGPD[51].

II.1.2. <u>Fins répressives</u>

28. Comme cela a été annoncé, ETIAS contribue à la prévention, à la détection et aux enquêtes concernant des infractions terroristes ou d'autres infractions pénales graves, soit les « **FINS RÉPRESSIVES** » d'ETIAS[52].

[49] Considérants nos 22-23.

[50] Voir le considérant n° 29.

[51] Voir la note de bas de page n° 48.

[52] Voir le Chapitre X du Règlement ETIAS (articles 50 et s.). Voir les considérants nos 84 et s.

29. Les traitements de données réalisés dans ce contexte sont soumis à la **directive 2016/680**[53]. Chaque Etat membre doit veiller à « *ce que les dispositions législatives, réglementaires et administratives nationales qu'il a adoptées en application de la directive (UE) 2016/680 s'appliquent aussi à l'accès à ETIAS par ses autorités nationales conformément au chapitre X du présent règlement, y compris pour ce qui est des droits des personnes dont les données sont ainsi consultées* » (souligné par l'Autorité)[54].

30. Et **l'Autorité de contrôle** désignée en vertu de l'article 41, 1., de la directive 2016/680 est compétente en la matière[55].

31. De nouveau, s'agissant du rôle que pourraient jouer en la matière les **services de renseignements et de sécurité**[56], comme cela vient d'être évoqué *mutatis mutandis*, ces services devraient, conformément au Règlement ETIAS, être soumis aux règles consacrées dans le titre 2 de la LTD. Il appartiendrait alors au Projet d'identifier comme autorité de contrôle, soit le COC, soit l'Autorité de Protection des Données. **Pour que le Comité R puisse être l'autorité de contrôle compétente en la matière, il faudrait que le législateur belge le désigne comme autorité compétente à l'égard des services de renseignements et de sécurité lorsqu'ils agissent en tant qu'autorité compétente au sens de la Directive 2016/680 et en exécution de l'article 41 de celle-ci[57]**. 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.

II.1.3. Autres finalités

32. ETIAS sera également utilisé par les entreprises de transport[58] et par les autorités compétentes aux frontières[59], ainsi que par les autorités chargées de l'immigration[60], afin de vérifier que les personnes concernées disposent bien de l'autorisation de voyage requise – **finalité de CONTRÔLE DE L'ACCÈS AU TERRITOIRE**.

33. Le traitement de données à caractère personnel réalisé à cette fin par ces autorités publiques est soumis au **RGPD**[61].

---

[53] Article 56, 3., du Règlement ETIAS.

[54] Article 66, 2., du Règlement ETIAS.

[55] Article 66, 3., du Règlement ETIAS.

[56] Voir le considérant n° 96.

[57] Voir également le considérant n° 27.

[58] Voir le Chapitre VII du Règlement ETIAS (articles 45 et s.).

[59] Voir le Chapitre VIII du Règlement ETIAS (articles 47 et s.).

[60] Voir le Chapitre IX du Règlement ETIAS (article 49).

[61] Article 56, 2., al. 1er, du Règlement ETIAS.

34. Enfin, ETIAS contribue aux objectifs de trois autres systèmes d'information européens – **finalité de SOUTIEN**. Premièrement, il soutient les **objectifs du Système d'information Schengen** (ci-après, le « **SIS** »)[62] concernant certains signalements de personnes concernées. Deuxièmement, il soutient les objectifs du système d'entrée/de sortie (soit l' « *Entry/Exit System* », ci-après, l' « **EES** »)[63] (notamment, un processus automatisé d'EES consulte ETIAS pour créer ou mettre à jour la fiche d'entrée/de sortie ou la fiche de refus d'entrée[64]). Il contribue troisièmement, en lien avec d'autres systèmes d'information, à l'identification correcte des personnes, en relation avec le répertoire commun de données d'identité (soit « *Common Identity Repository* », ci-après « **CIR** »)[65].

---

[62] Voir les Règlements européens suivants :

Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 *relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier* ;

Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 *sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) no 1987/2006* ;

Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 *sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) no 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission*.

Selon l'article 5, e), du Règlement ETIAS, les **signalements** suivants sont concernés : « *les objectifs du SIS relatifs aux signalements concernant des ressortissants de pays tiers faisant l'objet d'une non-admission et d'une interdiction de séjour, aux signalements concernant des personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition, aux signalements concernant des personnes disparues, aux signalements concernant des personnes recherchées pour prêter leur concours dans le cadre d'une procédure judiciaire, aux signalements concernant des personnes aux fins de contrôles discrets ou de contrôles spécifiques et aux signalements concernant des ressortissants de pays tiers faisant l'objet d'une décision de retour* ».

A propos de **SIS**, voir https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en, dernièrement consulté le 27/06/2023.

Voir **l'avis de l'Autorité n° 121/2022** du 1er juillet 2022 *concernant un avant-projet de loi relatif au fonctionnement et à l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, dans le domaine des vérifications aux frontières et aux fins du retour des ressortissants de pays tiers en séjour irrégulier (CO-A-2022-125)*.

Voir **CEPD, avis 7/2017** *sur la nouvelle base juridique du système d'information Schengen*, 2 mai 2017.

[63] Voir le Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 *portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) no 767/2008 et (UE) no 1077/2011*.

Voir **l'avis de l'Autorité n° 122/2022** du 1er juillet 2022 *concernant un avant-projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, en ce qui concerne le système d'entrée/de sortie (CO-A-2022-138)*.

[64] Article 11*ter* du Règlement ETIAS. Voir également l'article 11*quater* du Règlement ETIAS (révocation d'une autorisation de voyage par le demandeur).

[65] Il s'agit du répertoire établi à l'article 17, 1., du Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 *portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) no 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil* (ci-après, « le **Règlement interopérabilité** »).

Voir **CEPD, avis 4/2018** *sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE*, 16 avril 2018.

Selon l'article 17, 1., du Règlement interopérabilité :

« *Un répertoire commun de données d'identité (CIR), créant un dossier individuel pour chaque personne enregistrée dans l'EES, le VIS, ETIAS, Eurodac ou l' ECRIS-TCN contenant les données visées à l'article 18, est établi afin de faciliter l'identification correcte des personnes enregistrées dans l'EES, le VIS, ETIAS, Eurodac et l'ECRIS-TCN et d'aider à cette identification conformément à l'article 20, de soutenir le fonctionnement du MID conformément à l'article 21 et de faciliter et de rationaliser l'accès des autorités désignées et d'Europol à l'EES, au VIS, à ETIAS et à Eurodac, lorsque cela est nécessaire à des fins de prévention ou de détection d'infractions terroristes ou d'autres infractions pénales graves ou d'enquêtes en la matière conformément à l'article 22* » (souligné par l'Autorité).

II.2. SCREENING ET AUTORISATIONS DE VOYAGE

35. Le Règlement ETIAS met en place un processus de *screening* automatisé qui a pour but d'aboutir à la délivrance d'une autorisation de voyage ou à son refus.

36. Dans le cadre de son fonctionnement et afin de permettre des vérifications automatisées, le système d'information ETIAS est **interopérable avec cinq autres systèmes d'informations de l'UE**, à savoir : les systèmes **SIS** et **EES** déjà évoqués, le système d'information sur les visas (ci-après, « **VIS** »)[66], **Eurodac**[67] et le et le système européen d'information sur les casiers judiciaires pour les

---

Le **CIR** comporte une infrastructure centrale (développée et gérée par eu-LISA) qui remplace les systèmes centraux de l'EES, du VIS, d'ETIAS, d'Eurodac et de l'ECRIS-TCN, dans la mesure où elle stocke les données visées à l'article 18 du Règlement précité. L'article 18, précité, 1., prévoit ce qui suit :

« *1. Le CIR stocke les données suivantes, séparées logiquement en fonction du système d'information d'où elles proviennent:*

a) les données visées à l'article 16, paragraphe 1, points a) à d), à l'article 17, paragraphe 1, points a), b) et c), et à l'article 18, paragraphes 1 et 2, du règlement (UE) 2017/2226 [(soit le Règlement EES)] ;

b) les données visées à l'article 9, point 4) a) à c), et points 5) et 6), du règlement (CE) no 767/2008 [(soit le Règlement VIS)];

c) les données visées à l'article 17, paragraphe 2, points a) à e), du règlement (UE) 2018/1240 [(soit le Règlement ETIAS)] ».

L'article 6, 2. *bis*, du Règlement ETIAS, concernant l'architecture technique du système d'information ETIAS, dispose que « *Le CIR contient les données d'identité et les données du document de voyage. Les autres données sont stockées dans le système central* ».

Ces données sont les suivantes : le nom (nom de famille), le ou les prénoms (le ou les surnoms), le nom à la naissance; la date de naissance, le lieu de naissance, le sexe, la nationalité actuelle ; le pays de naissance, le ou les prénom(s) des parents du demandeur ; les autres noms (pseudonyme(s), nom(s) d'artiste, nom(s) d'usage), le cas échéant ; les autres nationalités, le cas échéant ; le type de document de voyage, le numéro et le pays de délivrance de ce document ; la date de délivrance du document de voyage et la date d'expiration de sa validité.

Le CIR contient en outre les **données du dossier individuel des ressortissants de pays tiers exemptés de l'obligation de visa** créé par l'autorité frontalière (le garde-frontière chargé, conformément au droit national, d'effectuer des vérifications aux frontières au sens de l'article 2, point 11), du règlement (UE) 2016/399) et visé à l'article 17 du Règlement EES, parmi lesquelles l'image faciale et les données dactyloscopiques de la main droite.

[66] Voir le Règlement (CE) no 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 *concernant le système d'information sur les visas (VIS) et l'échange d'informations entre les États membres sur les visas de court séjour, les visas de long séjour et les titres de séjour (règlement VIS)*.

Entre autres au sujet de **VIS**, « *The Visa Information System (VIS) allows Schengen States to exchange visa data. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area.*

The system helps avoid 'visa shopping', supports documenting and prevents irregular migration. It can perform biometric matching, primarily of fingerprints, for identification and verification purposes and assists the authorities protecting the internal security of Member States », voir https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Vis, dernièrement consulté le 27/06/2023.

[67] Voir le Règlement (UE) no 603/2013 du Parlement européen et du Conseil du 26 juin 2013 *relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) no 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) no 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice*.

Notamment, **Eurodac** « *is a large-scale IT system that helps with the management of European asylum applications since 2003, by storing and processing the digitalized fingerprints of asylum seekers and irregular migrants who have entered a European country. In this way, the system helps to identify new asylum applications against those already registered in the database* », https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac, dernièrement consulté le 27/06/2023.

ressortissants de pays tiers (soit, « *European Criminal Records Information System – Third Country Nationals* », ci-après, « **ECRIS-TCN** »)[68].

37. Le système ETIAS effectue également des vérifications automatisées en interrogeant **les données d'Europol**[69].

38. Le système central ETIAS consultera encore et enfin **deux bases de données d'Interpol**[70] : celle concernant les documents de voyage volés ou perdus (soit « *Stolen and Lost Travel Documents Database* », ci-après « **SLTD** »)[71] et celle portant sur les documents de voyage associés aux notices (soit « *Travel Documents Associated With Notices* », ci-après, « **TDAWN** »).

39. Le processus de *screening* automatisé fonctionne comme suit.

II.2.1. Formulaire complété par la personne concernée

40. Le demandeur, la personne concernée, doit **compléter un formulaire par voie électronique**, à propos d'une série de données à caractère personnel (nom, nom à la naissance, prénoms, nationalités, études, prénoms des parents, profession dans une liste préétablie, réponse à des questions concernant notamment les condamnations pénales à une série d'infractions terroristes ou listée en annexe, etc.[72] ; le système collecte en outre l'adresse IP utilisée par le demandeur).

---

[68] Voir le Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 *portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726*.

En ce qui concerne **ECRIS-TCN**, notamment, « *The European Criminal Records Information System (ECRIS), operational since April 2012, provides an electronic exchange of criminal record information on a decentralised basis between Member States. It allows Member State's criminal records authorities to obtain complete information on previous convictions of EU nationals from the Member State of that person's nationality. ECRIS-TCN, once set up, will be a centralised system that allows Member State's authorities to identify which other Member States hold criminal records on the third country nationals or stateless persons being checked, so that they can then use the existing ECRIS system to address requests for conviction information only to the identified Member States* », voir https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn, dernièrement consulté le 27/06/2023.

[69] Définies par l'article 3, 1., 17., du Règlement Etias comme « *les données à caractère personnel traitées par Europol aux fins visées à l'article 18, paragraphe 2, point a), du 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*. Cette disposition vise la finalité de traitement de données poursuivie par Europol consistant à réaliser des :

« *recoupements visant à établir des liens ou d'autres rapports pertinents entre des informations relatives:*

i) aux personnes qui sont soupçonnées d'avoir commis une infraction pénale ou d'avoir participé à une infraction pénale relevant de la compétence d'Europol, ou qui ont été condamnées pour une telle infraction;

ii) aux personnes pour lesquelles il existe des indices concrets ou de bonnes raisons de croire qu'elles commettront des infractions pénales relevant de la compétence d'Europol ».

[70] Voir l'article 12 du Règlement ETIAS.

[71] Voir https://www.interpol.int/How-we-work/Databases/SLTD-database-travel-and-identity-documents,

dernièrement consulté le 27/06/2023.

[72] Voir l'article 17 du Règlement ETIAS.

41. L'Autorité relève au passage dans ce cadre que l'exposé des motifs du Projet confirme **qu'ETIAS collecte des informations au sujet des personnes concernées qui *ne* sont *pas* exigées dans le cadre des demandes de visas**[73]. Ce qui, de manière générale, soulève une interrogation quant au principe d'égalité, découlant toutefois du Règlement ETIAS lui-même[74].

II.2.2. Traitements automatisés

42. Après une analyse de recevabilité[75], les données à caractère personnel communiquées sont ensuite l'objet des **traitements *automatisés* de vérification *par le système central* ETIAS** suivants, à la recherche de « ***réponses positives*** » (c'est-à-dire, des correspondances)[76], conformément aux articles 20 et 23 du Règlement ETIAS.

Traitements automatisés article 20 (général)

43. **Comparaison avec d'autres bases de données** – Le système central ETIAS lance une recherche de correspondances via le portail de recherche européen (soit « *European Search Portal* », ci-après, l'

[73] « *ETIAS collecte des données similaires à ce qui est actuellement d'application pour les visas. Les données suivantes sont cependant collectées uniquement dans le cadre d'une demande d'autorisation de voyage : les autres nationalités du demandeur, le pays de naissance et les prénoms des parents du demandeur, l'adresse électronique, le numéro de téléphone si disponible, les études, l'adresse du premier séjour si disponible, les données personnelles du citoyen de l'Union auxquels s'applique la directive 2004/38/CE ou d'un ressortissant de pays tiers jouissant d'un droit à la libre circulation équivalent à celui des citoyens de l'Union en vertu d'un accord entre l'Union et ses Etats membres, d'une part, et un pays tiers, d'autre part, auquel le demandeur est lié conformément à l'article 2 § 1 c) du règlement ETIAS, les données de l'intermédiaire qui complète la demande au profit du demandeur, les questions complémentaires listées à l'article 17 § 4 du règlement ETIAS ou encore l'adresse IP utilisée par le demandeur lors de sa requête* » (souligné par l'Autorité) (exposé des motifs du Projet, p. 2).

[74] Dans son avis (considérant n° 16), le « *CEDP se demande si la proposition ne crée pas un régime plus intrusif pour les voyageurs exemptés de l'obligation de visa que pour ceux soumis à l'obligation de visas dès lors que davantage de données seront centralisées au niveau de l'Union européenne dans l'ETIAS*[…] *que dans le VIS* ».

[75] Voir l'article 19 du Règlement ETIAS.

Remarque : le screening (traitements automatisés et le cas échéant, traitement manuel dont il sera question dans les développements suivants) est également réalisé si une autorisation de voyage est modifiée en réponse à une demande **d'exercice de ses droits** par le demandeur (personne concernée), conformément à l'article 64, 2., du Règlement ETIAS.

[76] L'article 3, 1., 14., du Règlement ETIAS, définit la réponse positive comme suit :

« *l'existence d'une correspondance établie en comparant les données à caractère personnel enregistrées dans un dossier de demande du système central ETIAS aux indicateurs de risques spécifiques visés à l'article 33 ou aux données à caractère personnel figurant dans un relevé, un dossier ou un signalement enregistré dans le système central ETIAS, dans un autre système d'information ou une autre base de données de l'Union européenne énumérés à l'article 20, paragraphe 2, (ci-après dénommés 'systèmes d'information de l'Union européenne'), dans les données d'Europol ou dans une base de données d'Interpol interrogés par le système central ETIAS* » (souligné par l'Autorité).

« **ESP** »)[77] avec les données des systèmes suivants : ETIAS lui-même, le SIS[78], l'EES, le VIS, Eurodac, l'ECRIS-TCN, les données d'Europol ainsi que les bases de données SLTD et TDAWN[79].

44. **Réponse affirmative à une question et absence d'adresse de domicile** – Le système central vérifie si le demandeur a répondu par l'affirmative à une ou plusieurs des questions posées dans le formulaire et si ce dernier a communiqué une ville et un pays de résidence à la place d'une adresse de domicile[80].

45. **Comparaison avec la liste de surveillance ETIAS** – Des données sont comparées avec la liste de surveillance ETIAS[81].

46. Les articles 21 à 25 du Projet régissent la liste de surveillance ETIAS qui peut être complétée par les **services de police**, la Sûreté de l'Etat (ci-après, « **VSSE** »), le Service Général du Renseignement et de la Sécurité des Forces armées (ci-après, « **SGRS** ») et l'Administration générale des douanes et accises (ci-après, « **AGD&A** »)[82].

47. S'agissant de **l'alimentation de la liste** de surveillance ETIAS, le Projet se limite à se référer aux conditions visées à l'article 34 du Règlement ETIAS et à la **faculté**[83], pour les autorités concernées, d'introduire des données. Dans ce contexte, l'Autorité a interrogé le demandeur quant aux circonstances (et aux règles), notamment compte-tenu du risque de discrimination, dans lesquelles les autorités concernées contribueront à la liste de surveillance ETIAS. Celui-ci a répondu ce qui suit :

> « *L'art 34,§1 stipule que les autorités concernées doivent avoir identifié des personnes soupçonnées d'avoir commis une infraction ou d'y avoir participé et/ou des personnes pour lesquelles il existe des raisons de croire qu'elles pourraient commettre une infraction sur la base de leurs propres informations. L'art 22 du Projet se réfère également à l'art 35,§1 du Règlement qui fixe les conditions à remplir avant d'introduire une donnée.*

---

[77] L'**ESP** est établi part l'article 6 du Règlement interopérabilité. Le 1. de cet article prévoit ce qui suit :

« *Un portail de recherche européen (ESP) est créé afin de faciliter l'accès rapide, continu, efficace, systématique et contrôlé des autorités des États membres et des agences de l'Union aux systèmes d'information de l'UE, aux données d'Europol et aux bases de données d'Interpol pour l'accomplissement de leurs tâches et conformément à leurs droits d'accès ainsi qu'aux objectifs et finalités de l'EES, du VIS, d'ETIAS, d'Eurodac, du SIS et de l'ECRIS-TCN* ». L'ESP comporte notamment une infrastructure centrale, comportant un portail de recherche permettant d'interroger simultanément l'EES, le VIS, ETIAS, Eurodac, le SIS, l'ECRIS-TCN ainsi que les données d'Europol et les bases de données d'Interpol. Il est développé par l'eu-LISA qui en assure également la gestion technique.

[78] Pour certains signalements : non-admission et interdiction de séjour ou arrestation (mandat d'arrêt ou extradition).

[79] Voir l'article 20, 2., du Règlement ETIAS. Voir également l'article 11 du Règlement ETIAS qui prévoit les vérifications automatisées entre systèmes interopérables.

[80] Article 20, 3., du Règlement ETIAS.

[81] Voir l'article 20, 4., du Règlement ETIAS et le considérant n° 19.

[82] Article 21 du Projet.

[83] L'article 21 du Projet précise clairement que les services concernés « *peuvent introduire des données dans la liste de surveillance ETIAS* ».

Un acte d'exécution EU est prévu pour donner un cadre assurant la journalisation et la sécurité des traitements liés à la liste de surveillance.

Le respect du principe de non-discrimination dans l'ensemble des traitements au sein du système d'information ETIAS (y compris la liste de surveillance) est prévu par l'article 14 du Règlement ETIAS.

Le Comité d'examen ETIAS (art 9 du Règlement) et le Comité d'orientation pour les droits fondamentaux (art 10 du Règlement) veillent au respect de ce principe, en particulier en ce qui concerne la mise en œuvre de la liste de surveillance (art 9,§2,b)) ».

48. L'Autorité prend acte de cette explication. Elle relève néanmoins que le Comité d'examen ETIAS est consulté par les Etats membres au sujet de la mise en œuvre de la liste de surveillance et qu'il émet des avis, des lignes directrices, des recommandations et bonnes pratiques en la matière (notamment)[84]. Le Règlement ETIAS fixe un seuil de suspicion à partir duquel une personne peut être signalée dans la liste de surveillance ETIAS mais ne détermine pas **les conditions dans lesquelles les autorités concernées *doivent* signaler une personne dans la liste de surveillance ETIAS**, **ce qui, de l'avis de l'Autorité, est nécessaire** au regard des principes de prévisibilité et de légalité consacré dans l'article 22 de la Constitution et 8 de la CEDH, et afin de diminuer le risque de discrimination des personnes concernées. Le dispositif du Projet doit par conséquent être adapté en conséquence.

49. **Comparaison à des indicateurs de risques spécifiques** – A l'aide d'un algorithme permettant un profilage (les **règles d'examen ETIAS**)[85], une série de données sont comparées à des indicateurs de risques spécifiques[86]. Dans ce contexte, *a priori*, **l'alimentation, par les Etats membres, de la Commission européenne en information afin d'établir des indicateurs de risques spécifiques,** visée à l'article 33, 2., du Règlement ETIAS, nécessitera à la base, du traitement de données à caractère personnel et in fine, aura un impact sur les traitements des données relatives aux personnes concernées par ETIAS.

[84] Article 9, 4., du Règlement ETIAS.

[85] Article 20, 5., du Règlement ETIAS.

[86] À propos de ces risques, voir le considérant n° 12, premier tiret (finalité de prévention des risques d'ETIAS). L'article 33 du Règlement ETIAS détermine ce que constituent les règles d'examen ETIAS et la manière dont elles doivent être établies. La Commission adoptera un acte délégué pour préciser les risques spécifiques concernés, sur la base notamment de statistiques et d'informations, attestées par des éléments factuels et concrets, fournies par les Etats membres. Sur la base des risques spécifiques, l'unité centrale ETIAS établira un ensemble d'indicateurs de risques spécifiques consistant en une combinaison des données visées à l'article 33, 4., du Règlement ETIAS.

50. La manière dont seront établis les indicateurs de risques est d'autant plus importante que comme le CEPD l'a souligné, malgré la disposition générale du Règlement ETIAS visant à lutter contre les discriminations notamment sur la base de certaines catégories particulières de données[87] et l'interdiction de fonder des indicateurs de risques spécifiques sur des catégories particulières de données[88] :

> « *Le CEPD souhaite souligner que, même si les indicateurs de risques ne seront pas directement définis sur la base des premiers critères susmentionnés, le résultat risque d'être très similaire à celui que l'on obtiendrait en utilisant ceux-ci. Sur la base d'informations telles que la nationalité et le lieu de résidence, surtout lorsqu'elles sont combinées à d'autres données, il est possible de se faire une idée relativement précise de la race ou de l'origine ethnique d'un demandeur. De même, les indicateurs de risques ne peuvent pas se fonder sur l'appartenance à un syndicat, mais pourraient être définis en fonction des informations relatives à la profession actuelle. Ces deux types d'informations sont très étroitement liés, raison pour laquelle un profilage sur cette base ne prévient pas réellement le risque de discrimination* »[89].

51. Sur ce point et dans un sens similaire, l'Autorité a déjà souligné que le traitement de la donnée nationale pouvait être considéré comme un traitement portant sur des catégories particulières de données visé à l'article 9 du RGPD[90].

52. L'Autorité a interrogé le demandeur quant aux règles encadrent ces traitements de données à caractère personnel. Celui-ci a répondu ce qui suit :

> « *Nous supposons que la question vise les informations que les Etats membres doivent fournir et qui sont visées à l'article 33,§2, points d), e) et f)*[91].
>
> *Ces informations doivent être fournies par les autorités compétentes pour chaque type de risques soit :*
> *pour le point d) Fedpol, Douanes, Services de renseignements et de sécurité ;*

---

[87] Voir l'article 14 du Règlement ETIAS

[88] L'article 33, 5., du Règlement ETIAS dispose que :

« *Les indicateurs de risques spécifiques sont ciblés et proportionnés. Ils ne sont en aucun cas fondés uniquement sur le sexe ou l'âge d'une personne. Ils ne sont en aucun cas fondés sur des informations révélant la couleur, la race, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, les opinions politiques ou toute autre opinion, la religion ou les convictions philosophiques, l'appartenance à un syndicat, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap ou l'orientation sexuelle d'une personne* ».

[89] Avis CEPD ETIAS, considérant n° 40.

[90] Voir l'avis n° 211/2022 du 9 septembre 2022 *concernant un projet d'arrêté royal portant modification de l'arrêté royal du 22 février 2017 portant création du Service public fédéral Stratégie et Appui (CO-A-2022-187)*.

[91] Ce qui est exact.

pour le point e) Office des étrangers ;
pour le point f) SPF Santé publique.

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 « loi de 2018 ») et éventuellement d'autres règles spécifiques de protection des données qui s'appliquent aux autorités concernées encadrent les traitements de données qui leur permettront de fournir ces informations.

L'article 31 du Projet prévoit l'application de la loi de 2018 dans le cadre de l'évaluation des risques ».

53. L'Autorité attire l'attention du demandeur sur le fait que n'est pas ici visée l'évaluation des risques (dans le cadre des demandes concrètes d'autorisation) mais bien la contribution à l'identification des risques à prévenir via les règles d'examen ETIAS, qui implique d'autres traitements de données qui doivent également être encadrés par le Projet. **Le dispositif de ce dernier doit ainsi déterminer les éléments essentiels de ces traitements de données, en particulier les (catégories de) données traitées ainsi que les autorités publiques responsables de ces traitements de données**.

Traitements automatisés article 23 (SIS particulier)

54. **Comparaison avec SIS pour une partie des signalements**[92] – Le système central ETIAS lance une recherche via l'ESP pour effectuer une comparaison avec certaines données de signalement figurant dans le SIS.

Absence de réponse positive

55. Au terme de ces traitements automatisés, **en l'absence de réponse positive**, l'autorisation de voyage est automatiquement délivrée[93].

II.2.3. <u>Réponse(s) positive(s) et traitement manuel</u>

[92] Personnes disparues, personnes recherchées pour concours à une procédure judiciaire ou signalement aux fins de contrôles discrets (etc.).

[93] Article 21, 1., du Règlement ETIAS.

56. S'il y a **une ou plusieurs réponses positives** aux traitements automatisés article 20 (général)[94, 95], l'unité centrale ETIAS procède à des **vérifications**[96]. En cas de faux positif, l'autorisation de voyage est délivrée automatiquement.

57. Si les vérifications sont positives ou s'il subsiste un doute quant à l'identité du demandeur, **la demande est alors traitée *manuellement* conformément à l'article 26 du Règlement ETIAS, par l'unité *nationale* ETIAS responsable**[97]. Il s'agit par exemple de l'Etat membre qui seul, a introduit ou fourni les données qui ont déclenché une réponse positive. Dans cette hypothèse, les unités nationales ETIAS ont également accès aux données d'autres systèmes d'informations de l'UE visées à l'article 25*bis* du Règlement ETIAS, et dans certaines circonstances, des informations ou documents supplémentaires peuvent être demandés au demandeur et, dans des conditions plus limitées encore, un entretien peut être organisé[98]. Enfin, notamment si plusieurs Etats membres ont communiqué des données ayant déclenché une réponse positive, un processus de consultation entre eux et l'unité nationale ETIAS de l'Etat membre responsable est organisée[99].

Evaluation des risques

58. Le traitement manuel réalisé par l'unité nationale ETIAS responsable[100] mène à une décision de refus ou d'autorisation de voyage prise par celle-ci, dans la plupart des cas[101] au terme d'une **évaluation de risques**[102] qu'elle a réalisé, voire encore, en cas de refus, lorsqu'une unité nationale ETIAS d'un

---

[94] Article 21, 2., et 22 du Règlement ETIAS.

[95] S'il y a une ou plusieurs réponses positives aux traitements automatisés **article 23 (SIS particulier)**, l'unité centrale ETIAS procède également à des vérifications et si la correspondance est confirmée, une notification est envoyée au bureau **SIRENE** (« *Supplementary Information Request at the National Entries* ») de l'Etat membre qui a introduit le signalement. Une telle notification est également envoyée si un traitement manuel a été enclenché à la suite des **traitements automatisés article 20 (général)**.

En ce qui concerne le bureau SIRENE, voir l'article 7 du Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 *sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) no 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission*. En Belgique il s'agit de « Commission SIRENE, Police Fédérale — Direction de la coopération policière internationale (CGI) », voir Document C2023/085/02, Liste des offices N.SIS et des bureaux SIRENE nationaux, *J.O.*, C, 85 du 7.3.2023, pp. 299-308, accessible à partir de https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation_fr,

dernièrement consulté le 28/06/2023, et l'article 5 de la loi du 2 mars 2023 *relative au fonctionnement et à l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, dans le domaine des vérifications aux frontières et aux fins du retour des ressortissants de pays tiers en séjour irrégulier*.

[96] Prévues à l'article 22 du Règlement ETIAS.

[97] L'article 25 du Règlement ETIAS identifie l'Etat membre responsable, selon les hypothèses.

Le commentaire des articles du Projet (p. 11), indique que « *toute donnée introduite dans une base de données européenne trouve son origine dans une base de données 'source', qui est en réalité une base de données nationale* ».

[98] Voir l'article 27 du Règlement ETIAS.

[99] Voir l'article 28 du Règlement ETIAS. Un processus similaire existe lorsque les données concernées proviennent d'Europol, voir l'article 29 du Règlement ETIAS.

[100] Article 26 du Règlement ETIAS.

[101] Pour les hypothèses où un refus doit être délivré sans évaluation de risque, voir l'article 26, 3., a), 3*bis*, a),

[102] Voir l'article 26, 3., b), 3*bis*, b), 4., 5. et 6., du Règlement ETIAS.

Etat membre consulté a rendu un avis négatif motivé (c'est alors cet autre Etat Membre qui a évalué les risques)[103]. La **décision** sur la demande doit être rendue dans un délai de principe particulièrement réduit : **96 heures** à compter de la recevabilité de la demande[104].

59. Selon le Projet, au sein de l'U.N.E. belge, un avis motivé sur l'évaluation des risques en matière de **SÉCURITÉ** et de **RISQUE ÉPIDÉMIQUE ÉLEVÉ** est réalisé par les « ***membres détachés*** »[105] des services concernés (services de police, le SPF Santé Publique, la VSSE, le SGRS et l'AGD&A)[106] relevant de la **Section du CCN**[107], qui a cette fin, ont « *accès aux bases de données nécessaires gérés par leurs services d'origine respectifs* » (souligné par l'Autorité)[108], et relèvent dans ce contexte, de l'autorité du fonctionnaire dirigeant[109]. Ce qui soulève les deux commentaires suivants.

60. Premièrement, l'Autorité a interrogé le demandeur afin que celui-ci confirme que les **évaluations des risques** réalisées par les membres détachés de la Section CCN sont bien réalisées par ceux-ci **sous l'autorité du fonctionnaire dirigeant** (s'agissant de l'exécution des missions de l'U.N.E.). Le demandeur l'a confirmé.

61. Deuxièmement, l'Autorité est d'avis qu'en se limitant à viser « *les bases de données nécessaires* », le Projet **ne répond pas aux principes de prévisibilité et de légalité** consacrés dans les articles 8 CEDH et 22 de la Constitution : il ne permet pas d'identifier les (catégories de) données qui originellement traitées par ces services, seront ultérieurement traitées aux finalités poursuivies par le Règlement ETIAS. Le dispositif du Projet **doit identifier les bases de données qui *doivent* être consultées en se référant à leur fondement légal et en précisant quelles (catégories de) données à caractère personnel issues de ces banques de données peuvent être réutilisées aux fins du Règlement ETIAS**. Cette adaptation permettra également **d'identifier dans le cadre de quelles missions de ces autres autorités, les données collectées (et quelles données) peuvent être réutilisées aux fins d'ETIAS**. A défaut de précision en la matière, il est également impossible pour l'Autorité de contrôler l'application de l'article 6, 4., du RGPD et de l'article 4, 1. et 2., de la Directive 2016/680.

---

[103] Voir l'article 28 du Règlement ETIAS.

[104] Voir l'article 32 du Règlement ETIAS.

[105] Définis à l'article 6, 2°, du Projet.

[106] De ces autorités, le SPF Santé Publique (soumis au RGPD) et l'AGD&A (bien que soumise au titre 2 de la LTD dans certaines conditions – voir notamment, le *Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données, Convention entre l'Autorité de Protection des données, l'Organe de Contrôle de l'Information Policière, le Comité Permanent de contrôle des services de renseignement et le Comité Permanent de contrôle des services de police*, 24 novembre 2020, p. 10, disponible sur https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-controle-federales-belges-en-matiere-de-protection-des-donnees.pdf, dernièrement consulté le 05/07/2023) **relèvent de la compétence de contrôle de l'Autorité de Protection des Données**.

[107] Article 11, § 1er, du Projet.

[108] Article 12, § 1er, du Projet. Le paragraphe 2 de cette disposition prévoit également un accès au casier judiciaire central en cas de réponse positive en lien avec ECRIS-TCN.

[109] Article 8, § 2, du Projet.

62. Il se dégage de la logique du Projet que la **Section OE** est compétente pour évaluer et se prononcer en cas de risque **d'IMMIGRATION ILLÉGALE**[110]. L'article 27 du Projet ne l'exprime toutefois pas directement et devrait être formulé plus clairement, à la manière des dispositions applicables à la Section du CCN.

63. Dans ce contexte en outre, le Projet n'identifie pas **sur la base de quelles informations ((catégories de) données) et systèmes d'information belges** la Section OE va réaliser son analyse. L'Autorité a interrogé le demandeur à ce sujet et celui-ci a répondu ce qui suit :

> « *L'OE n'a pas jugé utile de prévoir cela pour leur section. Nous savons qu'ils utiliseront au moins leur base de données Evibel* »[111].

64. La position développée au considérant n° 61 vaut en l'occurrence également : le dispositif du Projet doit identifier les **banques de données (et leur fondement légal) et (catégories de) données qui *doivent* être réutilisées aux fins du Règlement** ETIAS par l'O.E. A défaut de précision en la matière, il est également de nouveau impossible pour l'Autorité de contrôler l'application de l'article 6, 4., du RGPD[112].

Décision de l'U.N.E.

65. S'il n'existe aucun indice concret ni aucun motif raisonnable fondé sur des indices concrets permettant de conclure que la présence de la personne sur le territoire des Etats membres présente un risque en matière de sécurité ou d'immigration illégale ou un risque épidémique élevé, **une autorisation de voyage (valable 3 ans) est délivrée**[113].

66. En **cas de doute**, l'unité nationale ETIAS a la possibilité de délivrer l'autorisation moyennant la mise en œuvre d'une **vérification de deuxième ligne**[114]. L'Autorité a interrogé le demandeur quant aux circonstances (les règles) dans lesquelles cette vérification de deuxième ligne peut être exigée. Celui-

---

[110] Voir l'article 27 du Projet.

[111] « Evibel » apparaît être la base de données de l'OE dans laquelle se trouve les données relatives à l'asile, la migration et aux procédures de retour, voir European Migration Network Belgium, « *Accurate, timely, interoperable : data management in the asylum procedure* », disponible sur https://emnbelgium.be/sites/default/files/publications/Standalone%20FINAL_1.pdf, dernièrement consulté le 06/07/2023, p. 15.

[112] Ou de l'article 4, 1. et 2., de la Directive 2016/680, voir le considérant n° 87.

[113] Article 36, 1., du Règlement ETIAS.

[114] Article 36, 2., du Règlement ETIAS. Cette vérification est définie comme (article 3, 1., 3., du Règlement ETIAS) « *une vérification de deuxième ligne au sens de l'article 2, point 13), du règlement (UE) 2016/399* », soit « *une vérification supplémentaire pouvant être effectuée en un lieu spécial à l'écart de celui où toutes les personnes sont soumises à des vérifications (première ligne)* », s'agissant de vérifications aux frontières. Une telle mention peut aussi être demandée par un Etat membre consulté. Conformément à l'article 36, 3., du Règlement ETIAS, une mention peut aussi être insérée dans le système selon laquelle une réponse positive spécifique a été déclenchée pendant le traitement de la demande.

ci a notamment rappelé que cette possibilité était encadrée par un acte délégué de la Commission européenne (non encore publié toutefois mais accessible en ligne[115]).

67. C'est « ***la section*** » compétente de l'U.N.E., qui « *prend ses décisions* »[116], étant entendu que le « *fonctionnaire dirigeant* » de la Section est responsable « *de la bonne exécution des missions de l'U.N.E. qui incombent à sa section* »[117]. Si des réponses positives pour une même demande, doivent être évaluées par les deux Sections, la Section du CCN prend la décision et doit suivre l'avis négatif de la Section OE[118]. L'Autorité a interrogé le demandeur afin que celui-ci confirme cette analyse (décision prise par le fonctionnaire dirigeant) et le demandeur a répondu ce qui suit :

> « *Oui. Un arrêté royal d'exécution est prévu qui précise que le fonctionnaire dirigeant désigne les membres de sa section habilités à prendre les décisions. Ce ne seront pas les détachés des services compétents qui eux évaluent les risques mais des collaborateurs opérationnels (attachés NCCN)* » (souligné par l'Autorité)[119].

68. L'Autorité prend acte de cette explication mais **est d'avis que le dispositif du Projet lui-même doit spécifier que le fonctionnaire dirigeant prend les décisions, dès lors que cela a un impact direct** (notamment) **sur la détermination des rôles et responsabilités au regard du traitement de données à caractère personnel** et des éventuelles incompatibilités dans l'exercice des fonctions concernées[120].

69. L'article 37 du Règlement ETIAS liste les hypothèses où sont **refusées** les autorisations de voyage. Les décisions prises par les Section de l'U.N.E. doivent être **motivées**[121].

70. **Exceptionnellement**, lorsque le traitement manuel n'est pas encore achevé ou lorsqu'une autorisation de voyage a été refusée, annulée ou révoquée, l'Etat membre de destination du

---

[115] Voir la note de bas de page n° 15, huitième référence.

[116] Articles 11, § 3, et 29 du Projet.

[117] Article 7, 1°, du Projet, et article 26, § 2, du Projet.

[118] Article 29 du Projet.

[119] En outre, le commentaire des articles du Projet (p. 11), précise, au sujet du processus d'évaluation de risque que ce « *processus implique que ce ne sont pas les membres détachés qui prennent la décision finale mais les collaborateurs opérationnels habilités par le fonctionnaire dirigeant* ».

[120] Voir les considérants nos 102.

[121] Voir les articles 28, 3., et 39, 4., du Règlement ETIAS. De manière générale, les motifs de la décision sont en principe toujours renseignés dans le dossier de demande. En vertu de l'article 26, 7., du Règlement ETIAS : « *Les résultats de l'évaluation du risque en matière de sécurité ou d'immigration illégale ou du risque épidémique élevé et les motifs sous-tendant la décision de délivrer ou de refuser une autorisation de voyage sont enregistrés dans le dossier de demande par l'agent ayant réalisé l'évaluation des risques* ». Voir également l'article 39, 3., d), et les articles 40, 4. (annulation), 41, 6. (révocation) et 43 (décision d'annuler ou révoquer), 2., du Règlement ETIAS.

Voir également les annexes de la Décision d'exécution (UE) 2022/102 de la Commission du 25 janvier 2022 *établissant des formulaires de refus, d'annulation ou de révocation d'une autorisation de voyage*, prévoyant des formulaires de notification de décisions reprenant, outre l'identification du motif de la décision (disposition concernée du Règlement ETIAS), un cadre intitulé « *Exposé des faits pertinents et motivation supplémentaire sous-jacente à la décision* ».

demandeur peut délivrer une autorisation de voyage à **validité territoriale limitée** pour des motifs humanitaires, pour des raisons d'intérêt national ou en vertu d'obligations internationales, conformément à l'article 44 du Règlement ETIAS.

Procédure de recours

71. Un **recours** est ouvert au demandeur contre un refus d'autorisation de voyage, processus organisé en droit belge dans le cadre du **Projet modificatif**[122]. Ce dernier précise que les décisions prises par l'U.N.E. sont susceptibles de **recours *en annulation* devant le Conseil du contentieux des étrangers, visé à l'article 39/1 de la loi du 15 décembre 1980**[123]. Le recours en annulation est consacré aux articles 39/78 et s., de la loi du 15 décembre 1980 *sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers* (ci-après, « **la loi de 1980** »). L'article 39/2 de la loi de 1980 établit une distinction entre le recours de pleine juridiction introduit contre les décisions du Commissaire général aux réfugiés et aux apatrides et le recours en annulation, pour violation des formes soit substantielles, soit prescrites à peine de nullité, excès ou détournement de pouvoir[124]. **L'exposé des motifs n'explique pas ce choix d'un recours en annulation plutôt qu'un recours en pleine juridiction**.

72. **Or l'Autorité est d'avis qu'*a priori*, un recours en pleine juridiction est de nature à mieux garantir les droits et libertés des personnes concernées**. Par conséquent, l'exposé des motifs doit motiver la raison pour laquelle il est recouru à un recours en annulation plutôt qu'un recours en pleine juridiction.

---

[122] Article 37, 3., du Règlement ETIAS.

[123] Voir également le considérant n° 78, concernant le recours à l'égard d'une décision prise par l'U.N.E. sur une demande de rectification ou de suppression des données.

[124] Selon cette disposition :

« *§ 1er. Le Conseil statue, par voie d'arrêts, sur les recours introduits à l'encontre des décisions du Commissaire général aux réfugiés et aux apatrides.*

Le Conseil peut :

1° confirmer ou réformer la décision attaquée du Commissaire général aux réfugiés et aux apatrides;

2° annuler la décision attaquée du Commissaire général aux réfugiés et aux apatrides soit pour la raison que la décision attaquée est entachée d'une irrégularité substantielle qui ne saurait être réparée par le Conseil, soit parce qu'il manque des éléments essentiels qui impliquent que le Conseil ne peut conclure à la confirmation ou à la réformation visée au 1° sans qu'il soit procédé à des mesures d'instruction complémentaires;

3° sans préjudice du 1° ou du 2°, annuler la décision attaquée du Commissaire général aux réfugiés et aux apatrides d'irrecevabilité de la demande de protection internationale visée à l'article 57/6 § 3, pour le motif qu'il existe des indications sérieuses que le requérant peut prétendre à la reconnaissance de la qualité de réfugié au sens de l'article 48/3 ou à l'octroi de la protection subsidiaire au sens de l'article 48/4.

§ 2. Le Conseil statue en annulation, par voie d'arrêts, sur les autres recours pour violation des formes soit substantielles, soit prescrites à peine de nullité, excès ou détournement de pouvoir ».

Pour ce qui concerne les dispositions spécifiques applicables aux recours de pleine juridiction contre les décisions du Commissaire précité, voir les articles 39/69 et s. de la loi de 1980. Les articles 39/78 et s. concernent le recours en annulation.

73. En outre, il découle du dispositif ETIAS[125] que lorsque l'U.N.E. d'un Etat membre refuse une autorisation de voyage en raison d'un **avis négatif émis par l'autorité d'un autre Etat membre** émis à l'occasion d'une consultation par la première U.N.E.[126], la personne concernée dispose d'un recours contre l'avis négatif rendu par l'U.N.E. de cet autre Etat Membre, conformément au droit de cet autre Etat Membre. Or le Projet modificatif se réfère de manière générale aux « *décisions* » de l'U.N.E., tandis que le Règlement ETIAS se réfère à refuser/délivrer (*décision* sur la demande) et rendre un avis dans le cadre des consultations entre Etats Membres. **L'Autorité est d'avis que le Projet modificatif doit clarifier que *l'avis* négatif émis par une Section de l'U.N.E. dans le cadre des consultations visées à l'article 28 du Règlement ETIAS constitue une décision susceptible de recours**.

74. Pendant la procédure de recours, « *le requérant a **accès aux informations** figurant dans le dossier de demande **conformément aux règles en matière de protection des données** visées à l'article 56 du présent règlement* » (gras ajouté par l'Autorité)[127]. Dans ce contexte, l'Autorité a invité le demandeur à confirmer que les **évaluations des risques** réalisées par les membres détachés de la Section CCN seront bien communiquées à la Section CCN (au fonctionnaire dirigeant) afin que celle-ci prenne sa décision (plus que le simple *résultat* de l'évaluation), de telle sorte que la personne concernée disposera d'un droit d'accès à l'égard de cette évaluation (ce document), en vertu des règles de protection des données. Le demandeur a répondu dans un deuxième temps[128] ce qui suit :

> « *Je vous confirme que la personne concernée pourra bien avoir accès au raisonnement justifiant le résultat de l'évaluation, lequel servira également à motiver la décision qui sera prise par l'UNE et qui lui sera notifiée. Cela ressort, selon nous, de l'article 26, §7, al 2 du Règlement (qui vise le résultat de l'évaluation et les motifs sous-tendant la décision) ainsi que de l'article 11,§1 du Projet (qui mentionne un 'avis motivé').*

[125] Voir le formulaire repris à l'annexe I de la **décision d'exécution 2022/102**.

Dans cette logique, ne sont pas accessibles à la personne concernée, dans le dossier de demande, l'avis émis par un Etat membre consulté (voir l'article 28, 3., al. 3, du Règlement ETIAS) ainsi que le motif y lié de la décision (article 39, 4., du Règlement ETIAS), ou notamment la mention relative à un contrôle de deuxième ligne (lorsqu'elle est demandée par un Etat membre consulté ; voir l'article 36, 2., al. 2, du Règlement ETIAS ; à noter que cette mention est effacée automatiquement une fois que les autorités frontalières ont procédé à la vérification) (article 36, 2., al. 3, du Règlement ETIAS).

[126] Voir l'article 28 du Règlement ETIAS qui régit les hypothèses de consultations d'autres Etats Membres.

[127] Article 37, 3., du Règlement ETIAS.

[128] Pour être complet, avant d'être réinterrogé sur le sujet, le demandeur avait répondu ce qui suit à l'Autorité :

« *Nous confirmons que les résultats de l'évaluation du risque seront enregistrés dans le dossier du demandeur mais pas sous la forme d'un « document », en vertu de l'art 26, §7, al 2, du Règlement. Pour y accéder, il faudra consulter le software ETIAS. Cet avis motivé servira de base à la décision. En cas de recours, il devrait être disponible dans le dossier administratif (nous ne pouvons le garantir à ce stade car nous ne sommes pas responsables du software ETIAS mais nous avons fait cette demande en vue d'assurer le contrôle de légalité des décisions ETIAS). La personne concernée pourra également y avoir accès, comme prévu par l'article 64 du Règlement* ».

Pour être exhaustive, je vous signale qu'il se peut que cet accès soit limité si l'évaluation du risque en cause relève de la Directive 2016/680, soit des titres 2 ou 3 de la loi de 2018[129] *- nouveau sous-titre 5bis inséré par l'article 41 du Projet* ».

75. L'Autorité prend acte de cette explication. **Elle est toutefois d'avis qu'en tout état de cause, la personne concernée doit pouvoir disposer de l'évaluation de risques produite et communiquée au fonctionnaire dirigeant (ou à ses collaborateurs opérationnels[130]) en vue de prendre sa décision**. Ce qui n'exclut pas que les traitements de données (et les données traitées dans ce contexte) réalisés afin de rédiger l'évaluation par les autorités compétentes soumises à la Directive 2016/680 puissent eux-mêmes être soumis à des règles limitatives des droits de la personne concernée en exécution de la Directive 2016/680. La Section (le fonctionnaire dirigeant) qui prend une décision dans le cadre d'ETIAS est soumise au RGPD et **l'évaluation de risques** au-delà de son simple résultat (à savoir, présente ou pas un risque spécifique) **constitue l'élément déterminant qui motive sa prise de décision et est nécessaire à la personne concernée tant pour vérifier que les données à caractère personnel traitées à son sujet le sont licitement**, **qu'en vue de l'éventuel exercice de son droit de recours** contre la décision de l'U.N.E. En l'état du Projet, l'Autorité est d'avis que c'est aux membres détachés qu'incombe la responsabilité d'être attentifs dans la production de leur analyse de risques : l'interaction directe de leur activité d'analyse avec les droits et libertés des personnes concernées nécessite que la personne concernée puisse accéder à cette analyse[131]. Cela étant précisé, corrélativement, dans le cadre d'un **contrôle interne**, lorsque cela est nécessaire pour **vérifier l'exactitude d'une donnée à caractère personnel de l'analyse** qui lui est communiquée (par exemple, une imputation à l'égard de la personne concernée), le Projet devrait également permettre au fonctionnaire dirigeant (responsable de la décision à prendre et autorité hiérarchique des membres détachés) de consulter la donnée à caractère personnel de base, dans la base de donnée concernée, *conformément aux règles (y compris de protection des données) régissant cette base de données*. Remarque : cette possibilité ne peut être détournée en vue de vider les analyses de risques de leur substance, en particulier au motif qu'elles seraient accessibles aux personnes concernées.

76. Toujours à propos de l'évaluation des risques dont il vient d'être question, l'Autorité relève que le Projet doit également établir clairement que celle-ci, émanant des membres détachés mais réalisée sous l'autorité du fonctionnaire dirigeant de la Section, **n'est pas soumise aux exceptions générales aux droits des personnes concernées consacrées dans les articles 11 et 14 de la LTD**

---

[129] Sur l'accès indirect via les autorités de contrôles, voir les conclusions de l'Avocate générale L. Medina présentées le 15 juin 2023 dans l'Aff. C-333/22, *Ligue des droits humains ASBL, BA c/ L'organe de contrôle de l'information policière*.

[130] Voir la note de bas de page n° 119.

[131] Et ce d'autant plus que le Règlement ETIAS lie le droit d'accès au dossier dans le cadre d'un recours à l'accès aux données sous l'angle de la protection des données. En tout état de cause, l'Autorité ne percevrait pas pour quelle raison l'analyse pourrait être consultée dans le cadre d'un recours mais pas dans le cadre d'un accès sur le plan de la protection des données.

(inapplicabilité de droits à l'égard de données reçues notamment des services de police et des services de renseignements et de sécurité).

77. Enfin, dans le contexte de **l'exercice de ses droits par le demandeur**, le Règlement ETIAS prévoit que l'unité nationale ETIAS (ou l'unité centrale ETIAS) qui ne partage pas la position du demandeur quant à la rectification ou suppression de ses données « *adopte sans retard une décision administrative expliquant par écrit à la personne concernée pourquoi elle n'est pas disposée à rectifier ou à effacer les données la concernant* », décision devant indiquer la voie de recours disponible[132].

78. Il est par conséquent question d'une **hypothèse additionnelle de « *décision* » de l'U.N.E.** qui, en l'état du Projet modificatif, pourra faire l'objet d'un recours devant le Conseil du contentieux des étrangers. L'article 55, 8., du Règlement ETIAS prévoit d'ailleurs que sans « *préjudice de tout recours administratif ou extrajudiciaire à leur disposition, les personnes concernées* ***disposent d'un droit de recours juridictionnel effectif pour garantir que les données conservées dans ETIAS sont modifiées ou effacées*** » (gras ajouté par l'Autorité). Ceci est sans préjudice de la possibilité qui est offerte à la personne concernée, conformément aux règles de protection des données, d'introduire une plainte auprès de l'autorité de contrôle compétente. **L'Autorité est d'avis dans ce contexte, qu'afin de garantir au mieux l'effectivité des règles de protection des données, c'est un recours *de pleine juridiction* qui doit être mis en place,** de manière telle que le Conseil du contentieux des étrangers (une juridiction administrative) puisse substituer son analyse à celle de l'U.N.E.

Possibilités d'annulation ou de révocation

79. Lorsqu'un Etat membre est en mesure de prouver que les conditions de délivrance d'une autorisation de voyage n'étaient pas remplies au moment de la délivrance ou ne le sont plus, l'unité nationale concernée *doit* respectivement annuler (annulation) ou révoquer (révocation) l'autorisation de voyage[133].

80. Outre **l'interaction automatique avec le SIS ainsi que l'interaction avec la liste de surveillance ETIAS** (traitements automatisés additionnels) qui sont directement encadrées par le Règlement ETIAS[134], l'Autorité a interrogé le demandeur quant aux **circonstances** dans lesquelles (et aux règles selon lesquelles) l'U.N.E. serait susceptible de devoir se prononcer au sujet d'une annulation ou d'une révocation. Le demandeur a répondu ce qui suit :

[132] Article 64, 3. et 4., du Règlement ETIAS.

[133] Voir les articles 40 et 41 du Règlement ETIAS.

[134] Visées à l'article visée l'article 41, 3. et 4. du Règlement ETIAS.

> « *Nous considérons que toute autorité belge impliquée directement ou indirectement dans le processus d'examen des demandes pourrait avoir connaissance d'une nouvelle information ou d'une information qui n'aurait pas été prise en compte au moment de la prise de décision, qui serait de nature à entraîner une annulation ou une révocation de l'autorisation de voyage. Il semble aller de soi que cette information doit être communiquée à l'UNE. Les dispositions exigent des preuves, ce qui suppose des éléments tangibles et vérifiables. Ceux-ci doivent être mis en parallèle avec les motifs pouvant être utilisés pour annuler ou révoquer l'autorisation de voyage (art 37, §1 et 2 du Règlement).*
>
> *Nous avons renoncé à introduire une disposition à ce sujet dans le Projet car nous ne sommes pas parvenus à la formuler de manière à lui donner une valeur ajoutée par rapport aux dispositions du Règlement* » (souligner par l'Autorité).

81. D'une manière ou d'une autre, cette approche implique par conséquent un suivi (avec quelle périodicité ?)[135] des personnes concernées auxquelles une autorisation de voyage a été délivrée, et **une responsabilité/une obligation** (également au regard du traitement de données[136]) des autorités qui sont impliquées dans le processus d'examen des demandes. Celles-ci ont l'obligation de communiquer à l'U.N.E., potentiellement *même en dehors d'un processus d'évaluation d'une demande d'autorisation*[137] (si telle est bien l'intention du demandeur), les informations pertinentes dont elles prendraient connaissance à l'occasion de l'exercice de leurs missions (à identifier). **L'Autorité est d'avis qu'une telle obligation, mettant en place un traitement de données à caractère personnel, doit être organisée par le dispositif du Projet** devant fixer les éléments essentiels des traitements de données envisagés.

II.2.4. Mise à jour et exactitude des données

82. **Obligation de mise à jour et de veiller à l'exactitude des données**. L'unité centrale ETIAS et les unités nationales ont l'obligation de mettre à jour les données et de veiller à leur exactitude[138]. Dans ce contexte, l'Autorité a interrogé le demandeur quant aux mesures d'exécution prises en exécution de l'article 55, 1., du Règlement ETIAS afin d'assurer que les données sont mises à jour.

---

[135] L'autorité concernée doit pouvoir lier, dans l'exercice de ses missions et selon le suivi escompté, les données dont elle dispose au sujet du personne concernée au fait que celle-ci est ou pas titulaire d'une autorisation de voyage couverte par le Règlement ETIAS.

[136] Voir les considérants nos 102 et s.

[137] Ainsi, la mise à jour pourrait n'être effectuée que lorsqu'à l'occasion d'une demande d'autorisation, sont identifiées des données également pertinentes pour une autre demande d'autorisation. Pour une hypothèse de ce type, dans un autre contexte de *screening*, voir l'Avis de l'Autorité n° 245/2022 du 21 octobre 2022 *concernant un avant-projet de loi relative à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Evaluation de l'Intégrité pour les Pouvoirs publics (CO-A-2022-248)*, considérants nos 51 et s. et considérant n° 56 en particulier.

[138] Voir l'article 55, 1. à 4., du Règlement ETIAS.

Etant entendu que pour ce qui concerne la liste de surveillance ETIAS, l'article 35 du Règlement ETIAS consacre lui-même une obligation périodique. Le demandeur a répondu ce qui suit :

> « *L'art 55,§1 vise uniquement les données que l'UCE ou l'UNE ont elles-mêmes enregistrées sur la base des dispositions du Règlement (ex : art 39 qui prévoit les données à ajouter après la prise de décision – ces données devront être modifiées en cas d'annulation ou de révocation subséquente en vertu des art 40 et 41). Nous considérons que l'obligation de mise à jour est explicitée dans les autres § de l'article 55. Il faut en effet un déclencheur qui peut provenir d'une demande d'accès aux données personnelles, de la communication d'une nouvelle information par une autorité impliquée,..* ».

83. L'Autorité prend acte de cette explication qui est à lier aux développements concernant l'annulation et la révocation des autorisations[139].

II.3. UTILISATION D'ETIAS À DES FINS RÉPRESSIVES

84. Comme évoqué précédemment, ETIAS peut être consulté par les autorités désignées par les Etats membres à des fins répressives.

II.3.1. Autorités concernées

85. Dans ce cadre, les Etats membres doivent désigner les **autorités habilitées (les autorités désignées)** à demander la consultation des données d'ETIAS[140], et lister les **unités opérationnelles** qui seules[141], au sein de ces autorités[142], sont autorisées à demander la consultation d'ETIAS. Ils doivent encore désigner un **point d'accès central** qui a accès au système ETIAS et qui vérifie que les conditions d'accès à ETIAS établies à l'article 52 sont remplies[143]. Le Règlement ETIAS prévoit en outre l'indépendance du point d'accès central par rapport aux autorités désignées[144]. L'article 52 du Règlement ETIAS détermine les conditions cumulatives dans lesquelles les données peuvent être consultées[145].

---

[139] Voir les considérants nos 79-81.

[140] Article 50, 1., du Règlement ETIAS

[141] C'est en effet l'unité opérationnelle qui doit présenter la demande motivée de consultation d'ETIAS, voir l'article 51 du Règlement ETIAS.

[142] Article 50, 3., du Règlement ETIAS.

[143] Article 50, 2., du Règlement ETIAS.

[144] Voir l'article 50, 2., als 2 et 3, du Règlement ETIAS.

[145] L'article 52, 1*bis*, vise également l'hypothèse où l'autorité désignée est informée de l'existence de données dans ETIAS via une consultation du **CIR** visée à l'article 22 du Règlement **interopérabilité**. Voir la note de bas de page n° 65.

86. Les articles 14 à 20 du Projet exécutent le Règlement ETIAS en la matière. Ils identifient *a priori* comme **autorités habilités (désignées)** : les services de police, la VSSE, le SGRS, l'AGD&A et l'Office des Etrangers (ci-après, « **OE** »).

87. 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[146]. 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[147].

88. 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.

89. L'Autorité a interrogé le demandeur quant aux **unités opérationnelles** au sens du Règlement ETIAS, qui seront désignées (le seront-elles ultérieurement et par qui ?). Le demandeur a répondu ce qui suit :

> « *Chaque service devra en effet désigner les unités opérationnelles autorisées à faire une demande de consultation et en communiquer la liste à l'UNE. Les services de renseignements et de sécurité ainsi que l'Administration des douanes et accises ont souhaité ajouter un processus de validation interne de ces demandes par un responsable hiérarchique (art 15, al 1, du Projet)* » (souligné par l'Autorité).

90. L'Autorité ne retrouve cependant *a priori* pas dans le dispositif du Projet le principe selon lequel les autorités désignées doivent identifier les unités opérationnelles au sens du Règlement ETIAS. En tout état de cause, dès lors que la désignation de ces unités a un impact direct sur les rôles et responsabilités en matière de traitement de données à caractère personnel, l'Autorité est d'avis que c'est **une norme qui doit les identifier,** et que ce pouvoir (de désignation) ne peut être laissé à l'appréciation des services concernés. En l'occurrence, **le dispositif du Projet peut prévoir que le**

---

[146] Selon cette disposition :

« *Les infractions à la présente loi (et aux articles 433quinquies à 433octies et 433decies à 433duodecies du Code pénal) sont recherchées et constatées par tous les officiers de police judiciaire, en ce compris ceux dont la compétence est limitée, (par les fonctionnaires de la police fédérale et de la police locale), par les (agents de l'Office des étrangers) et de l'Administration des douanes et accises, par les inspecteurs du Ministère de l'Emploi et du Travail et du Ministère des Classes moyennes ainsi que par ceux de l'Office national de la sécurité sociale.*

Ils rassemblent les preuves des infractions et en livrent les auteurs aux autorités judiciaires, conformément aux dispositions du Code d'instruction criminelle.

Ils communiquent au ministre ou à son délégué tous documents et informations utiles à l'exercice de ses missions.

Les documents ou informations visés à l'alinéa précédent peuvent également être communiqués par les inspecteurs du Ministère flamand du Travail et de l'Economie sociale, par les inspecteurs de la Direction générale opérationnelle Economie, Emploi et Recherche du Service public de Wallonie, par les inspecteurs de la Direction de l'Inspection régionale de l'emploi de la Région Bruxelles-Capitale, par les inspecteurs du Ministère de la Communauté germanophone, département emploi ».

[147] P. 20.

Roi détermine au sein des services précités, quelles sont les unités opérationnelles au sens du Règlement ETIAS.

II.3.2. Finalité et extension aux services de renseignements et de sécurité

91. Avant tout, l'Autorité est d'avis que l'article 31, §§ 2 et 3, du Projet (déterminant les règles de protection des données applicables), doit être précisé afin de bien confirmer que « *la consultation du système d'information ETIAS* » dont il est question est la **consultation du système d'information ETIAS aux fins répressives** au sens du Règlement ETIAS, à savoir les consultations visées à la section 4, du Chapitre 3, du Projet, sans préjudice du commentaire émis ci-après.

92. Ensuite concernant les fins répressives, le commentaire des articles[148] explique que les infractions concernées en droit belge ne sont pas directement listées (il est simplement renvoyé aux textes européens, comme y procède ETIAS) pour les raisons suivantes :

> « […] *il est renvoyé à leur traduction en droit national pour justifier la consultation des données. Il n'est en effet pas souhaitable de dresser une liste exhaustive de ces infractions dans la loi même d'une part en raison de l'évolution constante du Code pénal et des autres réglementations pertinentes et, d'autre part, en raison du fait que le seuil de gravité des infractions pénales établi par le règlement ne suffit pas à lui seul pour écarter les infractions de criminalité 'ordinaire' (voir à cet égard le point 151*[149] *de l'arrêt de la CJUE du 21 juin 2022 relatif à l'affaire 'Ligue des droits humains' C-817/19* » (souligné par l'Autorité).

93. **L'Autorité est d'avis que cette motivation n'est pas complètement convaincante** et ce, pour les deux raisons suivantes. Premièrement, l'évolution du droit pénal n'empêche pas le législateur dans d'autres domaines, de légiférer sur la base de listes d'infractions de droit pénal belge concernées, afin de définir la criminalité grave, et ce, en se référant aux fondements légaux de ces infractions[150]. Les incriminations visées par le Règlement ETIAS sont pour le reste déjà très variées (infractions terroristes, participation à une organisation criminelle, traite des êtres humains, trafic illicite de stupéfiants et de substances psychotropes, corruption, cybercriminalité, faux monnayage, escroquerie,

---

[148] P. 12.

[149] Les considérants nos 151 et 152 sont rédigés comme suit :

« *151. Toutefois, 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.*

152. Il incombe donc aux États membres d'assurer que l'application du système établi par la directive PNR est effectivement limitée à la lutte contre des formes graves de criminalité et que ce système n'est pas étendu à des infractions qui relèvent de la criminalité ordinaire » (souligné par l'Autorité).

[150] Voir à ce sujet, notamment, l'Avis de l'Autorité n° 245/2022 du 21 octobre 2022 *concernant un avant-projet de loi relative à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Evaluation de l'Intégrité pour les Pouvoirs publics (CO-A-2022-248)*, considérants nos 18 et s.

contrefaçon et piratage de produits, racisme et xénophobie, racket, falsifications de documents administratifs et trafic de faux, viol, incendie volontaire, détournement d'avion, ***etc.***) de telle sorte qu'il puisse être douté du fait que des mises à jour fréquentes seront nécessaires. En outre, un renvoi vers l'incrimination de droit belge n'empêche pas celle-ci d'évoluer dans le Code pénal, sans qu'une modification du Projet ne soit nécessaire (sauf évidemment si la modification a un impact sous l'angle de la gravité de l'incrimination concernée).

94. Deuxièmement plus fondamentalement, l'approche proposée dans le dispositif du Projet **ne répond pas à la préoccupation exprimée par la Cour de justice** dès lors qu'elle ne comporte aucune règle – aucune condition – permettant la prise en compte de la position de la Cour – elle se borne à renvoyer à la liste des infractions visées par ETIAS et à la peine maximale minimum considérée. En conclusion sur ce point, **l'Autorité est d'avis que le Projet doit identifier les infractions de droit belge de criminalité grave concernées**.

95. Dans un tout autre registre, le Projet[151] **étend les possibilités de consultation ETIAS à des finalités poursuivies par les services de renseignements et de sécurité**, en prévoyant qu'un accès au système central peut être demandé en matière « *de suivi des activités visées aux articles 7, 1°*[152], *et 3°/1*[153], *et 11, § 1er, 1°, 2°, 3°, et 5°*[154] *de la loi du 30 novembre 1998 organique des*

---

[151] Article 14, § 1er, 3°, du Projet.

[152] « *1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique ou économique défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité* » (souligné par l'Autorité).

[153] Il s'agit « *de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge* » (souligné par l'Autorité).

[154] Il s'agit de « *1° de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer:*

a) l'intégrité du territoire national ou la population,

b) les plans de défense militaires,

c) le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,

d) l'accomplissement des missions des Forces armées,

e) la sécurité des ressortissants belges à l'étranger,

f) tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité;

et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense;

2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés;

[…]

5° de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge » (souligné par l'Autorité).

services de renseignement et de sécurité ». **Or** comme cela a été précédemment mis en évidence, ETIAS peut être consulté par les autorités désignées par les Etats membres dans le domaine de la **prévention, de la détection et des enquêtes concernant des infractions terroristes ou d'autres infractions pénales graves**, ces deux derniers concepts étant en outre définis (limitativement) par le Règlement ETIAS[155]. Force est de constater que les finalités poursuivies par la VSSE et le SGRS visées par le Projet **excèdent ce qui est permis par le Règlement ETIAS**. L'Autorité a interrogé le demandeur à propos de la justification de l'extension des finalités de la consultation d'ETIAS réalisée via le Projet et celui-ci a répondu ce qui suit :

> « *Voyez l'exposé des motifs, page 5.*
>
> *Il a été décidé d'inclure les services de renseignements et de sécurité dans les traitements liés aux finalités répressives à l'instar de ce qui a été mis en place pour l'Unité d'information des passagers (système PNR), dans la mesure où ils jouent un rôle important en matière de détection et de prévention des infractions terroristes et d'autres phénomènes de criminalité grave visés dans le Règlement. Il faut également prendre en considération ces deux éléments*
> *-la Belgique est un pays particulièrement 'à risque' du point de vue sécuritaire à la fois comme pays hôte de l'UE et de l'OTAN, notamment, et comme nœud de transports internationaux pouvant être utilisé comme 'plaque tournante' par les organisations criminelles ;*
> *-les phénomènes criminels sont de plus en plus hybrides et la détection des menaces requière une approche intégrée et complémentaire des différents services impliqués.*
>
> *Nous considérions qu'il n'était pas nécessaire pour autant d'ajouter ce point 3° à l'article 14, §1 du Projet dans la mesure où la demande de consultation devra mentionner l'infraction précise en cause (article 14,§2 du Projet), étant entendu que cette infraction fait partie de celles visées aux points 1° et 2°. Les services de renseignements et de sécurité ont cependant insisté pour ajouter ce point 3°, du moins tant que la Cour constitutionnelle ne l'aura pas formellement invalidé (voir l'Affaire Ligue des droits humains, CJUE C-817/19, cinquième question préjudicielle, arrêt de la Cour constitutionnelle attendu -n° de rôle 6713)* » (souligné par l'Autorité).

96. L'Autorité est d'avis que **le dispositif du Projet doit être adapté de manière telle que la VSSE et le SGRS ne puissent, en exécution du Projet, consulter ETIAS** (et plus largement, interagir

[155] Voir l'article 3, 1., 2., du Règlement ETIAS. L'article 3, 1., 15., du Règlement ETIAS définit **l'infraction terroriste** comme « *une infraction qui correspond ou est équivalente à l'une des infractions visées dans 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*.

L'article 3, 1., 16., du Règlement ETIAS définit **l'infraction pénale grave** comme « *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 maximale d'au moins trois ans* ».

avec l'écosystème ETIAS) **<u>que</u> lorsqu'ils exercent leurs compétences *dans la finalité poursuivie par ETIAS***, à savoir dans le cadre des fins répressives telles que définies exhaustivement par le Règlement ETIAS[156] (et ce, **sans préjudice des développements précédents concernant le droit de la protection des données applicables à ces services et l'autorité de contrôle compétente en la matière**)[157]. Si l'Etat belge entend joindre les services de renseignement et de sécurité aux unités opérationnelles qui peuvent accéder au système central ETIAS, cela ne peut se faire que dans les limites permises par le Règlement ETIAS lui-même et autrement dit, dans le cadre de la prévention, de la détection et des enquêtes relatives aux infractions pénales visées par le Règlement ETIAS et aux conditions fixées par ce Règlement. Dans le cas contraire, le Projet méconnaîtrait la délimitation des finalités du système ETIAS et violerait les principes de licéité des traitements et de finalité. **En d'autres termes, l'Autorité est d'avis que l'article 14, § 1er, 3°, du Projet doit être omis**.

97. **Cette constatation a également un impact direct sur l'article 21 du Projet** qui permet à la VSSE et au SGRS d'introduire des données dans la liste de surveillance ETIAS pour les finalités visées à l'article 14, § 1er, du Projet. De nouveau, la finalité poursuivie par le Règlement ETIAS ne peut pas être détournée par une norme de droit belge.

II.3.3. <u>Point d'accès central</u>

98. C'est la **Section du CCN** qui est désignée comme point d'accès central, et « *vérifie en toute indépendance* » la satisfaction des conditions d'accès prévues à l'article 52 du Règlement ETIAS[158].

99. Comme l'Autorité l'a déjà mis en évidence, il doit tout d'abord se dégager clairement du Projet que c'est le **fonctionnaire dirigeant** qui prend les décisions en la matière. Ceci est d'autant plus important que les membres détachés sont issus des services qui sont demandeurs des consultations des données. Autrement dit, leur implication directe dans le processus de vérification indépendante exigé par le Règlement ETIAS est susceptible de causer problème à cet égard, et ce d'autant plus pour les trois raisons suivantes additionnelles.

---

[156] Dans un sens similaire, voir C.J.U.E. (Gr. Ch.), 21 juin 2022 (LIGUE DES DROITS HUMAINS C/ CONSEIL DES MINISTRES), aff. C-817/19, considérants nos 230-237.

[157] Voir les considérants nos 22-26 et 31.

[158] Article 16 du Projet. Plus en détails, l'article 50, 2., als 2 et 3, du Règlement ETIAS prévoit ce qui suit :

« *L'autorité désignée et le point d'accès central <u>peuvent faire partie de la même organisation</u> si le droit national le permet, mais <u>le point d'accès central agit en toute indépendance à l'égard des autorités désignées</u> quand il accomplit ses missions au titre du présent règlement. Le point d'accès central <u>est distinct des autorités désignées</u> et <u>ne reçoit d'elles aucune instruction</u> concernant le résultat de ses vérifications, qu'il effectue de manière indépendante.*

Les États membres peuvent désigner plusieurs points d'accès centraux afin de tenir compte de leurs structures organisationnelles et administratives dans l'accomplissement de leurs obligations constitutionnelles ou autres obligations légales » (souligné par l'Autorité).

100. Premièrement, l'exposé des motifs prévoit que « *L'autorité hiérarchique est également conservée par les services d'origine en ce qui concerne l'évaluation des détachés et les aspects disciplinaires* »[159]. Deuxièmement, il prévoit également que les membres détachés continueront d'assumer des fonctions pour leurs services d'origine dans le cadre d'ETIAS, dans la mise à jour de la liste de surveillance ETIAS[160]. Et troisièmement, le Projet n'encadre pas le détachement de conditions particulières (durée, possibilité d'y mettre un terme, par qui et dans quelles conditions, etc.).

101. **Dans ce contexte, l'Autorité est d'avis que les membres détachés ne peuvent pas être impliqués dans le processus de vérification incombant au point d'accès central, processus qui doit relever de la compétence d'autres agents de la Section CCN**. Ce que le dispositif du Projet doit prévoir, étant entendu qu'en l'état, il est silencieux sur ce point.

II.4. RESPONSABLES DU TRAITEMENT

102. Au-delà de la fixation de la responsabilité des institutions européennes concernées (dont eu-LISA), le Règlement ETIAS prévoit directement qu'en « *ce qui concerne les traitement de données à caractère personnel dans le système central ETIAS par un Etat membre,* ***l'unité nationale ETIAS*** *est considérée comme le* ***responsable du traitement*** » au sens du RGPD ; elle « *assume la* ***responsabilité centrale*** *du traitement de données à caractère personnel dans le système central ETIAS par le dit Etat membre* »[161] (gras ajouté et souligné par l'Autorité).

103. L'article 32, al. 1er, du Projet prévoit quant à lui en outre que « *le président du SPF Intérieur est en charge de la responsabilité opérationnelle du traitement des données à caractère personnel dans le système central ETIAS. A ce titre, il veille à ce que les accès prévus pour les autorités visées à l'article 13, § 2, 4, 4bis et 4ter du Règlement ETIAS seront limités à des personnes dûment autorisées et respectent les finalités de traitement définies dans le règlement* » (souligné par l'Autorité).

104. S'agissant de l'identification du responsable du traitement, l'Autorité rappelle sa pratique d'avis selon laquelle une autorité publique est en principe **responsable du traitement de données nécessaire à la mise en œuvre de la mission d'intérêt public ou de l'obligation légale[162] qui lui incombent, ou encore, qui relève de l'autorité publique dont elle est investie, en vertu de**

---

[159] P. 10.

[160] « *Quand ils assurent une mission de leurs services, ils en répondent à leur hiérarchie. La mise à jour des données de la liste de surveillance doit être contrôlée par la hiérarchie des services d'origine et non par le fonctionnaire dirigeant de la section* », p. 10.

[161] Article 57, 2., du Règlement ETIAS.

[162] Pour une application dans le domaine de l'analyse de la menace, voir l'avis de l'Autorité n° 184/2021 du 4 octobre 2021 *concernant un avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace (CO-A-2021-174)*, considérants nos 36-38.

la norme concernée[163, 164]. Les responsables du traitement peuvent en outre être **conjoints**[165]. L'objectif de la définition large du concept de responsable du traitement[166] est d'assurer une protection efficace et complète des personnes concernées[167]. Selon les faits, une responsabilité conjointe de traitement peut lier plusieurs acteurs, la personne concernée pouvant alors exercer ses droits à l'égard de et contre chacun d'entre eux[168]. Toutefois, « *l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente* [… et a]*u contraire*, [l]*es opérateurs peuvent être impliqués à différents stades du traitement de données et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce* »[169]. C'est dans « *le cadre de ses responsabilités, de ses compétences et de ses possibilités* » que le responsable conjoint veillera à la conformité de son activité aux règles de protection des données[170]. Les responsables conjoints du traitement **devront conclure un accord entre eux déterminant leurs obligations respectives**, « *sauf si, et dans la mesure où leurs obligations respectives sont définies* » dans le contexte normatif national pertinent[171].

---

[163] Et la responsabilité au regard du traitement peut porter sur des obligations/missions de nature technique au regard de ce traitement, voir par exemple l'article 57, 1., du Règlement ETIAS (responsabilité d'eu-LISA au regard de la sécurité de l'information dans le système central ETIAS, et

Sur la pratique de l'Autorité en matière de désignation du responsable du traitement, voir : avis n° 129/2022 du 1er juillet 2022 *concernant les articles 2 et 7 à 47 d'un projet de loi portant des dispositions diverses en matière d'Economie*, considérants nos 42 et s. ; avis n° 131/2022 du 1er juillet 2022 *concernant un projet de loi portant création de la Commission du travail des arts et améliorant la protection sociale des travailleurs des arts*, considérants nos 55 et s. ; l'avis n° 112/2022 du 3 juin 2022 *concernant un projet de loi modifiant le Code pénal social en vue de la mise en place de la plateforme eDossier*, considérants nos 3-41 et 87-88 ; avis n° 231/2021 du 3 décembre 2021 *concernant un avant-projet d'ordonnance concernant l'interopérabilité des systèmes de télépéage routier*, considérants nos 35-37 ; l'avis n° 37/2022 du 16 février 2022 *concernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage'*, considérant n° 22 ; l'avis n° 13/2022 du 21 janvier 2022 *concernant un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale relatif à l'octroi de primes à l'amélioration de l'habitat et un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale modifiant l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 9 février 2012 relatif à l'octroi d'aides financières en matière d'énergie*, considérants nos 9-17 ; l'avis n° 65/2019 du 27 février 2019 *concernant un projet d'accord de coopération modifiant l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative*, considérants nos 90-113.

[164] Voir également sur le sujet les conclusions de l'Avocate générale L. Medina présentées le 8 juin 2023 dans l'Aff. C-231/22, *Etat belge c/ Autorité de protection des données*.

[165] Pour une application dans le domaine de **l'analyse de la menace**, voir l'avis de l'Autorité n° 184/2021 du 4 octobre 2021 *concernant un avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace (CO-A-2021-174)*, considérants nos 59-62.

Pour une application dans le cadre de l'**EES**, voir l'avis de l'Autorité n° 122/2022 du 1er juillet 2022 précité, note de bas de page n° 9.

Pour une application dans le cadre du **SIS**, voir l'avis de l'Autorité n° 121/2022 du 1er juillet 2022 précité, considérants n° 17 et 25 et s.

[166] Les notions de responsable du traitement et de sous-traitant sont définies à l'article 4, 7) et 8) du RGPD. Lire également l'avis G29 n° 1/2010 « sur les notions de "responsable du traitement" et de "sous-traitant" (WP169) », 16 février 2010.

[167] CJUE (Gr. Ch.), 13 mai 2014 (GOOGLE SPAIN SL, GOOGLE INC. c/ AEPD), aff. C-132/12, considérant n° 34 ; CJUE (Gr. Ch.), 5 juin 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH), aff. C-210/16, considérant n° 28.

[168] Article 26, 3., du RGPD.

[169] CJUE (Gr. Ch.), 5 juin 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH), aff. C-210/16, considérant n° 43. Lire également, notamment, G29, Avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, p. 20.

[170] CJUE (Gr. Ch.), 13 mai 2014 (GOOGLE SPAIN SL, GOOGLE INC. c/ AEPD), aff. C-132/12, considérant n° 38.

[171] Article 26, 1., *in fine* du RGPD.

105. L'Autorité souligne que les concepts de responsabilités « *centrale* » (Règlement ETIAS) et « *opérationnelle* » (Projet), n'existent pas dans le RGPD. Elle est par conséquent d'avis **qu'il convient d'omettre du Projet le concept de « *responsabilité opérationnelle du traitement* »**.

106. Le **Règlement ETIAS prévoit explicitement que la personne concernée peut exercer ses droits auprès de l'unité centrale ETIAS ou de l'U.N.E.**[172]. Pour le reste, le Règlement ETIAS et le Projet assurent une répartition des rôles et responsabilités entre les autorités publiques nationales et européennes concernées, qui de concert et indissociablement, participent à la réalisation des finalités poursuivies par le Règlement ETIAS. L'Autorité est d'avis que ces autorités se trouvent dans une situation de **responsabilité conjointe au regard des traitements de données à caractère personnel** mis en œuvre en exécution du Projet et du Règlement ETIAS, **chacune étant responsable du traitement à la mesure des obligations et missions qui lui incombent en vertu du Projet et du Règlement ETIAS**, **et conformément aux règles de protection des données qui s'appliquent à elles[173]**.

107. Cela n'empêche pas que le Projet puisse imputer au président du SPF Intérieur une responsabilité spécifique au regard du traitement, découlant d'obligations qui seraient mises à sa charge par le Projet. En l'état, l'article 32 du Projet lui impute une responsabilité particulière au titre des mesures techniques et organisationnelles à mettre en œuvre ainsi qu'en matière d'*accountability*.

108. Par ailleurs, ces responsabilités seront organisées selon les finalités d'ETIAS, dont la finalité de prévention de risques d'ETIAS[174] et la consultation à des fins répressives de ce dernier[175]. Les rôles des différentes autorités concernées varient en effet selon les finalités et missions poursuivies, tout comme les règles de protection des données matériellement applicables.

II.5. SANCTIONS SPÉCIFIQUES AU RÈGLEMENT ETIAS

109. L'article 62 du Règlement ETIAS, consacré dans un titre relatif à la protection des données, prévoit que les Etats membres doivent déterminer un régime de sanctions (effectives, proportionnées et dissuasives) applicables en cas de violation du Règlement. Le Projet ne prévoit rien en la matière de telle sorte que l'Autorité a interrogé le demandeur à ce sujet. Celui-ci a répondu ce qui suit :

---

[172] Voir l'article 64, 2., du Règlement ETIAS.

[173] Par exemple, si une autorité publique évalue un risque selon les règles du titre 2 ou du titre 3 de la LTD, cela n'empêche pas que les données à caractère personnel qu'elle communique à une autre autorité pour l'exercice de ses propres missions, devront être traitées par cette autorité, conformément au RGPD si celle-ci relève du champ d'application du RGPD. Voir notamment l'avis de l'Autorité n° 184/2021 du 4 octobre 2021 *concernant un avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace (CO-A-2021-174)*, considérant n° 12.

[174] Voir les considérants nos 13-27.

[175] Voir les considérants nos 28-30.

> « *Nous avons considéré que cette disposition qui est incluse dans le chapitre Protection des données du Règlement, visait en particulier la violation du droit applicable en matière de protection des données. Nous avons donc considéré que les sanctions prévues par la loi de 2018 étaient d'application et qu'il n'était pas nécessaire de prévoir une disposition à ce sujet dans le Projet* » (souligné par l'Autorité).

110. L'Autorité prend acte de cette motivation. Cela étant précisé, force est de constater que les auteurs du Règlement ETIAS ont estimé utile d'insérer une telle disposition en étant à la fois tout à fait conscient de l'existence du RGPD et de la Directive 2016/680 ainsi que des règles les exécutant/transposant en droit national.

111. Dans ces conditions, **l'Autorité invite le demandeur à réfléchir à des possibilités de sanctions spécifiques qui pourraient s'appliquer dans le contexte du Règlement ETIAS**. Par exemple, le sujet de la recevabilité des preuves et des poursuites pourrait être exploré, dans la mesure pertinente, etc.

112. De manière générale, l'Autorité est d'avis que le Projet devrait prévoir une obligation spécifique à charge de l'U.N.E. de publier un rapport synthétique et anonymisé sur les manquements en matière de protection des données constatés par les autorités de contrôle, notamment au terme des audits que celles-ci doivent mener. Une telle mesure de transparence est de nature à garantir un meilleur contrôle par la société, des activités de l'U.N.E., et de la sorte, une meilleure effectivité des règles de protection des données. Au passage, l'Autorité rappelle qu'il « *convient que chaque autorité de contrôle soit dotée des moyens financiers et humains,* […] *nécessaires à la bonne exécution de ses missions, y compris celles qui sont liées à l'assistance mutuelle et à la coopération avec d'autres autorités de contrôle dans l'ensemble de l'Union* »[176]. La publication juste évoquée devrait également être assortie de cette mise en contexte, compte-tenu du fait que le Règlement ETIAS aura un impact sur la charge de travail de ces autorités.

II.6. DIVERS

II.6.1. Autorité de contrôle de l'AGD&A

113. 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**

[176] Considérant n° 120 du RGPD.

Données[177]. Or l'article 34 du Projet, concernant l'accès à ETIAS à des fins répressives[178], ne modifie que l'article 281 de la loi du 18 juillet 1977 *générale sur les douanes et accises*[179]. 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 LTD**[180]. 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.

II.6.2. Outils techniques

114. Outils techniques. L'article 25, § 1er, du Projet se réfère aux « *outils techniques nationaux nécessaires afin d'accomplir les missions* » incombant au fonctionnaire dirigeant et aux personnes de sa section. L'Autorité a interrogé le demandeur quant à la question de savoir ce qu'il était entendu par « *outils techniques* » et celui-ci a répondu ce qui suit :

> « *Les outils propres à l'UNE : Application nationale Beltias nécessaire pour gérer la liste de surveillance et les demandes de consultation (mentionnée dans l'exposé des motifs, p 14), les accès prévus dans le Projet au RNN et au Casier judiciaire.*

---

[177] Voir la note de bas de page n° 106.

[178] Pour l'évaluation des risques en matière de sécurité, l'AGD&A doit continuer de relever de la compétence de l'Autorité de Protection des Données, voir le considérant n° 17.

[179] Celui-ci est rédigé comme suit :

« *Art. 281.§ 1er. Toutes actions du chef de contraventions, fraudes ou délits, contre lesquels les lois en matière de douanes et accises prononcent des peines seront portées en première instance devant les tribunaux correctionnels, et, en cas d'appel, devant la cour d'appel du ressort, pour y être instruites et jugées conformément au Code d'instruction criminelle.*

§ 2. Toutes celles des actions susmentionnées qui tendent à l'application d'amendes, de confiscations, ou à la fermeture de fabriques ou usines, seront intentées et poursuivies par l'administration ou en son nom devant lesdits tribunaux, lesquels, en tout cas, ne prononceront sur ces affaires qu'après avoir entendu les conclusions du ministère public. Toutefois, sur la demande écrite qui lui en est faite par un fonctionnaire de l'Administration générale des douanes et accises ayant au moins le grade de conseiller général désigné pour l'administration en charge des contentieux, le ministère public peut requérir le juge d'instruction d'informer, l'exercice de l'action publique restant pour le surplus réservé à l'administration.

§ 3. Dans les cas qu'un même fait de transgression aux lois précitées donne lieu à deux actions différentes, dont l'une doit être intentée par le ministère public et l'autre par l'administration ou en son nom, ces actions seront instruites simultanément, et il y sera statué par un seul et même jugement; mais, dans ces cas, le ministère public n'agira pas avant que l'administration ait, de son côté, porté plainte ou intenté l'action.

§ 4. En recherchant les crimes et délits visés à l'article 8, § 1er, 5°, de la loi du 25 décembre 2016 relative au traitement des données des passagers, le conseiller-général désigné pour l'administration en charge des contentieux peut, par une décision écrite et motivée, charger un agent des douanes et accises, de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers.

La motivation de la décision reflète le caractère proportionnel eu égard à la protection des données à caractère personnel et subsidiaire à tout autre devoir d'enquête.

La décision et sa motivation sont notifiées à l'Organe de contrôle de l'information policière visé à l'article 71 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

L'Organe de contrôle de l'information policière interdit au conseiller-général désigné pour l'administration en charge des contentieux d'exploiter les données recueillies dans des conditions qui ne respectent pas les conditions légales ».

[180] 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).

Divers outils IT nécessaires pour faciliter les missions de l'UNE : JBOX ou autre système permettant un échange électronique des pièces de procédure pour les recours, application Teams pour les interviews[181]*,…*

Nous avons utilisé ce terme générique car ces outils peuvent évoluer » (souligné par l'Autorité).

115. L'Autorité prend acte de cette explication et du fait que cette disposition **n'ait pas pour objectif d'encadrer le traitement de données à caractère personnel**.

II.6.3. Communication de données à des pays non-Membres de l'Union

116. **Sans préjudice des divers commentaires qui ont déjà été émis au sujet du rôle des services de renseignements et de sécurité dans le cadre du Règlement ETIAS**, l'article 20 du Projet prévoit une possibilité, en vertu des articles 93 et 94 de la LTD, ainsi que dans les conditions fixées par cette disposition elle-même, pour ces services, de communiquer des données à des pays non-membres de l'Union européenne. C'est l'article 65 du Règlement ETIAS qui encadre ces possibilités de flux transfrontières. L'article 65, 2., du Règlement ETIAS consacre une interdiction très générale s'appliquant « *également si ces données font l'objet d'un traitement ultérieur au niveau national ou entre Etats membres* ».

117. Parmi les exceptions pertinentes, **c'est l'article 65, 5.**, du Règlement ETIAS qui vise l'hypothèse de la communication de données visées à l'article 52, 4., du Règlement ETIAS, après une consultation aux fins répressives et dans les limites fixées par cette disposition[182]. Notamment, un tel transfert ne peut être réalisé que conformément aux dispositions pertinentes de la Directive 2016/680, et il se dégage du Règlement ETIAS qu'il est alors soumis à l'autorité de contrôle désignée conformément à l'article 41, 1., de la Directive 2016/680. **Le législateur belge ne dispose pas de marge de manœuvre en la matière et l'article 20 du Projet doit par conséquent doit être omis ou adapté de manière telle que les services de renseignements et de sécurité soient à cette fin, considérés comme des autorités compétentes visées par le titre 2 de la LTD** (avec désignation de l'autorité de contrôle compétente).

---

[181] Voir quant au moyen audiovisuel utilisé pour les entretiens, la **Décision d'exécution (UE) 2022/1462 de la Commission du 2 septembre 2022** *relative aux exigences applicables aux moyens de communication audiovisuels utilisés pour l'entretien conformément à l'article 27, paragraphe 5, du règlement (UE) 2018/1240 du Parlement européen et du Conseil*.

[182] L'article 65, 3., vise l'hypothèse particulière d'un retour qui n'est pas pertinente au regard de l'article 20 du Projet.

Par ces motifs,
L'Autorité est d'avis que

1. Le Règlement ETIAS et le Projet entraînent une ingérence importante dans les droits et libertés des personnes concernées (**considérant n° 8**) ;

2. l'article 31, § 2, du Projet peut prévoir l'application du titre 2 de la LTD à « *l'évaluation des risques sécuritaires* », pour autant que l'Autorité de Protection des Données soit l'autorité de contrôle compétente dans ce contexte, sauf pour ce qui concerne la compétence du COC à l'égard des services de police, dès lors que celui-ci a aussi été désigné comme autorité de contrôle en vertu du RGPD (**considérants nos 14 et 17-19**) ;

3. Le Projet doit être revu en ce qui concerne les règles régissant le droit de la protection des données applicable aux services de renseignements et de sécurité ainsi que l'autorité compétente à leur égard en ce qui concerne d'une part, les membres détachés dans le cadre de l'évaluation des risques liés à la sécurité, et d'autre part, l'accès à ETIAS à des fins répressives (**considérant nos 22-26 et 31**) ;

4. L'article 21 du Projet doit être adapté en ce qu'il se réfère aux finalités répressives d'ETIAS plutôt qu'à la finalité de prévention du risque de sécurité. Et il peut prévoir l'application du titre 2 de la LTD en vue de l'alimentation de la liste de surveillance ETIAS, pour autant que l'Autorité de Protection des Données soit l'autorité de contrôle compétente, sauf pour les services de police (**considérant nos 17 et 21**) ;

5. ETIAS soulève une interrogation quant au respect du principe d'égalité entre personnes devant être titulaires d'un visa et personnes devant disposer d'une autorisation de voyage selon ETIAS (**considérants nos 40-41**) ;

6. Le dispositif du Projet ne peut se limiter à prévoir une faculté d'alimenter la liste de surveillance ETIAS mais doit fixer les conditions dans lesquelles les autorités concernées doivent signaler une personne dans la liste de surveillance ETIAS (**considérants nos 45-48**);

7. Le dispositif du Projet doit déterminer les éléments essentiels des traitements de données nécessaires à la contribution de l'Etat belge à l'établissement des indicateurs de risques spécifiques (**considérants nos 49-53**) ;

8. Le dispositif du Projet doit identifier les « *bases de données nécessaires* » qui doivent être consultées par les membres détachés aux fins de la réalisation de l'évaluation des risques de sécurité, sous l'autorité du fonctionnaire dirigeant de la Section CCN de l'U.N.E. (**considérants nos 58-61**) ;

9. L'article 27 du Projet doit clairement préciser que la Section OE de l'U.N.E. est chargée de se prononcer sur le risque d'immigration illégale et d'évaluer ce dernier. Et le Projet doit encore identifier les (catégories de) données à caractère personnel et systèmes d'information qui doivent être réutilisés à cette fin (**considérants nos 62-64**) ;

10. Le dispositif du Projet lui-même doit spécifier que le fonctionnaire dirigeant prend les décisions pour la Section qu'il dirige (**considérants nos 67-68**) ;

11. Un recours en pleine juridiction contre les décisions de l'U.N.E. constitue *a priori* une meilleure garantie pour les droits et libertés des personnes concernées et l'exposé des motifs du Projet modificatif doit en tout état de cause justifier la raison pour laquelle un recours en annulation serait plutôt nécessaire (**considérants nos 71-72**) ;

Le mise en œuvre d'un recours en pleine juridiction se justifie d'autant plus à l'égard des décisions de l'U.N.E. concernant la rectification ou la suppression des données à caractère personnel, de telle sorte qu'un tel recours devrait être prévu dans cette hypothèse par le Projet modificatif (**considérants nos 77-78**) ;

12. Le dispositif du Projet modificatif doit clarifier que l'avis négatif émis par une Section de l'U.N.E. dans le cadre des consultations visées à l'article 28 du Règlement ETIAS constitue une décision susceptible de recours (**considérants n° 73**) ;

13. Le dispositif du Projet doit être adapté et garantir clairement que la personne concernée disposera du droit d'accès à l'évaluation des risques qui a été réalisée à son sujet et sur la base de laquelle une décision administrative est prise à son sujet par l'U.N.E. (**considérants nos 74-76**) ;

14. Le dispositif du Projet doit déterminer dans quelles conditions les autorités concernées doivent communiquer à l'U.N.E. les données à caractère personnel de nature à entraîner l'annulation ou la révocation d'une autorisation de voyage (**considérants nos 79-81**) ;

15. Une norme (et non une décision des services concernés) doit identifier quelles sont les unités opérationnelles au sens du Règlement ETIAS qui peuvent introduire des demandes de consultation d'ETIAS aux fins répressives (**considérants nos 89-90**) ;

16. L'article 31, §§ 2 et 3, du Projet, doit être adapté afin de clarifier qu'il vise la consultation d'ETIAS aux fins répressives (**considérants n° 91**) ;

17. Le Projet doit identifier les infractions de droit belge pertinentes relevant de la criminalité grave visée par le Règlement ETIAS (**considérants nos 92-94**) ;

18. Le Projet doit être modifié (notamment, l'article 14, § 1er, 3°, doit être omis) en ce qu'il entend étendre les finalités d'ETIAS à d'autres finalités poursuivies par les services de renseignement et de sécurité, contrairement à ce que permet le Règlement ETIAS (**considérants nos 95-97**) ;

19. Les membres détachés ne peuvent pas être impliqués dans le processus de vérification incombant au point d'accès central, processus qui doit relever de la compétence d'autres agents de la Section CCN. Ce que le dispositif du Projet doit prévoir, étant entendu qu'en l'état, il est silencieux sur ce point (**considérants nos 98-101**) ;

20. Le Règlement ETIAS et le Projet organisent des responsabilités conjointes au regard du traitement de données et le Projet doit être adapté en conséquence (**considérants nos 102-108**) ;

21. Le demandeur doit explorer la possibilité de consacrer des sanctions particulières en cas de violation des règles de protection des données en exécution du Règlement ETIAS (**considérants nos 109-111**) ;

22. Le Projet doit modifier l'article 71 de la LTD afin que le COC soit également l'Autorité de contrôle de l'AGD&A lorsque celle-ci consulte ETIAS aux fins répressives (**considérant n° 113**) ;

23. L'article 25, § 1er, du Projet (visant les « *outils techniques nationaux nécessaires* ») ne peut pas avoir pour objectif d'encadrer le traitement de données à caractère personnel (**considérants nos 114-115**) ;

24. L'article 20 du Projet doit être omis ou adapté à l'aune de l'article 65, 5., du Règlement ETIAS (**considérants nos 116-117**).

Pour le Centre de Connaissances,
(sé) Cédrine Morlière , Directrice