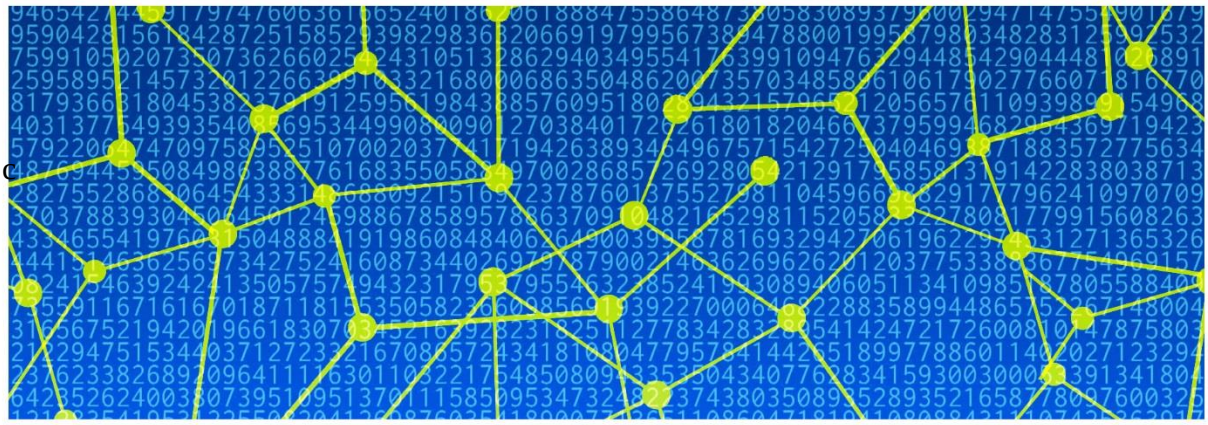

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 3/2017

Avis du CEPD sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

EDPS

6 mars 2017

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE chargée, en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001, «[e]*n ce qui concerne le traitement de données à caractère personnel,* [...] *de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et «*[...] *de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, «lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel», de consulter le CEPD.*

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis se rapporte à la mission du CEPD de conseiller les institutions de l'UE sur les implications de leurs politiques en matière de protection des données et de promotion d'une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Le CEPD considère que le respect des exigences en matière de protection des données sera indispensable au succès du futur système européen d'information et d'autorisation concernant les voyages.

Résumé

La politique de gestion des frontières de l'Union européenne a connu des évolutions notables au cours des dernières années, dues en partie aux difficultés causées par l'afflux de réfugiés et de migrants, ainsi qu'à des préoccupations sécuritaires accrues en raison des attaques à Paris, à Bruxelles et à Nice. La situation actuelle et la nécessité de garantir la sécurité sur le territoire des États membres ont incité la Commission à lancer plusieurs initiatives législatives visant à améliorer la surveillance des personnes qui entrent dans l'espace Schengen.

La proposition de règlement du Parlement européen et du Conseil portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/794 et (UE) 2016/1624 présentée par la Commission le 16 novembre 2016 compte parmi ces initiatives.

Selon ladite proposition, ce système exigerait que les voyageurs exemptés de l'obligation de visa soient soumis à une évaluation des risques qu'ils posent en matière de sécurité, d'immigration irrégulière et de santé publique préalablement à leur arrivée aux frontières de l'espace Schengen. Cette évaluation serait menée au moyen d'un recoupement entre les données que les demandeurs auront communiquées dans l'ETIAS et celles provenant d'autres systèmes d'information de l'Union européenne, d'une liste de surveillance spéciale pour l'ETIAS et de règles d'examen. Ce processus aboutirait à l'octroi – ou au refus – d'une autorisation automatisée d'entrée sur le territoire de l'Union européenne.

Au vu de la proposition ETIAS, le législateur de l'Union européenne semble souscrire à la tendance de plus en plus prononcée qui consiste à répondre de manière conjointe aux objectifs en matière de sécurité et de gestion des migrations, sans tenir compte des différences non négligeables qui existent entre ces deux domaines d'action. La mise en place de l'ETIAS aurait une incidence considérable sur le droit à la protection des données à caractère personnel, étant donné que de nombreux types de données, initialement collectées à des fins très différentes, deviendront accessibles à un plus large éventail d'autorités publiques (à savoir aux autorités compétentes en matière d'immigration, aux garde-frontières, aux autorités répressives, etc.). C'est pourquoi le CEPD estime nécessaire de procéder à une évaluation de l'incidence qu'aura ladite proposition sur le droit au respect de la vie privée et sur le droit à la protection des données à caractère personnel, consacrés dans la charte des droits fondamentaux de l'Union européenne; cette évaluation abordera toutes les mesures relatives aux objectifs en matière de migration et de sécurité qui existent au niveau de l'Union européenne.

En outre, la proposition ETIAS suscite des préoccupations concernant le processus de détermination des risques potentiels que représente le demandeur. À cet égard, il convient d'accorder une attention particulière à la définition desdits risques en tant que tels. Dès lors que ladite évaluation peut avoir pour conséquence sur une personne le refus de l'entrée sur le territoire, la législation doit définir clairement quels sont les risques évalués. Le CEPD s'interroge également sur les règles d'examen de l'ETIAS. Il a conscience que l'objectif du législateur est de créer un outil permettant le repérage automatique des ressortissants de pays tiers exemptés de l'obligation de visa soupçonnés de présenter des risques de ce type. Néanmoins, le profilage, à l'instar de toute forme d'analyse de données par ordinateur appliquée aux personnes, soulève d'importantes questions d'ordre technique, juridique et éthique. Dès lors, le CEPD exige la production d'éléments de preuve convaincants attestant la nécessité de recourir à des outils de profilage aux fins de l'ETIAS.

Par ailleurs, le CEPD s'interroge sur la pertinence de la collecte et du traitement de données relatives à la santé tels qu'envisagés dans la proposition. Il demande une meilleure justification de la durée de conservation des données qui a été choisie et de la nécessité d'octroyer l'accès aux données aux agences répressives nationales et à Europol.

Enfin, il énonce des recommandations concernant, notamment, la répartition des rôles et des responsabilités entre les différentes entités concernées, ainsi que la sécurité de l'information et l'architecture de l'ETIAS.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1],

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[2], et notamment son article 28, paragraphe 2, son article 41, paragraphe 2, et son article 46, point d),

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[3],

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. L'initiative de la Commission européenne visant à adopter un règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) remonte à une communication de 2008 intitulée «Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne»[4]. Dans ladite communication, la Commission suggérait de nouveaux outils pour la gestion future des frontières européennes, notamment le système d'entrée/sortie (EES) et le programme d'enregistrement des voyageurs (RTP), et envisageait pour la première fois l'introduction de l'ETIAS, appelé à l'époque le système d'autorisation électronique de voyage (ESTA) de l'Union européenne. Le CEPD a publié des observations préliminaires[5] sur cette communication la même année.

2. En février 2011, la Commission a publié une étude[6] dans laquelle elle analyse quatre options différentes pour l'introduction d'un ESTA de l'Union européenne. Ladite étude est parvenue à la conclusion que les conditions n'étaient pas remplies à l'époque pour justifier la mise en place d'un ESTA de l'Union européenne. Dans une communication[7] de 2012 concernant les frontières intelligentes, la Commission a estimé qu'il convenait d'écarter temporairement la mise en place d'un ESTA de l'Union européenne mais a annoncé son intention de continuer à travailler sur l'EES et le RTP.

3. Dans sa communication[8] intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité» du 6 avril 2016, la Commission a annoncé qu'elle comptait apprécier la nécessité, la faisabilité technique et la proportionnalité de la mise en place d'un futur système européen d'information et d'autorisation concernant les voyages. Cette même année, la Commission a mené une étude de faisabilité, dans laquelle trois autres systèmes d'autorisation de voyage existants ont été

utilisés comme références: l'ESTA aux États-Unis, l'AVE au Canada et l'eVisitor en Australie.

4. Le 16 novembre, la Commission a publié le rapport final de cette étude de faisabilité[9] (ci-après l'«étude de faisabilité de 2016»), ainsi que la proposition relative à l'ETIAS (ci-après la «proposition»).

5. Le CEPD se félicite d'avoir été consulté de manière informelle par les services de la Commission avant l'adoption de la proposition. Il regrette cependant que, en raison du délai très serré ainsi que de l'importance et de la complexité de la proposition, il lui ait été impossible d'apporter une contribution utile à ce moment-là.

II. OBJECTIF DE LA PROPOSITION

6. Le CEPD croit comprendre, sur la base de la proposition et des documents qui l'accompagnent, que l'ETIAS serait un système d'information automatisé créé dans le but de détecter les risques en matière d'immigration, de sécurité et de santé publique posés par les visiteurs exemptés de l'obligation de visa qui entrent dans l'espace Schengen. Il remarque que les autorités répressives nationales, tout comme Europol, pourraient également avoir accès aux données traitées dans l'ETIAS lorsque ces organes en ont besoin pour prévenir ou détecter des infractions terroristes et d'autres infractions pénales graves, ou mener des enquêtes en la matière.

7. Selon la proposition, tous les ressortissants de pays tiers exemptés de l'obligation de visa devront indiquer une série d'informations sur un formulaire de demande en ligne avant leur voyage. Lors du contrôle et de l'évaluation des informations communiquées par les voyageurs exemptés de l'obligation de visa en vue de l'octroi ou du refus d'une autorisation de voyage, le système comparera automatiquement chaque demande:
   - à d'autres systèmes d'information de l'Union européenne: au système d'information Schengen (SIS), au système d'information sur les visas (VIS), aux données d'Europol, à la base de données d'Interpol sur les documents de voyage perdus ou volés (SLTD), et éventuellement à la base de données d'Eurodac, au futur système européen d'information sur les casiers judiciaires (ECRIS) pour les ressortissants de pays tiers et au futur EES;
   - à une liste de surveillance spécifique à l'ETIAS qui sera établie par Europol et se composera de données relatives aux personnes soupçonnées d'avoir commis une infraction pénale ou d'y avoir participé, ou pour lesquelles il existe des indices concrets ou des motifs raisonnables portant à croire qu'elles commettront une telle infraction; et
   - aux règles d'examen établies dans le cadre du système central ETIAS.

8. Lorsque le traitement automatisé ne donne pas lieu à une réponse positive, le système délivrera automatiquement une autorisation de voyage. S'il aboutit à une ou plusieurs réponses positives, la demande sera traitée manuellement par l'unité nationale ETIAS de l'État membre dans lequel le voyageur a prévu sa première entrée, indiqué dans son formulaire de demande. La mission de l'unité nationale ETIAS responsable serait d'évaluer le risque en matière d'immigration irrégulière, de sécurité ou de santé publique et de décider de délivrer ou de refuser l'autorisation de voyage.

III. RECOMMANDATIONS PRINCIPALES

1. Incidence de l'ETIAS sur le respect de la vie privée et la protection des données

9. Le CEPD constate le nombre croissant de mesures politiques adoptées par l'Union européenne sur des questions relatives à la sécurité et à la migration. Dans son rôle en tant que conseiller auprès du législateur, le CEPD ne se positionne a priori ni pour ni contre une mesure mais se concentre sur la question de savoir dans quelle mesure le choix du législateur est limité par les principes de la protection des données et s'il les respecte le cas échéant.

10. Le CEPD rappelle que le droit à la protection des données à caractère personnel, tel que consacré à l'article 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»), s'applique à toute personne dont les données sont traitées par un responsable du traitement dans l'Union européenne, qu'il s'agisse ou non d'un citoyen/d'une citoyenne de l'Union européenne, d'un migrant/d'une migrante (irrégulier/irrégulière ou non), d'un demandeur/d'une demandeuse d'asile ou d'une personne présumée innocente. Conformément aux principes de nécessité et de proportionnalité, tels que consacrés à l'article 52, paragraphe 1, de la charte, toute limitation de l'exercice du droit à la protection des données à caractère personnel ou toute ingérence dans cet exercice doit être nécessaire et répondre effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui. Le CEPD souligne que lesdits principes constituent des exigences juridiques de haut niveau de la législation de l'Union européenne et qu'ils feront dès lors inévitablement l'objet d'un contrôle minutieux de la part de la Cour de justice de l'Union européenne.

11. Tout d'abord, le CEPD se réjouit de l'attention accordée à la protection des données tout au long de la proposition. Plus particulièrement, il se réjouit notamment de l'harmonisation avec les définitions établies dans le règlement général sur la protection des données[10], dans la directive concernant les secteurs policier et judiciaire[11] et dans le règlement (CE) nº 45/2001 (article 3, paragraphes 2, 3 et 4); de la disposition prévoyant une formation en matière de sécurité et de protection des données pour le personnel de l'Agence européenne de garde-frontières et de garde-côtes qui travaille dans l'unité centrale ETIAS et pour le personnel des unités nationales ETIAS avant que leurs membres soient autorisés à traiter des données enregistrées dans le système central ETIAS (article 65, paragraphe 2, et article 66, paragraphe 3, de la proposition); de la mention des cadres juridiques relatifs à la protection des données qui s'appliquent aux différentes parties prenantes (article 49 de la proposition); et de l'interdiction des transferts et transferts ultérieurs de données provenant de l'ETIAS à des pays tiers, à des organisations internationales et à des personnes privées à l'intérieur ou à l'extérieur de l'Union (article 55).

12. D'après l'exposé des motifs et les documents joints à la proposition, l'ETIAS tel qu'il est proposé actuellement contribuerait, entre autres, à prévenir l'immigration irrégulière, à assurer un niveau élevé de sécurité intérieure et à protéger la santé publique. Dans ce contexte, le CEPD constate que la proposition prévoit un autre système supplémentaire dans le domaine de l'immigration et de la sécurité qui collectera une quantité encore plus importante de données sur les ressortissants de pays tiers (notamment des données relatives à la santé et des données judiciaires). Le CEPD rappelle que la nécessité et la proportionnalité de ce dispositif doivent toutes deux faire l'objet d'une appréciation globale, qui tient compte des systèmes qui existent déjà dans l'Union européenne, de la nature des

données (y compris les données relatives à la santé et les données judiciaires) et de l'étendue du traitement envisagé (il concerne tous les ressortissants de pays tiers exemptés de l'obligation de visa qui entrent dans l'espace Schengen).

13. Le CEPD constate que la proposition ne s'accompagne pas d'une analyse d'impact relative à la protection des données, qui permettrait d'analyser différentes politiques envisageables pour atteindre les objectifs visés en tenant compte de toutes les mesures qui existent à l'échelle de l'Union européenne dans le même domaine d'action et d'évaluer leur incidence sur les (droits fondamentaux des) personnes pour chacune de ces options. **Le CEPD souligne 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**. Le CEPD met cependant en évidence certaines questions qui doivent absolument être abordées dans ladite analyse d'impact relative à la protection des données, telles que:

1) Les domaines d'action distincts qui traitent respectivement de l'immigration et de la sécurité

14. Le CEPD fait remarquer que la gestion de la migration et les objectifs en matière de sécurité sont de plus en plus souvent associés dans le cadre de l'octroi d'accès à des systèmes existants à des fins de répression (au VIS et à l'Eurodac[12], par exemple), de la mise en place de nouveaux systèmes d'information (proposition relative à un système d'entrée/sortie[13], par exemple), ou encore de l'extension des compétences d'un organe existant (des garde-frontières et garde-côtes[14], par exemple).

15. En traitant conjointement les questions relatives à l'immigration irrégulière et les objectifs en matière de sécurité et en établissant une base de données unique dans laquelle figureront à la fois des données liées à la migration et des données relatives à la criminalité, la proposition ETIAS s'inscrit dans ladite tendance actuelle. Cette décision a des conséquences en matière de protection des données, puisque davantage de données à caractère personnel seront collectées et consultées par diverses autorités (autorités compétentes en matière d'immigration, garde-frontières, autorités répressives, etc.). De plus, il pourrait exister un risque de redondance entre les différentes tâches et les différents traitements de données dès lors que, selon la proposition, l'Agence européenne de garde-frontières et de garde-côtes et Europol participeront toutes deux, dans une certaine mesure, à l'évaluation des risques en matière de sécurité. 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.

2) Le risque d'inégalité de traitement entre les voyageurs exemptés de l'obligation de visa et les voyageurs soumis à l'obligation de visa

16. Le CEPD 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 visa dès lors que davantage de données seront centralisées au niveau de l'Union européenne dans l'ETIAS[15] que dans le VIS. En conséquence, davantage de données pourront également être consultées par diverses autorités disposant d'un accès à l'ETIAS. De plus, le CEPD souligne que les données fournies par un demandeur pour obtenir une autorisation

électronique de voyage seront recoupées avec des indicateurs de risques spécifiques et une liste de surveillance, des outils qui ne sont pas utilisés pour l'octroi d'un visa.

3) La redondance entre l'ETIAS et le traitement des données API et PNR

17. En outre, le CEPD s'interroge sur la redondance entre l'ETIAS et les données relatives aux voyageurs exemptés de l'obligation de visa qui proviennent de l'information préalable sur les passagers (API) et du dossier passager (PNR) déjà collectées avant qu'ils n'atteignent l'espace Schengen. Le CEPD constate que, pour les ressortissants de pays tiers exemptés de l'obligation de visa qui voyagent par voie aérienne, une grande partie des informations que recueillera l'ETIAS sont déjà collectées dans le cadre de l'API et du PNR pour évaluer les passagers avant leur arrivée sur le territoire de l'espace Schengen (une fois que le système sera opérationnel). Eu égard à cette constatation, le CEPD se demande si l'ETIAS ne générerait pas des copies d'informations déjà disponibles.

18. En conclusion, le CEPD **insiste sur le fait qu'une analyse d'impact de l'ETIAS sur le respect de la vie privée et la protection des données doit prendre en considération toutes les mesures adoptées à l'échelle de l'Union européenne concernant les objectifs en matière de migration et de sécurité et analyser en profondeur leur application concrète, leur efficacité et leur incidence sur les droits fondamentaux des personnes avant que de nouveaux systèmes entraînant le traitement de données à caractère personnel ne soient créés. Cette analyse doit tenir compte des domaines d'action dans lesquels les mesures s'appliquent et du rôle respectif de chacun des acteurs clés concernés.**

2. Définition des objectifs de l'ETIAS

19. Le CEPD rappelle que, conformément à l'objectif poursuivi par le principe de limitation, lequel se trouve au centre de la protection des données, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes. La ou les finalités doivent être suffisamment précises pour déterminer quel type de traitement leur est associé. Seule une définition claire des finalités permettra une évaluation correcte de la proportionnalité et de la pertinence des données à caractère personnel collectées.

20. Le CEPD souligne également qu'une définition des finalités est non seulement fondamentale en ce qui concerne la protection des données mais aussi essentielle pour assurer l'efficacité du système. Comment une autorité compétente pourrait-elle apprécier si une personne présente un risque en matière d'immigration irrégulière et/ou de sécurité si cette autorité ne dispose pas d'une définition claire des éléments qu'englobent ces termes?

21. L'article premier de la proposition établit que la finalité de l'ETIAS est de déterminer si la présence de voyageurs exemptés de l'obligation de visa sur le territoire des États membres pose un risque en matière d'immigration irrégulière, de sécurité et/ou de santé publique. Le CEPD remarque que la proposition définit le risque en matière de santé publique sur la base de catégories spécifiques de maladies[16] mais n'offre aucune définition des risques en matière de sécurité ou d'immigration irrégulière.

22. La migration (ou l'immigration) est généralement perçue de façon binaire comme soit légale (régulière) soit illégale (irrégulière). Cependant, dans les faits, l'immigration irrégulière se compose d'un large spectre de violations de la législation relative à l'immigration ou d'autres actes législatifs, telles que l'entrée sur le territoire d'un État membre sans l'autorisation ou les documents requis, le dépassement de la durée d'un séjour sans obligation de visa, la fuite durant la procédure d'asile ou le refus de quitter le territoire d'un État membre à la suite d'une décision négative.

23. Le CEPD constate que la proposition ne détermine pas clairement les catégories de violations de la législation en matière d'immigration (et d'autres actes législatifs) susceptibles de poser un risque en matière d'immigration irrégulière. Il déduit de diverses dispositions de la proposition que le fait de dépasser la durée de séjour ou celui de faire l'objet d'une décision de retour seraient, entre autres, des éléments à prendre en considération dans l'évaluation du risque d'immigration irrégulière. Le CEPD recommande de mieux déterminer de quelles violations de la législation en matière de migration et d'immigration il convient de tenir compte. La gravité de l'infraction diffère si un ressortissant d'un pays tiers est entré dans un État membre en utilisant de faux documents ou s'il a dépassé sa durée de séjour d'un ou deux jours.

24. En ce qui concerne les risques en matière de sécurité, le CEPD constate qu'ils ne sont pas non plus définis dans la proposition. La définition de base de la sécurité est le maintien de la sûreté et de l'ordre publics. Elle peut s'appliquer à une pléthore de situations, allant du vandalisme aux actes terroristes. Bien que cela ne soit pas clairement précisé dans la proposition, le CEPD croit comprendre qu'un des éléments clés dans l'évaluation du risque en matière de sécurité serait de savoir si le ressortissant d'un pays tiers est soupçonné d'avoir commis une ou plusieurs infractions pénales ou s'il a été condamné pour infraction pénale. Quant aux risques relatifs à l'immigration, seules les infractions pénales graves devraient être prises en considération dans la détermination des risques en matière de sécurité.

25. **Le CEPD recommande d'inclure une définition des risques en matière d'immigration irrégulière et de sécurité dans la proposition. La définition du risque en matière d'immigration irrégulière devrait préciser les catégories de violations graves de la législation en matière d'immigration (en définissant un seuil de gravité pour la violation, *par exemple,*) qui sont susceptibles de poser un risque d'immigration irrégulière. En ce qui concerne la définition des risques en matière de sécurité, le CEPD recommande de réfléchir aux infractions pénales à cibler, en tenant également compte de celles définies à l'article 3, paragraphe 1, point m), de la proposition.**

3. Les règles d'examen de l'ETIAS en tant qu'outil de profilage

Profilage dans l'ETIAS

26. L'article 28, paragraphe 1, de la proposition prévoit que les dossiers de demande de l'ETIAS seront évalués à l'aune des règles d'examen de l'ETIAS, définies comme «*un algorithme permettant de comparer les données enregistrées dans un dossier de demande du système central ETIAS aux indicateurs de risques spécifiques en matière d'immigration irrégulière, de sécurité ou de santé publique*».

27. L'article 28, paragraphe 2, de la proposition dresse la liste des types d'informations à prendre en considération pour repérer les risques en matière d'immigration irrégulière, de sécurité ou de santé publique (telles que les statistiques et les informations fournies par les États membres), tandis que son article 28, paragraphe 4, contient une liste de données sur la base desquelles l'unité centrale ETIAS définira les indicateurs de risques spécifiques. L'unité centrale ETIAS sera responsable de la définition et des modifications desdits indicateurs de risques spécifiques après consultation du comité d'examen ETIAS, qui se compose de représentants d'Europol et de chaque unité nationale ETIAS (article 28, paragraphe 5). L'article 28 précise encore que l'algorithme sera conservé dans le système central ETIAS et que la Commission pourra adopter des actes délégués afin de spécifier les risques en matière d'immigration irrégulière, de sécurité et de santé publique. Néanmoins, conformément à ce que le CEPD a mentionné ci-avant, une précision préalable de la signification exacte desdits risques est nécessaire[17].

28. Le CEPD a conscience que l'objectif des règles d'examen de l'ETIAS est de créer un outil permettant le repérage automatique des ressortissants de pays tiers exemptés de l'obligation de visa soupçonnés de poser des risques en matière d'immigration irrégulière, de sécurité ou de santé publique. Cet outil est susceptible d'avoir des conséquences néfastes sur lesdites personnes, étant donné que sa finalité est, en définitive, de les empêcher d'entrer sur le territoire d'un des États membres. **À des fins de clarté et de transparence, la technique de traitement des données proposée à l'article 28, qui consiste clairement en une technique de profilage, devrait être explicitement nommée comme telle afin que toutes les garanties qu'il est nécessaire de mettre en place dans le cadre de ce type de traitement soient prévues.**

Analyse d'impact portant sur le profilage

29. Le profilage, à l'instar de toute forme d'analyse de données par ordinateur, soulève d'importantes questions d'ordre technique, juridique et éthique lorsqu'il est utilisé dans un processus de prise de décision qui a des conséquences sur les personnes physiques. L'une des préoccupations principales concernant le profilage est le fait qu'il est inévitablement lié à un haut degré de généralisation et d'incertitude relatif tant à l'exactitude des comportements prédits qu'à la fiabilité de l'attribution de corrélations entre les schémas détectés et certaines caractéristiques spécifiques des personnes. Par ailleurs, l'évaluation des risques que pose une personne au départ d'un profil créé nécessite non seulement d'avoir classé cette personne dans une catégorie au préalable, mais risque également de résulter en un traitement injuste ou préjudiciable de certaines catégories ou de certains groupes de personnes[18].

30. C'est pourquoi le CEPD est préoccupé par la question de la parfaite conformité de l'utilisation des règles d'examen de l'ETIAS avec les droits fondamentaux consacrés dans la charte, en particulier avec les droits au respect de la vie privée, à la protection des données et à la non-discrimination. **Le CEPD recommande que les règles d'examen de l'ETIAS proposées fassent l'objet d'une évaluation préalable exhaustive de leur incidence sur les droits fondamentaux, laquelle appréciera également la nécessité et la proportionnalité de l'utilisation d'un tel outil.**

Nécessité des outils de profilage

31. Outre l'évaluation des demandes au regard des règles d'examen de l'ETIAS, la proposition ETIAS prévoit que chaque demande introduite dans le système central ETIAS sera automatiquement:
    - contrôlée par comparaison avec des informations provenant d'autres systèmes d'information de l'Union européenne cités à l'article 18, paragraphe 2, et
    - comparée à certaines valeurs spécifiques (un numéro de téléphone ou une adresse IP, par exemple) figurant dans la liste de surveillance ETIAS établie conformément à l'article 29.

32. Même si la méthode des règles d'examen s'appuie sur l'analyse de données et constitue une forme de profilage, ces deux méthodes se basent sur la comparaison des données de l'ETIAS aux informations disponibles dans des bases de données de l'Union européenne ou regroupées dans la liste de surveillance afin de rechercher des correspondances potentielles («réponses positives»). Les informations conservées dans d'autres systèmes d'information et dans la liste de surveillance devraient être plus fiables que l'examen par rapport à un profil non transparent créé par un algorithme. Dès lors, le CEPD invite le législateur à réfléchir à la nécessité d'utiliser des règles d'examen aux fins de l'ETIAS, alors que la proposition prévoit d'autres instruments servant à examiner si la présence du demandeur sur le territoire des États membres est susceptible de poser un risque en matière d'immigration irrégulière, de sécurité ou de santé publique.

33. **Le CEPD demande des éléments convaincants attestant qu'il est nécessaire d'utiliser des outils de profilage aux fins de l'ETIAS et, dans le cas contraire, encourage le législateur à réévaluer dans quelle mesure l'utilisation du profilage est nécessaire dans le cadre des objectifs visés**.

Proportionnalité

34. S'il est démontré qu'elle s'avère nécessaire, l'utilisation d'outils de profilage doit aussi être proportionnée. Le CEPD se réjouit que la Commission mette en évidence le fait que les indicateurs de risque doivent être ciblés et proportionnés. Le CEPD n'est pas convaincu que la proposition prévoit des garanties en ce sens ni qu'elle assure un niveau suffisant de protection des droits fondamentaux.

35. La proposition prévoit l'évaluation de toutes les demandes introduites par des ressortissants de pays tiers exemptés de l'obligation de visa au regard des règles d'examen de l'ETIAS[19], alors que seul un nombre restreint d'entre eux est réellement susceptible de poser certains types de risques et de se voir refuser une autorisation de voyage. Ces opérations automatisées et non transparentes de traitement de données à caractère personnel entraînent en tant que telles une ingérence non négligeable dans les droits fondamentaux d'un nombre illimité de demandeurs, qui seront soumis à un profilage; il convient de rechercher un équilibre entre cette ingérence et les résultats escomptés de ce type d'outil.

36. En outre, en fonction de la méthode utilisée pour déterminer les indicateurs de risques spécifiques, que l'on peut interpréter dans un sens très large, le nombre de personnes qui se verraient refuser une autorisation automatique en raison d'une réponse positive se

fondant sur les règles d'examen risque d'être relativement élevé, alors que ces personnes ne présentent en réalité aucun risque.

37. Le CEPD se réjouit du fait que, en cas de refus, la demande est par la suite traitée manuellement par les unités nationales ETIAS (article 22). Cependant, lorsqu'une autorisation automatique est refusée, ce refus peut entraîner des effets non négligeables sur le demandeur. En raison du manque de transparence dans le processus de création des profils, il y a lieu de douter de l'efficacité du traitement manuel des demandes mené par l'unité centrale ETIAS ou par les unités nationales ETIAS. Comment peut-on garantir un examen minutieux et approfondi des risques potentiels détectés dès lors qu'il est probable que les membres du personnel desdites unités ne connaissent pas ou ne comprennent pas eux-mêmes les raisons du refus des autorisations de voyage? Le CEPD ne relève dans la proposition aucun instrument permettant à l'unité centrale ETIAS ou aux unités nationales ETIAS d'apprécier sur le fond une réponse positive au regard des règles d'examen de l'ETIAS.

38. Dans le même ordre d'idées, le CEPD émet des doutes concernant l'efficacité du droit de recours exercé par un demandeur lorsque l'autorisation est refusée en raison d'une correspondance avec un profil. Afin d'apporter au demandeur une véritable solution juridique, l'État membre responsable de cette procédure doit être en mesure de connaître et de comprendre les raisons qui sous-tendent la détermination des risques. Le demandeur dont l'autorisation a été refusée doit également pouvoir comprendre cette décision pour avoir une chance de la faire annuler par une instance de recours.

Risque de discrimination

39. Conformément à la proposition, il est interdit de définir les indicateurs de risques spécifiques sur la base de la race ou de l'origine ethnique d'une personne, de ses opinions politiques, de sa religion ou de ses convictions philosophiques, de son appartenance à un syndicat, de sa vie sexuelle ou de son orientation sexuelle. Il se peut cependant que cette disposition ne réduise pas totalement le risque de discrimination fondée sur de tels critères. Selon l'article 28, paragraphe 4, les données utilisées pour définir les indicateurs de risques spécifiques comprendront, entre autres, la nationalité actuelle, le pays et la ville de résidence du demandeur, ainsi que son sexe et sa profession actuelle.

40. 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.

41. Pour toutes les raisons susmentionnées, **le CEPD demande au législateur de démontrer la nécessité et la proportionnalité du profilage en effectuant une analyse d'impact approfondie portant sur la protection des données.**

4. Données relatives à la santé

42. L'une des finalités de l'ETIAS est d'apprécier si un ressortissant d'un pays tiers exempté de l'obligation de visa est susceptible de poser un risque en matière de santé publique avant son arrivée dans l'État membre. À cette fin, les demandeurs d'autorisation de voyage devront répondre à des questions générales relatives à leur santé lorsqu'ils rempliront leur demande dans l'ETIAS. L'article 15, paragraphe 4, point a), prévoit que chaque demandeur devra répondre à la question de savoir s'il est atteint d'une maladie à potentiel épidémique telle que définie par le règlement sanitaire international de l'Organisation mondiale de la santé ou d'une autre maladie infectieuse ou parasitaire contagieuse. Le contenu et le format de ces questions doivent être déterminés par la suite par la Commission dans des actes délégués. Les seules données pertinentes en matière de santé publique enregistrées dans l'ETIAS sont les réponses par «oui» ou par «non» apportées aux questions générales relatives à la santé. Une réponse par «oui» à n'importe laquelle des questions générales entraînerait un suivi manuel de la demande et exigerait la fourniture d'informations supplémentaires de la part du demandeur.

43. Les données concernant la santé sont des données particulièrement sensibles qui méritent un haut degré de protection[20].

44. Le CEPD se réjouit que la consultation des données relatives à la santé ait été limitée dans la proposition de manière à ce qu'elles ne soient pas accessibles à des fins de répression, ni par des autorités répressives nationales (article 45, paragraphe 2) ni par Europol (article 25, paragraphe 3). Cependant, le CEPD remet en question la valeur ajoutée du traitement et de la collecte de données concernant la santé dans le système ETIAS dans le but de contribuer à protéger la santé publique dans l'Union européenne comme le prévoient les objectifs de la proposition (articles 1 et 4).

45. Les données concernant la santé seront collectées directement auprès du voyageur sans aucune possibilité de vérifier leur exactitude. Même si le demandeur a répondu honnêtement aux questions relatives à sa santé, l'autorisation ETIAS serait valable pour cinq ans et pour de multiples voyages, alors que l'on peut raisonnablement s'attendre à ce que l'état de santé d'une personne change au cours d'une telle période et qu'il n'est pas possible pour le demandeur de modifier les données fournies dans le formulaire de demande en ligne. Dès lors, les données concernant la santé enregistrées pourraient devenir obsolètes et non pertinentes aux fins de la protection de la santé publique.

46. À cet égard, selon l'étude de faisabilité de 2016, si les risques liés aux questions de santé publique (telles que l'éradication de la tuberculose, par exemple) ont récemment été soulignés comme l'une des priorités de l'Union européenne, il n'existe qu'un lien limité entre la réalisation des objectifs en la matière et la collecte d'informations relatives à la santé auprès de ressortissants de pays tiers exemptés de l'obligation de visa[21]. En effet, il est expliqué dans l'étude que les pays concernés par les risques en question sont ceux avec lesquels l'Union est encore en train de négocier des accords de libéralisation du régime des visas. Cette constatation amène le CEPD à s'interroger sur la pertinence et l'efficacité de l'utilisation de l'ETIAS tel qu'il est proposé actuellement pour contribuer à protéger la santé publique.

47. Au considérant 48 de la proposition, il est prévu qu'une interopérabilité sera assurée entre le système ETIAS et des systèmes existants, tels que le SIS, le VIS ou l'ECRIS, par exemple, afin d'évaluer les risques en matière de sécurité, d'immigration irrégulière ou de santé publique que pourrait poser un voyageur exempté de l'obligation de visa, pour permettre un recoupement entre ces systèmes. Toutefois, aucun desdits systèmes ne porte sur des questions de santé; ils sont donc dénués d'intérêt pour atteindre les objectifs de l'ETIAS en matière de santé publique.

48. Le CEPD doute que le traitement de cette catégorie de données particulièrement sensibles à une si grande échelle et pour la durée définie dans la proposition réponde aux conditions fixées à l'article 52, paragraphe 1, de la charte et, dès lors, qu'il soit considéré comme nécessaire et proportionné.

49. **Le CEPD s'interroge sur la pertinence de la collecte et du traitement de données concernant la santé tels qu'envisagés dans la proposition en raison de leur manque de fiabilité, ainsi que la nécessité du traitement de ces données au vu du lien limité qui existe entre les risques en matière de santé publique et les voyageurs exemptés de l'obligation de visa.**

5. Accès des autorités répressives

50. La proposition prévoit d'emblée que les autorités répressives nationales et Europol auront accès au système central ETIAS aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière (article 1, paragraphe 2).

51. L'octroi d'accès à l'ETIAS à des fins répressives s'inscrirait dans une tendance générale observée au sein de l'Union européenne au cours des dernières années visant à accorder auxdites autorités l'accès à des systèmes d'information à grande échelle concernant les frontières et la migration, à l'instar de l'Eurodac, du VIS, ainsi que des systèmes EES et ECRIS proposés[22]. L'accès aux bases de données de l'Union européenne existantes et à venir par les autorités répressives et par Europol ne devrait pas devenir la norme, mais plutôt être autorisé dans des cas restreints dans lesquels la nécessité et la proportionnalité de l'octroi d'un tel accès sont pleinement justifiées et prouvées.

52. Le CEPD estime que la proposition devrait uniquement prévoir l'accès à l'ETIAS à des fins répressives à condition qu'il ait été prouvé que cet accès est nécessaire et proportionné.

53. Dans l'exposé des motifs, la Commission prévoit qu'il «*est impératif* [...] *que les autorités répressives compétentes aient accès à des informations pertinentes et clairement définies dans ETIAS lorsqu'elles en ont besoin pour prévenir ou détecter des infractions terroristes ou d'autres infractions pénales graves, ou mener des enquêtes en la matière*»[23].

54. Toutefois, la Commission ne mentionne pas le futur EES qui devrait contenir des informations sur tous les ressortissants de pays tiers, exemptés ou non de l'obligation de visa, qui entrent dans l'espace Schengen, système auquel les autorités répressives auraient également accès. L'ensemble de données enregistrées dans l'EES serait pratiquement similaire à celui du VIS (à l'exception des données liées au visa lui-même, comme la vignette-visa)[24] et compléterait ces informations par l'ajout de fiches d'entrées et de sorties

pour tous les voyageurs. L'EES serait ainsi en mesure d'offrir aux autorités répressives à tout le moins le même niveau d'information sur les ressortissants de pays tiers exemptés de l'obligation de visas que celui que leur fournit le VIS sur les ressortissants de pays tiers soumis à l'obligation de visa. Le PNR de l'Union européenne sera également accessible aux autorités répressives et à Europol et contiendra des informations supplémentaires sur l'ensemble des passagers aériens, qu'ils soient ou non en possession d'un visa.

55. De plus, la Commission fait référence au VIS comme un exemple de système pour lequel l'accès à des fins répressives s'est montré efficace. À l'appui de cette affirmation, la Commission mentionne le fait que «[l]*'accès aux données du système d'information sur les visas (VIS) à des fins répressives a déjà prouvé son efficacité pour aider les enquêteurs à progresser de manière considérable sur des affaires en rapport avec la traite des êtres humains, le terrorisme ou le trafic de drogue. Le système d'information sur les visas ne contient toutefois aucune donnée relative aux ressortissants de pays tiers exemptés de l'obligation de visa*»[25]. Le CEPD fait remarquer qu'il existe une différence entre «efficace» et «nécessaire» en matière de protection des données[26]. En outre, le rapport d'évaluation concernant le système VIS publié par la Commission à la fin de l'année 2016 conclut que les résultats de son évaluation en matière d'accès à des fins répressives «*restent* [...] *fragmentés et peu concluants*»[27].

56. Eu égard aux considérations qui précèdent, **à ce stade, le CEPD rappelle la nécessité de produire des éléments de preuve convaincants attestant qu'il est nécessaire d'octroyer l'accès aux données ETIAS aux autorités répressives nationales et à Europol. Le CEPD rappelle que la nécessité et la proportionnalité de nouveaux systèmes doivent être appréciées aussi bien de manière globale, compte tenu des systèmes informatiques à grande échelle qui existent déjà au sein de l'UE, que de manière spécifique, dans le cas particulier des ressortissants de pays tiers qui se rendent légalement dans l'UE[28].**

IV. RECOMMANDATIONS COMPLÉMENTAIRES

1. Qualité des données et minimisation des données

57. Le CEPD rappelle que, conformément aux principes de qualité des données et de minimisation des données, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Pertinence des données recueillies auprès du demandeur

58. À l'article 15 de la proposition figure la liste des données concernant le demandeur qui seront collectées au moyen du formulaire de demande. Dans l'étude de faisabilité de 2016 relative à l'ETIAS, il est expliqué que le formulaire de demande ETIAS comptera un maximum de 26 champs de données à compléter, contre 44 pour une demande de visa[29]. Cependant, le CEPD est d'avis que ces nombres ne sont pas vraiment comparables car, selon la proposition, toutes les données collectées (y compris les données relatives à la santé et les données judiciaires) seront éventuellement centralisées et enregistrées dans l'ETIAS. Dès lors, en pratique, davantage de données seront conservées dans l'ETIAS que dans le VIS.

59. En ce qui concerne les catégories de données spécifiques collectées dans l'ETIAS, le CEPD souhaite répéter qu'il faut procéder à une évaluation approfondie de la nécessité de chaque type de données traitées aux fins prévues dans la proposition. Le CEPD ne considère pas toutes les catégories de données reprises à l'article 15 de la proposition comme nécessaires dans le cadre des objectifs en matière de sécurité, de migration ou de santé publique. Dès lors, il insiste sur la nécessité d'apporter des justifications à ce sujet, en particulier en ce qui concerne les données telles que, notamment, l'éducation du demandeur, sa profession actuelle et son adresse IP.

60. Par ailleurs, le CEPD constate que, si la liste de surveillance établie par Europol se base sur les infractions terroristes et autres infractions pénales graves (article 29 de la proposition), les questions générales auxquelles le demandeur doit répondre concernent, elles, *toute* condamnation pour une infraction pénale dans quelque pays que ce soit (article 15, paragraphe 4). Le CEPD estime qu'un certain nombre d'infractions (les infractions routières qui font l'objet de sanctions pénales, par exemple) ne seraient a priori pas pertinentes aux fins de l'ETIAS. **Il recommande que les informations recueillies en matière d'infractions pénales soient limitées à celles concernant des infractions terroristes et des infractions pénales graves telles que définies à l'article 3, paragraphe 1, points l) et m), de la proposition** (à savoir les infractions qui correspondent ou sont équivalentes à celles mentionnées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI si elles sont passibles, en droit national, d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins trois ans).

Pertinence des informations recueillies au départ d'autres systèmes

61. La proposition prévoit un système qui sera doté d'une interopérabilité avec d'autres systèmes de police, judiciaires et relatifs à l'immigration afin de vérifier les informations figurant dans l'ETIAS par rapport à celles enregistrées dans lesdits systèmes. Le CEPD observe que le recoupement des données disponibles dans l'ETIAS avec toutes les informations figurant dans d'autres systèmes n'est peut-être pas pertinent aux fins de l'ETIAS. À titre d'exemple, le CEPD se demande en quoi un signalement dans le SIS concernant des personnes recherchées pour apporter leur aide dans le cadre d'une procédure judiciaire en tant que témoins serait pertinent pour faire face aux risques en matière d'immigration, de sécurité ou de santé publique. De même, toutes les infractions criminelles pour lesquelles le demandeur a été condamné et qui sont conservées dans le système ECRIS ne sont pas pertinentes aux fins de l'ETIAS. **Dès lors, le CEPD recommande de définir précisément quelles informations figurant dans d'autres systèmes sont pertinentes aux fins de l'ETIAS et de limiter strictement à ces informations la comparaison avec des données ETIAS.**

2. Conservation des données

62. L'article 47, paragraphe 1, de la proposition prévoit que chaque dossier de demande ETIAS sera conservé dans le système pendant:

a) la durée de validité de l'autorisation de voyage accordée;
b) cinq ans à compter de la dernière fiche d'entrée du demandeur enregistrée dans l'EES; ou

c) cinq ans à compter de la dernière décision de refuser, de révoquer ou d'annuler l'autorisation de voyage.

63. Les normes en matière de protection des données en vigueur dans l'Union européenne imposent de choisir une durée de conservation des données qui soit la plus courte possible par rapport aux finalités poursuivies[30].

Durée de validité de cinq ans

64. Le CEPD prend note de la durée de validité de cinq ans des autorisations ETIAS (article 30, paragraphe 2, de la proposition). La durée de validité choisie pour les autorisations ETIAS aura une incidence directe sur la durée de conservation des données à caractère personnel enregistrées dans le système.

65. L'étude de faisabilité de 2016 soutient que «par commodité pour les voyageurs, il est préconisé de choisir la période la plus longue possible» et mentionne que «le choix de la période la plus longue possible aurait également des effets positifs sur la charge de travail et les coûts engendrés par la gestion des demandes[31]». Néanmoins, les avantages d'une longue durée de validité seraient contrebalancés par le fait que, «avec le temps, l'évaluation du risque réalisée après l'introduction de la demande perd en pertinence dès lors que la situation dans laquelle se trouve la personne est susceptible de changer». L'étude a conclu qu'une durée de validité de deux à cinq ans constituerait la solution la plus adéquate.

66. Le CEPD s'interroge sur le choix porté par la Commission sur la durée la plus longue envisagée dans l'étude de faisabilité de 2016, soit cinq ans, plutôt que sur une durée plus courte.

Cinq ans à compter de la dernière fiche d'entrée

67. Dans la majorité des cas[32], la durée de conservation des données de l'ETIAS correspondrait dans les faits à celle de l'EES, conformément à l'article 47, paragraphe 1, point b), de la proposition.

68. Selon l'exposé des motifs de la proposition, la Commission désire garantir «*que la fiche d'entrée et l'autorisation de voyage s'y rapportant sont conservées pendant la même durée*»[33] afin que chaque entrée d'un ressortissant d'un pays tiers exempté de l'obligation de visa dans l'espace Schengen soit liée à une autorisation de voyage dans l'ETIAS et à une fiche d'entrée correspondante dans l'EES.

69. Le CEPD estime que l'harmonisation et la cohérence de la durée de conservation proposée pour l'ETIAS avec la durée de conservation de l'EES – qui coïncide elle-même avec la durée de conservation du VIS – ne justifie pas forcément ce choix[34].

Cinq ans à compter du refus, de la révocation ou de l'annulation

70. Le CEPD ne voit pas la nécessité de conserver une demande ETIAS refusée, révoquée ou annulée pour une période aussi longue que cinq ans, comme le prévoit l'article 47, paragraphe 1, point c).

Autres observations

71. Si le caractère nécessaire des trois durées de conservation des données susmentionnées devait être démontré, le CEPD signale que, si l'intention de la Commission est en effet d'assurer un lien entre l'autorisation de voyage figurant dans l'ETIAS et la fiche d'entrée correspondante figurant dans l'EES, il n'apparaît pas clairement à l'article 47, paragraphe 1, point b), de la proposition que la durée de conservation de cinq ans applicable aux dossiers de demande ETIAS court à partir de la date de la dernière fiche d'entrée enregistrée dans l'EES au titre de l'autorisation de voyage *correspondante*.

72. Par ailleurs, le CEPD se demande quelle serait la valeur ajoutée apportée par la conservation du contenu du dossier de demande ETIAS dans son ensemble au-delà de la durée de validité de l'autorisation de voyage et pour une période aussi longue que la durée de conservation de la fiche d'entrée correspondante. La seule information relative au statut du dossier de demande (à savoir demande «accordée» ou «refusée») en lieu et place du contenu du dossier de demande dans son ensemble pourrait s'avérer suffisante aux fins de l'EES.

73. Le CEPD se demande également quelle valeur ajoutée découlerait de la conservation pendant d'aussi longues durées des réponses par «oui» ou par «non» apportées aux questions générales. Outre le fait que les données ETIAS sont d'une fiabilité moindre étant donné qu'elles sont purement déclaratives et recueillies auprès des demandeurs, les réponses aux mêmes questions générales sont particulièrement susceptibles de changer au cours d'une période de cinq ans.

74. **Le CEPD demande au législateur de mieux justifier les durées de conservation des données choisies à l'article 47, paragraphe 1, points a), b), et c), de la proposition afin de veiller à ce que le stockage de données ETIAS soit limité au strict nécessaire aux fins du système en question. Le CEPD recommande également l'établissement de durées différentes de conservation des données en fonction des différentes catégories de données enregistrées.**

3. Interactions entre l'ETIAS et d'autres systèmes d'information

75. Le CEPD constate que l'ETIAS serait doté d'une interopérabilité avec d'autres systèmes de police, judiciaires et relatifs à l'immigration. Le CEPD insiste sur le fait que chacun de ces systèmes a été créé pour une finalité spécifique qui n'est peut-être pas compatible avec les finalités de l'ETIAS. À titre d'exemple, la finalité du système Eurodac est d'aider à déterminer quel sera l'État membre responsable de l'examen d'une demande de protection internationale et de rendre plus aisée l'application du règlement de Dublin[35]. Il n'est pas destiné à contribuer à la détection de risques en matière d'immigration. De même, les propositions pendantes de modification de la base juridique des systèmes existants (à savoir de l'Eurodac, du SIS II, de l'ECRIS) ou de création de nouveaux systèmes (à savoir de l'EES) prévoient également des finalités spécifiques susceptibles de différer de celles du système ETIAS. Plus particulièrement, le CEPD croit comprendre que l'inclusion dans l'ECRIS des condamnations de ressortissants de pays tiers a pour objectifs d'aider les juges et les procureurs et de leur offrir un accès aisé à des informations relatives aux antécédents judiciaires des personnes concernées.

76. **Le CEPD n'a pas connaissance d'un quelconque examen de compatibilité entre les finalités respectives des systèmes mentionnés dans la proposition et celles énoncées dans la proposition ETIAS. Il met l'accent sur le fait que, selon les résultats dudit examen, il se peut que des modifications des bases juridiques des autres systèmes ainsi que des conditions supplémentaires soient requises. Il estime que, avant d'envisager l'accès aux données collectées et traitées dans d'autres systèmes et l'utilisation de ces données, un tel examen s'avère indispensable.**

4. Droits de la personne concernée et voies de recours

77. Le CEPD se réjouit de la possibilité qu'aura la personne concernée d'introduire un recours contre le refus d'une autorisation de séjour, qui lui permet d'intenter une action en justice dans l'État membre qui s'est prononcé sur la demande, conformément à la législation nationale de ce pays (article 31 de la proposition).

78. Toutefois, le CEPD estime que certains motifs de refus cités à l'article 31, paragraphe 1, de la proposition ne sont pas suffisamment clairs, notamment lorsque le motif invoqué est le fait que le demandeur «*(b) fait courir un risque en matière d'immigration irrégulière*» ou encore qu'il «*(c) fait courir un risque pour la sécurité*». Des indications suffisamment claires concernant le ou les motifs du refus doivent être communiquées au demandeur afin qu'il puisse exercer son droit de recours avec efficacité et contester les causes dudit refus. **Le CEPD recommande d'apporter davantage de précisions quant aux informations qui seront communiquées au demandeur en cas de refus d'une autorisation, en particulier si ce refus résulte d'une réponse positive à une règle d'examen dans un autre système d'information.** Ces informations plus précises permettront au demandeur de savoir pour quel système il doit faire valoir son droit d'accès aux données à caractère personnel le concernant enregistrées dans le système en question et, éventuellement, son droit de rectification et/ou son droit d'effacement si une erreur a été détectée ou si ses données ont été traitées de façon illicite.

79. La même réflexion devrait également s'appliquer aux cas dans lesquels une autorisation ETIAS a initialement été accordée avant d'être annulée ou révoquée (articles 34 et 35 de la proposition).

5. Examen indépendant des conditions d'accès

80. Si la nécessité et la proportionnalité de l'utilisation de l'ETIAS en tant qu'outil répressif devaient être démontrées, les conditions régissant l'accès aux données à ces fins devraient alors être strictement réglementées. Le CEPD prend note des conditions d'accès aux données ETIAS à des fins de répression prévues à l'article 45 de la proposition. Il accueille favorablement le considérant 35 de la proposition qui prévoit qu'une demande d'accès aux données ETIAS par les autorités répressives devra «*faire l'objet d'un contrôle préalable par une juridiction ou une autorité offrant des garanties de totale indépendance et impartialité*». **Le CEPD considère qu'un tel examen indépendant revêt la plus haute importance et recommande de le mentionner spécifiquement à l'article 45.**

81. Cependant, le CEPD estime que l'article 44, paragraphe 2, de la proposition introduit une certaine ambiguïté. D'une part, l'article 44, paragraphe 2, prévoit que les États membres

devront veiller à ce que les demandes d'accès émanant des autorités répressives fassent l'objet d'une vérification rapide et efficace du respect des conditions énoncées à l'article 45 conformément à leur droit national et à leur droit procédural. L'article 44, paragraphe 3, indique que, si les conditions énoncées à l'article 45 sont remplies, le point d'accès central devra traiter les demandes et communiquer les données. D'autre part, le considérant 37 de la proposition prévoit que les unités nationales ETIAS devraient servir de points d'accès centraux et s'assurer que les conditions de demande d'accès au système central ETIAS sont remplies dans le cas d'espèce.

82. Lu conjointement au considérant 35, l'article 44, paragraphe 2, suggère l'intervention d'un autre acteur, à savoir d'une juridiction ou d'une [autre] autorité indépendante et impartiale, qui vérifiera que les conditions sont respectées entre le moment où la demande est transmise au point d'accès central et celui ou la demande est traitée par le point d'accès central si les conditions énoncées à l'article 45 sont remplies. Pourtant, le considérant 37 attribue au contraire clairement ce rôle aux unités nationales ETIAS en leur qualité de points d'accès centraux. **Le CEPD recommande dès lors de clarifier la procédure d'accès.**

6. Répartition des rôles et des responsabilités

83. Dans la législation relative à la protection des données, le terme «responsable du traitement» désigne l'entité qui définit les finalités et les moyens du traitement des données. Lorsque les finalités et les moyens du traitement sont fixés par la législation, celle-ci peut également déterminer (les critères régissant) la désignation du responsable du traitement.

84. La répartition des rôles et des responsabilités dans le cadre du système ETIAS proposé est relativement complexe et le CEPD apprécie les efforts consentis pour les délimiter clairement dans la proposition. L'Agence européenne de garde-frontières et de garde-côtes assumera le rôle de responsable du traitement, tandis que 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 l'«agence eu-LISA») assumera celui de sous-traitant (articles 50 et 51 de la proposition). La proposition prévoit également que l'agence eu-LISA sera responsable du développement de l'ensemble du système et de sa sécurité. D'après la proposition, il semble que l'agence eu-LISA s'acquittera de ces rôles sans aucune intervention de l'Agence européenne de garde-frontières et de garde-côtes.

85. Même si la proposition définit bien évidemment les finalités (et, dans une certaine mesure, les moyens) de l'ETIAS, le responsable du traitement des données répond de la mise en application adéquate des mesures techniques et organisationnelles pour veiller à ce que le traitement soit effectué dans le respect des règles relatives à la protection des données, et doit être en mesure de prouver qu'elles sont effectivement respectées (de produire des éléments de preuve attestant que la sécurité de l'information est correctement gérée, par exemple).

86. Selon la répartition des rôles déterminée dans la proposition, l'Agence européenne de garde-frontières et de garde-côtes pourrait se retrouver dans une position où elle devrait répondre – en tant que responsable du traitement des données – de questions qui dépassent le cadre de ses compétences (la façon dont l'agence eu-LISA gère la sécurité de

l'information dans l'ETIAS, par exemple), dès lors que les compétences en question sont exclusivement attribuées à l'agence eu-LISA.

87. **Le CEPD recommande une description plus précise de la répartition des rôles entre l'Agence européenne de garde-frontières et de garde-côtes et l'agence eu-LISA qui envisagerait, le cas échéant, leur désignation au titre de responsables conjoints du traitement**[36].

7. Contrôle préalable par le CEPD des demandes d'accès introduites par Europol

88. Sous certaines conditions, les autorités répressives pourraient avoir accès aux données ETIAS. L'article 44, paragraphe 2, de la proposition prévoit que les États membres veillent «*à ce qu'aux termes de* [leur] *droit national et de* [leur] *droit procédural, les demandes de consultation fassent l'objet d'une vérification indépendante, rapide et efficace*». L'exposé des motifs précise qu'il s'agit d'une vérification menée par «*un tribunal ou une autorité offrant des garanties de totale indépendance et impartialité*»[37].

89. D'après l'article 46 de la proposition, les conditions qui régiront l'accès aux données ETIAS par Europol sont similaires à celles s'appliquant aux autorités répressives nationales (l'accès sera notamment autorisé si la consultation est nécessaire dans une affaire précise, ou si la consultation d'autres bases de données n'a produit aucun résultat, etc.). À l'instar de l'accès à ces données par les autorités répressives nationales, leur consultation par Europol est soumise à un contrôle préalable, dont la proposition confie la conduite au CEPD, «*le cas échéant, conformément à la procédure prévue par l'article 44 du règlement (UE) 2016/794*».

90. Il est de la plus haute importance de faire remarquer que le CEPD ne constitue pas un équivalent fonctionnel des autorités responsables de l'autorisation des accès au niveau national. Au niveau national, les autorités chargées de la vérification seraient les juridictions ou d'autres autorités similaires (en fonction du système juridique national: les juges d'instruction, les procureurs, etc.). Il est vrai qu'il n'existe actuellement aucun équivalent direct au niveau européen: la Cour de justice de l'Union européenne n'exerce pas ce type de rôle dans l'autorisation de mesures d'enquête particulières et la fonction de procureur européen n'a pas encore été créée (en outre, celui-ci disposera vraisemblablement de compétences différentes de celles d'Europol). Le rôle du CEPD est de surveiller et de vérifier le respect des règles relatives à la protection des données, et non d'autoriser des activités d'enquête particulières. Le CEPD a recommandé que les autorités chargées de la vérification soient indépendantes de l'autorité dont elles autorisent les activités[38], mais il n'en découle pas que le CEPD devrait incarner l'autorité chargée de la vérification.

91. En outre, conformément à l'article 44 du règlement (UE) 2016/794 du Parlement européen et du Conseil[39] relatif à Europol, si un cas porte sur des données provenant d'un État membre, le CEPD doit consulter les autorités chargées de la protection des données (ci-après les «APD») dudit État membre avant de prendre une décision. En cas d'autorisation de voyage révoquée ou annulée (décision prise par une unité nationale ETIAS), on peut considérer que les données relèvent de cette disposition. Lors de ce type de consultations, le CEPD peut fixer le délai, entre un et trois mois, dont dispose l'APD de l'État membre pour lui répondre[40]. Dans les situations «extrêmement urgentes»[41], le CEPD peut prendre

des mesures immédiates et en informer l'APD par la suite, en justifiant le caractère urgent de la situation ainsi que la mesure qu'il a prise. Cette option semble être envisagée comme une situation se présentant de manière exceptionnelle, et non comme la procédure opératoire standardisée. Bien que la proposition ne définisse pas ou ne précise pas ce qu'elle entend par contrôle préalable «*rapide et efficace*» (article 46, paragraphe 3), il semble que les délais escomptés soient bien plus courts que ceux que la procédure prévue à l'article 44 du règlement (UE) 2016/794 serait en mesure de proposer. Telle qu'elle est actuellement rédigée, cette procédure placerait dès lors le CEPD dans une position où il lui serait juridiquement impossible de respecter ce que l'on exige de lui.

92. **Pour les raisons mentionnées ci-dessus, le CEPD recommande de désigner une autorité chargée de la vérification indépendante qui ne soit pas le CEPD.**

8. Vérification par l'unité centrale ETIAS

93. Deux aspects de l'ETIAS ne sont pas décrits suffisamment en détail, que ce soit dans la proposition ou dans l'exposé des motifs: premièrement, le type de recherches qui seront effectuées dans d'autres systèmes d'information et la façon dont elles le seront et, deuxièmement, le type et la quantité d'informations que contiendra une réponse positive. Selon l'article 3, paragraphe 1, point k), de la proposition, par *réponse positive*, on entend «*l'existence d'une correspondance établie par comparaison des données à caractère personnel enregistrées dans un dossier de demande du système central ETIAS aux données à caractère personnel conservées dans un relevé* [...] *dans un système d'information interrogé par le système central ETIAS* [...]». Cette définition d'une valeur positive peut inciter à comprendre la réponse positive comme un champ purement *booléen* dont les seules valeurs possibles seraient *vrai* ou *faux*. En ce qui concerne la façon dont les recherches seront effectuées, le CEPD croit comprendre au départ de l'article 19, paragraphe 3, de la proposition qu'elles apporteront des réponses *non concluantes* en ce qui concerne l'identification du demandeur[42]. S'il existe des recherches non concluantes liées à une demande, l'unité centrale ETIAS est censée disposer de la capacité de vérifier «*si les données enregistrées dans le dossier de demande correspondent à celles qui figurent dans l'un des systèmes d'information ou l'une des bases de données consultés* [...]»[43].

94. Cependant, comment l'unité centrale ETIAS peut-elle procéder à cette vérification dès lors que les seules informations dont elle dispose sont le dossier de demande et les informations relatives aux réponses positives/négatives? Il n'existe que deux possibilités: soit une *réponse positive* contiendra en réalité davantage d'informations que celles mentionnées dans la proposition actuelle et exposera alors les informations enregistrées dans les systèmes interconnectés à l'ETIAS aux différentes parties qui participent à un quelconque contrôle, à savoir l'unité centrale ETIAS et les unités nationales ETIAS (dont la base juridique n'autorise pas forcément l'accès à ce type d'informations); soit l'unité centrale ETIAS et les unités nationales ETIAS sont supposées avoir accès à tous les systèmes d'information qui seront interrogés par l'ETIAS. Chacun de ces deux scénarios nécessite une révision non seulement de la proposition ETIAS, mais également des textes juridiques qui régissent tous les systèmes auxquels l'ETIAS aura accès.

95. **Le CEPD recommande d'apporter des éclaircissements quant à la façon dont l'unité centrale ETIAS pourra procéder à la vérification. Une fois que le processus sera clair, le législateur devra inclure dans la proposition tout changement nécessaire (a) afin**

d'apporter des précisions complètes au sujet de l'accès par l'unité centrale ETIAS aux informations dont elle a besoin pour vérifier la demande et/ou (b) afin de supprimer le rôle de vérificateur des demandes *non concluantes* dévolu à l'unité centrale ETIAS.

9. Architecture et sécurité de l'information

96. Dès lors qu'autant d'entités différentes consultent les données, et que le système central ETIAS en consulte autant d'autres, la coordination de la sécurité de l'information revêt une importance capitale, car chacune des entités et chacun des systèmes d'information concernés ne bénéficiera que du niveau de sécurité du maillon le plus faible. Par ailleurs, seule une analyse appropriée des risques auxquels le système est soumis en matière de sécurité de l'information permettra d'assurer un niveau adéquat de sécurité de l'information. Même si l'on pouvait considérer les mesures en la matière figurant dans la proposition comme la base de référence minimale, le CEPD souligne à quel point la mise en place d'une gestion correcte des risques liés à la sécurité de l'information telle qu'exigée par l'article 22 du règlement (CE) nº 45/2001 et également mentionnée à l'article 52 de la proposition est importante.

97. L'ETIAS introduirait des changements fondamentaux dans l'architecture actuelle des systèmes d'information à grande échelle hébergés et gérés par l'agence eu-LISA: dans un environnement jusqu'ici fermé, accessible uniquement aux États membres et, éventuellement, à quelques entités de l'Union européenne, l'ETIAS s'ouvrirait à l'internet dans son ensemble[44]. Les conséquences d'une telle décision en matière de sécurité de l'information ne sauraient être sous-estimées et une analyse adéquate doit être demandée, effectuée et examinée. En outre, jusqu'ici, un partage d'infrastructure tel que celui proposé entre l'ETIAS et l'EEE n'a encore jamais été mis en place entre plusieurs systèmes: là encore, une décision architecturale technique de ce type doit être bien conçue et étayée par des documents, et l'agence eu-LISA doit prévoir et mener une analyse spécifique des risques encourus dans chaque solution envisagée.

98. De plus, la proposition est très détaillée concernant l'architecture du système, ce qui limite les choix techniques qui peuvent être adoptés lors de l'analyse et de la définition d'une ou plusieurs solutions techniques. Le règlement proposé ne devrait pas imposer de décision architecturale particulière, sauf en cas d'incidence sur d'autres parties du règlement, mais devrait par contre exiger une analyse appropriée des risques en matière de protection des données et en matière de sécurité pour guider la mise au point du système.

99. Enfin, l'article 63 de la proposition décrit les responsabilités liées au développement et à la gestion opérationnelle du système ETIAS. Cependant, il n'y est fait aucune mention de la protection des données ou de la sécurité: tout nouveau système, et toute modification majeure d'un système existant (en l'occurrence, pas d'un seul, mais de plusieurs, à savoir le VIS, *les données Europol*, le SIS, l'Eurodac et l'ECRIS[45]), ne sauraient être réalisés professionnellement que dans le respect: (1) d'une procédure de sécurité adéquate comprenant une analyse détaillées des risques en matière de sécurité de l'information; et (2) des principes de protection des données dès la conception et par défaut.

100. En outre, la proposition charge la Commission d'«*adopter des règles détaillées* [...] *relatives à la protection et à la sécurité des données applicables* [...]. *Ces mesures*

d'exécution sont adoptées en conformité avec la procédure d'examen visée à l'article 79, paragraphe 2», notamment concernant le site web public et l'application pour appareils mobiles[46], l'accès aux données par les transporteurs à des fins de vérification[47] ou concernant l'utilisation des données à des fins de notification et d'établissement de statistiques[48]. Dans tous les cas susmentionnés, la proposition devrait imposer que lesdites *règles détaillées* relatives à la protection et à la sécurité des données se fondent sur les principes de gestion des risques liés à la sécurité de l'information et de protection des données dès la conception et par défaut respectivement.

101. **Le CEPD recommande d'ajouter à l'article 63 l'obligation d'effectuer et de conserver une évaluation des risques en matière de sécurité de l'information et de respecter les principes de protection des données dès la conception et par défaut.**

102. En ce qui concerne les articles chargeant la Commission d'adopter des règles détaillées relatives à la sécurité et à la protection des données (articles 14, 39, 40 et 73), **le CEPD recommande d'ajouter à ces articles la nécessité de tenir compte de la gestion des risques en matière de sécurité de l'information ainsi que de la protection des données dès la conception et par défaut.**

103. **Le CEPD recommande également de modifier l'article 6 pour qu'il ne mentionne que les éléments réellement nécessaires dans le cadre du règlement proposé, et qu'il laisse à l'agence eu-LISA et au reste des parties prenantes concernées la conception de l'architecture finale du système ETIAS.**

104. Bien que l'article 50 de la proposition confie le rôle de *responsable du traitement* à l'Agence européenne de garde-frontières et de garde-côtes, il ne lui est conféré aucune responsabilité concernant la sécurité du traitement. Cependant, la législation établit qu'un responsable du traitement des données est responsable de la sécurité des opérations de traitement[49]. Même si l'agence eu-LISA[50] fournissait toutes les mesures et analyses de sécurité et assumait la majorité, voire la totalité, des responsabilités en matière de sécurité pour le système ETIAS, l'Agence européenne de garde-frontières et de garde-côtes serait toujours responsable du traitement des données à caractère personnel réalisé par l'unité centrale ETIAS.

105. **Le CEPD recommande de modifier l'article 52 et/ou l'article 65 afin de reconnaître la responsabilité de l'Agence européenne de garde-frontières et de garde-côtes en ce qui concerne la sécurité de l'information.**

10. Statistiques

106. Le CEPD comprend que le personnel dûment autorisé des autorités compétentes des États membres, de la Commission, de l'agence eu-LISA et de l'unité centrale ETIAS doit élaborer des rapports et produire des statistiques sur les données contenues dans l'ETIAS. Toutefois, le volume de données pouvant être consultées est susceptible de permettre l'identification d'individus, contrairement à ce qui est affirmé à l'article 73 de la proposition. Par exemple, la combinaison de la nationalité, du sexe et de la date de naissance d'un ressortissant d'un pays tiers peut entraîner son identification.

107. **Le CEPD recommande par conséquent de reformuler l'article 73 en reconnaissant que les données énumérées à l'article 73, paragraphe 1, points a) à i), peuvent entraîner l'identification d'individus et qu'elles doivent dès lors être protégées de manière similaire au reste de l'ETIAS.** Cette protection implique de procéder à une évaluation adéquate des risques dans le domaine de la sécurité de l'information et de mettre en œuvre des mesures de sécurité appropriées avant de créer ce fichier central supplémentaire.

108. Le CEPD met vivement en garde contre le fait que la solution proposée actuellement pour générer des statistiques imposera une lourde charge à l'agence eu-LISA, qui devra gérer et sécuriser de manière appropriée un deuxième fichier, ainsi qu'au CEPD, qui devra le contrôler. Le CEPD serait favorable à une solution qui, au lieu de rendre nécessaire un fichier central supplémentaire, imposerait à l'agence eu-LISA de développer des fonctions permettant aux États membres, à la Commission, à l'agence eu-LISA elle-même et à l'unité centrale ETIAS d'extraire automatiquement et directement les statistiques demandées du système central ETIAS, sans qu'un fichier supplémentaire soit nécessaire.

109. Néanmoins, si un fichier différent est créé, et dans le cadre de l'utilisation explicitement consentie d'informations anonymes, la proposition pourrait examiner la possibilité de mettre en place l'une ou l'autre technologie renforçant la protection de la vie privée telle que l'*accès à distance aux données* ou le *respect différentiel de la vie privée* afin de permettre en effet le traitement de données à caractère personnel sans que celles-ci ne soient réellement consultées.

110. Enfin, contrairement aux autres règlements relatifs aux systèmes d'information à grande échelle, il n'est prévu, à l'article 73 de la proposition de règlement, aucune obligation de rendre publiques les statistiques annuelles.

11. Rôle du CEPD

111. Le CEPD est l'autorité chargée de la protection des données qui supervise à la fois l'agence eu-LISA et l'Agence européenne de garde-frontières et de garde-côtes[51]. Bien que le CEPD soit habilité à obtenir des institutions, organes et agences de l'Union européenne toutes les informations pertinentes pour l'exercice de ses fonctions[52], le processus doit être rationalisé par l'ajout du CEPD à la liste des destinataires des rapports que l'agence eu-LISA ou l'unité centrale ETIAS présenteront à la Commission, au Conseil ou au Parlement européen[53].

112. En outre, **le CEPD recommande d'ajouter à l'article 57 une disposition similaire à celle de l'article 56, paragraphe 2, de manière à ce que les ressources nécessaires lui soient allouées pour lui permettre d'assurer une surveillance adéquate de ce nouveau système**.

V. CONCLUSION

113. Le CEPD se réjouit de l'attention accordée à la protection des données tout au long de la proposition portant création de l'ETIAS.

114. Dans le plein respect du rôle du législateur dans l'appréciation de la nécessité et de la proportionnalité des mesures proposées, le CEPD rappelle que ces deux exigences juridiques de haut niveau consacrées par la charte peuvent faire l'objet d'un contrôle minutieux de la part de la Cour de justice de l'Union européenne et qu'il incombe au CEPD de veiller à leur respect. Il souligne qu'en l'absence d'une analyse d'impact (relative à la protection des données), il est impossible d'évaluer la nécessité et la proportionnalité de l'ETIAS tel qu'il est proposé actuellement.

115. Étant donné que la proposition met en place un système supplémentaire entraînant le traitement d'une quantité non négligeable d'informations à caractère personnel relatives à des ressortissants de pays tiers à des fins liées à l'immigration et à la sécurité, le CEPD conseille au législateur de prendre en considération toutes les mesures qui existent au niveau de l'Union européenne en lien avec le traitement de données à des fins relatives à la migration et à la sécurité, et d'effectuer une analyse approfondie de leurs objectifs et de leurs résultats.

116. Dans ce contexte, le CEPD recommande d'inclure une définition des risques en matière d'immigration irrégulière et de sécurité dans la proposition afin de respecter le principe de limitation.

117. De plus, le CEPD s'inquiète de savoir si l'utilisation des règles d'examen de l'ETIAS sera pleinement conforme aux droits fondamentaux consacrés dans la charte. Il recommande que les règles d'examen de l'ETIAS proposées fassent l'objet d'une évaluation préalable exhaustive de leur incidence sur les droits fondamentaux. Le CEPD se demande également si des éléments convaincants attestent qu'il est nécessaire d'utiliser des outils de profilage aux fins de l'ETIAS et, dans le cas contraire, encourage le législateur à revoir sa position quant au recours au profilage.

118. Le CEPD s'interroge sur la pertinence et l'efficacité de la collecte et du traitement de données concernant la santé tels qu'envisagés dans la proposition en raison de leur fiabilité limitée. Il s'interroge également quant à la nécessité de traiter ces données au vu du lien limité qui existe entre les risques en matière de santé publique et les voyageurs exemptés de l'obligation de visa.

119. En ce qui concerne l'accès des autorités répressives et d'Europol aux données ETIAS, le CEPD souligne qu'il n'existe actuellement pas d'élément attestant la nécessité desdits accès. Le CEPD rappelle que la nécessité et la proportionnalité de nouveaux systèmes doivent être appréciées aussi bien de manière globale, compte tenu des systèmes informatiques à grande échelle qui existent déjà au sein de l'UE, que de manière spécifique, dans le cas particulier des ressortissants de pays tiers qui se rendent légalement dans l'UE.

120. Au-delà des principales préoccupations recensées ci-dessus, les recommandations exprimées par le CEPD dans le présent avis concernent les aspects suivants de la proposition:

- la nécessité et la proportionnalité de l'ensemble de données collecté;

- les durées de conservation des données choisies;
- l'interopérabilité entre l'ETIAS et d'autres systèmes d'information;
- les droits de la personne concernée et les voies de recours prévues;
- l'examen indépendant des conditions d'accès par les autorités répressives;
- la répartition des rôles et des responsabilités entre l'Agence européenne de garde-frontières et de garde-côtes et l'agence eu-LISA;
- la vérification par l'unité centrale ETIAS;
- l'architecture et la sécurité de l'information de l'ETIAS;
- les statistiques générées par le système; et
- le rôle du CEPD.

121. Le CEPD reste disponible pour apporter des conseils supplémentaires concernant la proposition, ainsi que tout acte délégué ou d'exécution adopté portant sur le règlement proposé qui serait susceptible d'avoir une incidence sur le traitement de données à caractère personnel.

Bruxelles, le 6 mars 2017

Giovanni BUTTARELLI
Contrôleur européen de la protection des données

NOTES

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] JO L 350 du 30.12.2008, p. 60.
[4] Communication du 13 février 2008 de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions – Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne, COM(2008) 69 final.
[5] Observations préliminaires du CEPD du 3 mars 2008, disponibles à l'adresse: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf (version anglaise uniquement).
[6] Étude de la politique relative à un système d'autorisation électronique de voyage de l'Union européenne (ESTA de l'Union européenne) de février 2011, disponible à l'adresse: http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/esta_annexes_en.pdf (version anglaise uniquement).
[7] Communication de la Commission au Parlement européen et au Conseil du 25 octobre 2011 intitulée «Frontières intelligentes: options et pistes envisageables», COM(2011) 680 final.
[8] Communication de la Commission au Parlement européen et au Conseil du 6 avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité», COM(2016) 205 final.
[9] Étude de faisabilité du 16 novembre 2016 relative à un système européen d'information et d'autorisation concernant les voyages (ETIAS) – rapport final disponible à l'adresse: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20161116/etias_feasability_study_en.pdf (version anglaise uniquement).
[10] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1.
[11] 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, JO L 119 du 4.5.2016, p. 89.
[12] Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JO L 218 du 13.8.2008, p. 129; 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 (refonte), JO L 180 du 29.6.2013, p. 1.
[13] Proposition de règlement du Parlement européen et du Conseil relatif au corps européen de garde-frontières et de garde-côtes et abrogeant le règlement (CE) nº 2007/2004, le règlement (CE) nº 863/2007 et la décision 2005/267/CE du Conseil, COM(2015) 671 final.
[14] Règlement (UE) nº 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) 2016/399 du Parlement européen et du Conseil et abrogeant le règlement (CE) nº 863/2007 du Parlement européen et du Conseil, le règlement (CE) nº 2007/2004 du Conseil et la décision 2005/267/CE du Conseil, JO L 251, 16.9.2016, p. 1 à 76.
[15] Notamment les informations relatives aux réponses positives/négatives et les réponses à des questions générales relatives à la santé, aux condamnations pénales, à un séjour dans une zone de guerre ou de conflit particulière.
[16] L'article 3, paragraphe 1, de la proposition définit un risque pour la santé publique comme «*une menace pour la santé publique telle que définie à l'article 2, point 21), du règlement (UE) 2016/399*», c'est-à-dire comme «*toute maladie à potentiel épidémique telle que définie par le règlement sanitaire international de*

l'Organisation mondiale de la santé et les autres maladies infectieuses ou parasitaires contagieuses pour autant qu'elles fassent l'objet de dispositions de protection à l'égard des ressortissants des États membres».

[17] Voir chapitre III, section 2, ci-dessus – Définition des objectifs

[18] Voir, par exemple, *Profiling the European Citizen. Cross-Disciplinary Perspectives*, eds. M. Hildebrandt, S. Gutwirth, Springer 2008, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices*, L. Colonna, Stockholm 2016.

[19]Il n'existe qu'une exception mineure s'appliquant aux membres de la famille d'un citoyen de l'Union européenne ou d'un ressortissant de pays tiers jouissant du droit à la libre circulation en vertu du droit de l'Union, voir article 21 de la proposition.

[20] Les données concernant la santé sont définies à l'article 4, paragraphe 15, du règlement général sur la protection des données comme «*les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne*». Elles relèvent d'un régime de protection des données plus strict applicable à des catégories particulières de données. L'article 9 dudit règlement prévoit que, si le traitement est nécessaire pour des motifs d'intérêt public important, le droit de l'Union ou d'un 'État membre doit prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

[21] Voir étude de faisabilité de 2016, précitée, tableau 41, p 131.

[22] Avis du contrôleur européen de la protection des données du 7 octobre 2009 à propos de l'accès à Eurodac par les autorités répressives, point 18; avis du contrôleur européen de la protection des données du 18 juillet 2013 sur les propositions de règlement portant création d'un système d'entrée/sortie (EES) et de règlement portant création d'un programme d'enregistrement des voyageurs (RTP), point 68; observations formelles du CEPD du 3 novembre 2015 sur la consultation publique de la Commission européenne sur les frontières intelligentes, p. 5; avis 06/2016 du CEPD sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point 76.

[23] Exposé des motifs, p. 11.

[24] Voir articles 5 et 9 à 14 du 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 de données entre les États membres sur les visas de court séjour (règlement VIS), JO L 218 du 13.8.2008, p. 60 à 81.

[25] Exposé des motifs, p. 11.

[26] La Cour européenne des droits de l'homme a jugé que le concept de nécessité n'avait pas la souplesse de termes tels qu'«admissible», «normal» ou «utile», mais qu'il impliquait un «besoin social impérieux»; voir arrêt de la CEDH du 7 décembre 1976 dans l'affaire Handyside c. Royaume-Uni, requête nº 5493/72, point 48.

[27] Rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre du règlement (CE) nº 767/2008 du Parlement européen et du Conseil établissant le système d'information sur les visas (VIS), l'utilisation des empreintes digitales aux frontières extérieures et l'utilisation de la biométrie dans la procédure de demande de visa/évaluation REFIT, p. 11.

[28] Avis 06/2016 du CEPD du 21 septembre 2016 sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point 14.

[29] Étude de faisabilité de 2016, précitée, p. 156 à 158.

[30] Voir notamment l'avis 06/2016 du CEPD sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point 28.

[31] Voir étude de faisabilité de 2016, précitée, p 15.

[32] Il semble au CEPD que, conformément à l'article 47, paragraphe 1, point a), de la proposition, la durée de conservation des données ne correspondrait à la durée de validité de l'autorisation de voyage que dans quelques cas (peu probables), dans lesquels il n'existerait aucune fiche d'entrée dans l'EES en lien avec ladite autorisation. Cette situation se produirait lorsqu'un voyageur exempté de l'obligation de visa ayant reçu une autorisation ETIAS soit ne l'a pas utilisée au cours de sa durée de validité, soit est entré dans l'espace Schengen le même jour que celui où l'autorisation ETIAS a été délivrée, soit s'est vu refuser l'entrée dans l'espace Schengen malgré l'autorisation octroyée.

[33] Exposé des motifs, p. 34.

[34] Avis 06/2016 du CEPD sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point 29.

[35] Règlement (UE) nº 604/2013 du Parlement européen et du Conseil du 26 juin 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 (refonte), JO L 180 du 29.6.2013, p. 31.

[36] Voir article 28 de la proposition de règlement du Parlement européen et du Conseil 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) nº 45/2001 et la décision nº 1247/2002/CE, COM(2017) 8 final.
[37] Exposé des motifs, p. 12.
[38] Avis 06/2016 du CEPD sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point 86; avis 07/2016 du CEPD du 21 septembre 2016 sur le premier paquet de mesures pour une réforme du régime d'asile européen commun (Eurodac, EASO et règlement de Dublin), point 58.
[39] 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, JO L 135 du 24.5.2016, p. 53 à 114.
[40] Règlement (UE) 2016/794, article 44, paragraphe 4.
[41] *Ibid.*
[42] Cette situation peut se présenter dès lors que les réponses positives ne se basent pas sur des correspondances exactes mais sur des similarités entre les informations qui figurent dans le formulaire de demande et celles conservées dans les bases de données consultées, ou parce que, lors d'une recherche dans laquelle plusieurs des attributs du formulaire de demande sont utilisés, seuls certains d'entre eux correspondent à des informations figurant dans les bases de données consultées.

[43] Article 20 de la proposition – Vérification par l'unité centrale ETIAS.
[44] Article 6 de la proposition – Composition et architecture technique du système d'information ETIAS.
[45] Tous (ceux) figurant dans la liste à l'article 10 de la proposition – Interopérabilité avec d'autres systèmes d'information.
[46] Article 14 de la proposition – Le site web public et l'application pour appareils mobiles.
[47] Article 39 de la proposition – Accès aux données par les transporteurs à des fins de vérification.
[48] Article 73 de la proposition – Utilisation des données à des fins de notification et d'établissement de statistiques.
[49] Conformément à l'article 22 du règlement (CE) nº 45/2001.
[50] Selon l'article 23 du règlement (CE) nº 45/2001, l'agence eu-LISA devrait également respecter les obligations qui incombent au responsable du traitement définies à l'article 22: «*La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que: a) le sous-traitant n'agit que sur instruction du responsable du traitement; b) les obligations visées aux articles 21 et 22 incombent également au sous-traitant* [...]».
[51] Cette fonction est confirmée à l'article 49, paragraphe 1, de la proposition, où il est répété que le règlement (CE) nº 45/2001 s'applique tant à l'agence eu-LISA qu'à l'Agence européenne de garde-frontières et de garde-côtes; dès lors, le CEPD est leur autorité de contrôle en ce qui concerne le traitement de données à caractère personnel.
[52] Article 47, paragraphe 2, du règlement (CE) nº 45/2001; et disposition lui succédant (l'article 59, paragraphe 1, de la proposition de règlement du Parlement européen et du Conseil 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) nº 45/2001 et la décision nº 1247/2002/CE, COM(2017) 8 final, est similaire).
[53] À cette fin, le CEPD devrait être ajouté en tant que destinataire des rapports mentionnés aux articles suivants: article 77, paragraphe 3; article 78, paragraphe 4; et article 81, paragraphes 2, 4 et 5. De plus, l'article 52, paragraphe 4, devrait prévoir que le CEPD soit informé des mesures prises par l'eu-LISA en vertu de l'article 52, non seulement lors de la mise en service de l'ETIAS, mais aussi tout au long de la durée de vie de l'ETIAS et de ses données.