Les risques de l'utilisation de l'Intelligence Artificielle dans le règlement ETIAS pour les droits fondamentaux des voyageurs étrangers exemptés de visa

Marc Naro

Axe Intégration européenne

MASTER Droit européen

Les risques de l'utilisation de l'Intelligence Artificielle dans le règlement ETIAS pour les droits fondamentaux des voyageurs étrangers exemptés de visa

Mémoire pour le Master 1 Droit européen

Parcours Droit et globalisation économique (DEGE)

Présenté et soutenu par :

Marc Naro

Directrice de mémoire :

Sandrine Turgis

Maitre de Conférence à l'Université de Rennes – HDR

Suffragant :

Damien Franchi

Doctorant contractuel à l'Université de Rennes

Année universitaire 2023 / 2024

Illustration réalisée par *DALL-E 3* avec l'indication : « Illustre un mémoire de recherche en droit européen intitulé 'Les risques de l'utilisation de l'Intelligence Artificielle dans le règlement ETIAS pour les droits fondamentaux des voyageurs étrangers' », le 14 mai 2024.

Lorsque le suspect remplace le condamné, la police se substitue à la justice

Frédéric Gros

REMERCIEMENTS

Je tiens d'abord à exprimer ma reconnaissance auprès de ma directrice de mémoire, Madame Sandrine Turgis, pour ses conseils précieux, sa bienveillance et son accompagnement tout au long de cette année.

Je souhaite également remercier tous les professionnels avec qui j'ai pu m'entretenir dans le cadre de mes recherches. Leurs contributions ont été essentielles pour obtenir une vision représentative de la mise en œuvre concrète du règlement ETIAS.

Ainsi, au Service National des Enquêtes d'Autorisation de Voyage, je remercie Laurent Siam, commissaire divisionnaire de police et Chef de l'Unité Nationale ETIAS ainsi que Séverin Koffi, chef du département de soutien de l'Unité Nationale ETIAS.

Au sein d'EU-Lisa. je remercie Agnès Diallo, Directrice exécutive, Théofanis Syrigos, président du groupe de conseil sur la mise en oeuvre des règlements EES et ETIAS, Joris Vankeerberghen, responsable des plateformes d'hébergement intelligentes, Athanasia Papavasileiou, responsable des technologies d'information ainsi que Sasha Madzar, consultant.

Au sein de Frontex, je remercie Jonas Grimheden, chef du bureau des droits fondamentaux.

Ces remerciement vont également à Niovi Vavoula, professeure à l'Université de Luxembourg, pour son aide dans la réflexion qui a précédé ce mémoire.

Enfin, j'ai une pensée toute particulière à ma famille et mes amis pour leur présence et leur soutien au cours de cette année malgré la distance.

PRINCIPALES ABRÉVIATIONS

API	Advance Passenger Information
BMS	Biometric Matching Service
CEDH	Cour Européenne des Droits de l'Homme
CEPD	Comité Européen de la Protection des Données
CESE	Comité Économique et Social Européen
CIR	Common Identity Repository
CJUE	Cour de Justice de l'Union Européenne
CNIL	Commission Nationale de l'Informatique et des Libertés
COM	Communication
CRRS	Central Repository for Reporting and Statistics
CSDHLF	Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales
ECRIS-TCN	European Criminal Record Information System for Third-country Nationals
EES	Entry/Exit System
ESP	European Search Portal
ESTA	Electronic System for Travel Authorization
Etc.	Et caetera
ETIAS	European Travel Information and Authorization System
EU-Lisa	European Union Agency for the Operational Management of Large-Scale IT System
Eurodac	European Asylum Dactyloscopy Database
Europol	European Union Agency for Law Enforcement
FRA	European Union Agency for Fundamental Rights
Frontex	European Border and Coast Guard Agency
UE	Union Européenne
UIP	Unité Information Passagers
Ibid.	Ibidem
IA	Intelligence Artificielle
In	Dans
Interpol	Organisation Internationale de la Police Criminelle
JOUE	Journal Officiel de l'Union Européenne
MID	Multiple Identity Detector
N°	Numéro
OMS	Organisation Mondiale de la Santé
Op. cit.	Opus citatum
PNR	Passenger Name Record
P.	Page
RGPD	Règlement Général sur la Protection des Données
SIS	Schengen Information System
SLTD	Interpol Stolen and Lost Travel Documents
SNEAV	Service National des Enquêtes d'Autorisation de Voyage
Spéc.	Spécifiquement
TDAWN	Interpol Travel Documents Associated with Notices
TFUE	Traité sur le Fonctionnement de l'Union européenne
TUE	Traité sur l'Union européenne
V	Versus
Vol.	Volume
VIS	Visa Information System

SOMMAIRE

INTRODUCTION GÉNÉRALE

«Nous devons savoir qui franchit nos frontières. D'ici au mois de novembre, nous proposerons [...] un système automatisé visant à déterminer qui sera autorisé à voyager à destination de l'Europe. De cette manière, nous saurons qui voyage vers l'Europe avant même que cette personne n'arrive »[1] scandait le président de la Commission européenne Jean-Claude Juncker dans son discours sur l'état de l'Union le 14 septembre 2016.

Cette volonté de l'Union de combler un « déficit d'information » a été accélérée par la crise migratoire des années 2010 et la vague d'attentats subséquents à Paris en 2015 et Bruxelles en 2016. Pour assurer la sécurité des citoyens européens, l'Union a renforcé ses systèmes d'information se dotant de nouvelles technologies comme l'intelligence artificielle (IA) en faveur d'une « digitalisation de la politique migratoire de l'Union européenne »[2]. Ces technologies, de plus en plus utilisées pour faire face aux risques migratoires, sont ainsi instrumentalisées au service de choix politiques[3].

Le règlement pour le système européen d'information et d'autorisation concernant les voyages (ETIAS)[4], dont la mise en œuvre est attendue en mai 2025 est l'une des pièces du « puzzle »[5] que forment les systèmes d'information intéropérables pensés par l'Union européenne pour surveiller les flux migratoires et renforcer les contrôles aux frontières.

---

[1] Commission européenne, « Union de la sécurité: la Commission propose de créer un système européen d'autorisation et d'information concernant les voyages » (COM), 16 novembre 2016.

[2] BROM, Frans, BESTERS, Michiel,'"Greedy' Information Technology: The Digitalization of the European Migration Policy," *European Journal of Migration and Law* 12, no. 4, 2010, p.455-470.

[3] TURGIS, Sandrine, « Les systèmes d'information à grande échelle au carrefour de la politique du numérique et des politiques en matière d'asile, d'immigration et de contrôle des frontières », in Bertrand Brunessen (dir.), *La politique européenne du numérique,* Bruylant, Bruxelles, p. 444.

[4] Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nos 1077/2011, 515/2014, 2016/399, 2016/1624/ et 2017/2226, *JOUE*, L 236, 19 septembre 2018, p. 1.

[5] VAVOULA, Niovi, « The "Puzzle" of EU Large-Scale Information Systems for Third-Country Nationals : Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection », *European Law Review*, 2019, p. 1-32.

I. L'interopérabilité des systèmes d'information à grande échelle : un pas inédit vers un État de surveillance

La mise en place de l'intreopérabilité des systèmes d'information à grande échelle est un choix politique et une avancée technique qui traduit la nouvelle conception de la politique de migration et d'asile de l'Union.

1. *Le développement d'un État de surveillance en réponse aux velléités sécuritaires de l'Union*

Exacerbée par la montée de l'extrême droite au Parlement européen qui défend l'existence d'un lien fondamental entre l'insécurité et l'immigration[6], la politique de migration et d'asile est mise au service de la politique sécuritaire de l'Union. Ce lien est symbolisé par l'intéropérabilité des sytèmes d'information à grande échelle et le nouveau Pacte sur la migration et l'asile adopté en avril 2024[7]. Ces législations renforcent les moyens dont sont dotées les agences de l'Union européenne comme Frontex, Europol et EU-Lisa pour la lutte contre les risques migratoires, conduisant à une véritable « agenciarisation de la politique d'immigration et d'asile »[8] de l'Union.

Ainsi, ces agences sont chargées de surveiller et contrôler les flux migratoires en faveur d'une « fortification »[9] des frontières européennes. Elles déploient massivement des outils numériques comme l'intelligence artificielle, qui, grâce à sa capacité de traitement des données, est un nouvel outil privilégié pour assurer la surveillance des flux migratoires de l'Union européenne. Ces nouvelles technologies permettent aujourd'hui de reconnaître une personne grâce à la technologie de reconnaissance biométrique[10], ou de déceler la vérité ou les émotions dans d'une personne[11] presque

---

[6] BIGOT, Didier, « Sécurité et immigration : vers une gouvernementalité par l'inquiétude ? », *Cultures & Conflits*, vol. 31-32, 1998, p.14.

[7] Parlement européen, « Les députés approuvent le nouveau pacte sur la migration et l'asile » (Communiqué de presse), 10 avril 2024 (consulté le 25 avril 2024 à 12:33) < https://www.europarl.europa.eu/news/fr/press-room/20240408IPR20290/les-deputes-approuvent-le-nouveau-pacte-sur-la-migration-et-l-asile>.

[8] Rostane Medhi, L'Agenciarisation de la politique d'immigration et d'asile, collection confluences, 2020, 153p.

[9] RODIER, Claire et al. « Pour une autre vision de la frontière », *Revue projet*, n°335, 2013, p.61.

[10] DUSHI, Desara, « The use of facial recognition technology in EU law enforcement: Fundamental rights implications », *Global Campus of Human Rights,* 2020, p.2. ; ISRAEL, Tamir, « Facial recognition at a crossroads : Transformation at our Borders and Beyond », *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)*, 2020, p.1-189.

[11] GREMSL, Thomas, HODL, Elisabeth, « Emotional AI : Legal and Ethical Challenges », Information polity 27, 2022, p.164; VAN MOENSEL Lieve, et NEVIL, Nissy, « What if your emotions were tracked to spy on you? », *European Parliamentary Research Service*, mars 2019, p.1-2.

sans failles[12][13]. Elles peuvent également être utilisées pour prédire les mouvements migratoires afin d'anticiper les afflux de migrants et les contrôles aux frontières[14]. Cette nouvelle conception constitue un changement de paradigme de la politique migratoire, faisant passer cette dernière d'une logique de « contrôle » des migrations (réactif, axé sur des individus concrets) au « management » des migrations (proactive, axée sur des populations migrantes potentielles)[15] . L'utilisation de nouvelles technologies à cette fin n'est pas une première. Ainsi, des algorithmes sont utilisés depuis plusieurs années pour décider de l'octroi du statut de réfugié au Canada[16], et pour l'évaluation des risques que représentent un migrant arrivé irrégulièrement à la frontière États-Unis-Mexique[17]. Le développement de ces outils en ce sens a provoqué d'importantes critiques[18] soulevant les dangers que ces technologies représentent pour les droits fondamentaux[19], notamment le droit à la vie privée, à la protection des données et à la non-discrimination.

Cette nombreuses atteintes font craindre l'établissement d'un État de surveillance aux airs de 'Big Brother'[20]. Le règlement ETIAS qui est l'une des dernières composantes de la politique migratoire de l'Union a ainsi été comparé au panoptique de Bentham[21] dont parle Foucault, en ce qu'il permet l'établissement d'un système de surveillance dans lequel les ressortissants étrangers sont désormais perçus comme des « suspects »[22]. Cette suspicion qui pèse sur les voyageurs étrangers va à l'encontre du droit à la présomption d'innocence et constitue donc un danger pour les droits

---

[12] RAPTIS, George et al., « Using Eye Gaze Data and Visual Activities to Infer Human Cognitive Styles : Method and Feasibility Studies. » Proceedings of the 25th Conference on User Modeling, Adaptation and Personalization (July 2017), p.164-173.

[13] Quand bien même Victor Hugo disait que « Les mots manquent aux émotions » dans *Le dernier jour d'un condamné*, 1829.

[14] BEDUSCHI, Ana, « International Migration Management in the Age of Artificial Intelligence », *Migration studies vol 9*, 2020, p.576.

[15] DERAVE, Charly, GENICOT, Nathan, HETMANSKA, Nina, « The risks of trustworthy AI - The case of ETIAS », *European journal of risk regulation*, 2022, p. 10.

[16] MOLNAR, Petra, GILL, Lex,, « Bots at the Gate : A human rights analysis of Automated decision-making in Canada's immigration and refugee system », *University of Toronto and the Citizen Lab-Munk School of Global Affairs and Public Policy*, 2018, p.14.

[17] KOULISH, Robert, « Immigration Détention in the Risk Classification Assessment Era », *Connecticut Public Interest Law Journal*, Vol. 16, 2016, p.3.

[18] BOFFEY, Daniel, « EU Border 'Lie Detector' System criticized as Pseudoscience », The Guardian, 2 Novembre 2018, https://www.theguardian.com/world/2018/nov/02/eu-border-lie-detection-system-criticised-as-pseudoscience.

[19] European Union Agency for Fundamental Rights (FRA), Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, 2019, 34p.

[20] CHARMEIL, Thimothée, « George Orwell's Dystopian World Is Coming To Life And The European AI Act Will Not Stop It : The Collection Of Emotional Data By AI - HKS Student Policy Review » . *HKS Student Policy Review*, 10 mars 2024, https://studentreview.hks.harvard.edu/george-orwells-dystopian-world-is-coming-to-life-and-the-european-ai-act-will-not-stop-it-the-collection-of-emotional-data-by-ai/.

[21] LEESE, Matthias, « Exploring the Security/Facilitation Nexus: Foucault at the "Smart" Border », 30 Global Society, 2016, p.412.

[22] DERAVE, Charly, GENICOT, Nathan, HETMANSKA, Nina, op.cit, p.27.

fondamentaux. En effet, comme l'affirmait Frédéric Gros dans un entretien sur les systèmes de surveillance : « Lorsque le suspect remplace le condamné, la police se substitue à la justice » [23].

2. *L'interopérabilité grandissante des systèmes d'information à grande échelle*

Pour répondre à ces velléités sécuritaires[24], les institutions européennes ont adopté un ensemble ambitieux de règlements visant à instaurer des systèmes d'information à grande échelle afin de contrôler les risques intérieurs et extérieurs relatifs aux migrations. Ainsi, l'Union européenne dotée depuis le troisième pilier de Maastricht d'une compétence partagée en matière de politique migratoire et d'asile dans l'espace de liberté, sécurité et justice[25], a construit une véritable boîte à outils numérique pour surveiller, contrôler, réguler les flux migratoires de ressortissants étrangers[26]. Ce corpus règlementaire est composé du Système d'information Schengen (SIS II)[27], Système de comparaison des empreintes digitales (Eurodac)[28], Système d'information visas (VIS)[29], Système entrée et sortie (EES)[30], Système d'information et autorisation voyage (ETIAS) et Système d'information casier judiciaire (ECRIS-TCN)[31], dont les données seront rassemblées au sein des

[23] PROUST, Jean-Marc, «Surveiller et punir» est devenu surveiller, punir et jouir », *Slate*, publié le 4 février 2016 (consulté le 22 avril 2024 à 19h39) < https://www.slate.fr/story/113619/surveiller-punir-jouir#> (consulté le 31 mars 2024 à 15:11)

[24] BIGOT, Didier, « L'immigration à la croisée des chemins sécuritaires », dans *Revue européenne des migrations internationales*, vol. 1, 1998, p.26-27.

[25] Art. 3, § 2, Traité de l'Union Européenne (TUE).

[26] Voir annexe 4.

[27] Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006, *JOUE* L312/14.

[28] Règlement (UE) No 603/2013 du Parlement 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), *JOUE* L180/1.

[29] 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), *JOUE* L 218/60 L 218/60.

[30] Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) no 767/2008 et (UE) no 1077/2011, *JOUE* L 327/20.

[31] Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726, *JOUE* L 135/1.

composants du cadre d'interopérabilité européen[32] que sont le portail de recherche européen (ESP), le service partagé d'établissement de correspondances biométriques (BMS partagé), le répertoire commun de données d'identité (MID) et le détecteur d'identités multiples (CIR) et le répertoire central des rapports et statistiques (CRRS)[33].

L'intéropérabilité se définit ainsi comme la capacité des systèmes d'information à échanger des informations. Ceux-ci ont été pensés pour être interdépendants. Les données pourront ainsi être échangées à travers les composants du système d'interopérabilité pour les différents objectifs qui sont assignés aux systèmes d'information. Cette capacité nouvelle génère des risques pour les droits fondamentaux, notamment liés au fait que les données ne sont désormais plus traitées qu'à une seule fin. Le règlement ETIAS qui permet la collecte de donnée personnelles sur les voyageurs exemptés de visa est donc une composante clé du cadre de l'interopérabilité.

II. L'instauration du règlement ETIAS : un nouvel outil migratoire et sécuritaire

Le règlement est singulier ETIAS en ce qu'il revêt depuis une triple vocation migratoire, sécuritaire et sanitaire afin de renforcer la capacité de l'Union à faire face aux risques engendrés par les voyageurs étrangers.

3. *Les finalités multiples d'ETIAS*

ETIAS est un outil de la politique de migration et d'asile de l'Union instauré sur la base de l'article 77 §2 b) et d) du Traité sur le Fonctionnement de l'Union européenne (TFUE), qui permet à l'Union de prendre des mesures pour le développement d'un système intégré de gestion des frontières. Le système d'information vise à lutter contre des risques migratoires, sécuritaires et sanitaires[34]. Ces risques diverses sont traités par un seul et unique système qui solidifie ainsi les liens existant entre la gestion des migrations et la sécurité[35] ou de santé publique, en ce que l'un de ses principaux objectifs est de contribuer à un niveau renforcé de sécurité et de santé publique par l'évaluation des risques en matière en d'immigration illégale générés par les voyageurs. Le règlement permettra ainsi de

---

[32] Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil, *JOUE* L 135/27.

[33] Article 1 du règlement 2019/817 (Interopérabilité)

[34] Article 3 du règlement 2018/1240 (ETIAS).

[35] Niovi, VAVOULA , « Consultation of EU Immigration Databases for Law Enforcement Purposes/ a Privacy and Data Protection Assessment », *European Journal of Migration and Law, 22,* 2020, p. 145.

collecter les données renseignées par les voyageurs étrangers exemptés de visa, ce qui contribuera à la sécurisation des frontières par l'établissant de bases de données puissantes pour la gestion des flux migratoires. Ce règlement s'inscrit ainsi dans la logique de l'érection de « Smart Border »[36] aux frontières de l'Union européenne grâce à l'interopérabilité des systèmes d'information à grande échelle.

4. *La construction progressive d'ETIAS*

L'idée de la mise en place d'un système européen automatisé d'autorisation de voyage pour les ressortissants de pays tiers exemptés de visa avait été évoquée pour la première fois en 2008 par la Commission[37]. Une étude avait alors été lancée sur la potentielle création d'un système électronique d'autorisation de voyage, appelé « EU-ESTA » en référence à son homologue américain. Ainsi, le modèle s'inspire des systèmes d'autorisation de voyage comme l'ESTA aux États-Unis (Electronic System for Travel Authorization[38]) et l'eTA au Canada (Electronic Travel Authorization[39]).

Abandonné en 2011 par la Commission à cause des « coûts trop importants » qu'il aurait générés pour des résultats « incertains » sur la sécurité[40], le projet refait surface au printemps 2016[41] à la suite des attaques terroristes sur le sol européen. Il est proposé par la Commission cette année-la puis adopté par règlement du Parlement et du Conseil le 12 septembre 2018. Le texte a ensuite été modifié à deux reprises, avec la publication du règlement du 20 mai 2019 sur l'interopérabilité[42] et celui du 7 juillet 2021 sur les conditions d'accès aux autres systèmes d'information[43]. Le déploiement d'ETIAS

---

[36] Commission européenne, « Frontières intelligentes : options et pistes envisageables », COM(2011) 680 final, 25 octobre 2011.

[37] Commission européenne, « Preparing the next steps in border management in the European Union » (Communication) COM (2008) 69 final.

[38] Congrès américain, act to provide for the implementation of the recommendations of the National Commission on Terrorist Attacks Upon the United States, United States Congress, Public Law 110-53, 3 août 2007.

[39] Parlement canadien, règlement modifiant la loi sur l'immigration et la protection des réfugiés (LIPR), Section 11 (1.01), 30 juin 2017.

[40] Commission européenne, « Frontières intelligentes: options et pistes envisageables », COM (2011) 680 final, 25 octobre 2011, p.7.

[41] PwC, « Feasibility Study for a European Travel Information and Authorisation System (ETIAS) », Final Report, 16 novembre 2016.

[42] Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) no 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil, *JOUE* L 135, 22 mai 2019.

[43] Règlement (UE) 2021/1152 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (CE) no 767/2008, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861 et (UE) 2019/817 en ce qui concerne l'établissement des conditions d'accès aux autres systèmes d'information de l'UE aux fins du système européen d'information et d'autorisation concernant les voyages, *JOUE* L 249, 14 juillet 2021.

a été successivement retardé à cause du retard pris pour instaurer EES et des Jeux Olympiques[44]. Son exécution est conduite par trois agences européennes : EU-Lisa, chargée de développer le logiciel ETIAS, Frontex qui héberge et met en exécution le système ETIAS à travers son unité centrale, et Europol qui joue un rôle central dans le fonctionnement ETIAS et l'échange d'information criminelles. Cette coopération accrue entre Frontex et Europol brouillera davantage les frontières entre le contrôle des frontières et la sécurité intérieure et encouragera la tendance à considérer les migrants comme un risque pour la sécurité[45].

5. *Le champ d'application spécifique d'ETIAS*

Le règlement ETIAS s'applique aux voyageurs étrangers exemptés de visa, qui pouvaient jusqu'alors voyager dans l'Union sans formalités administratives[46]. Le public cible d'ETIAS concerne donc les citoyens de 61 pays tiers, 2 régions administratives spéciales (Hong-Kong et Macao) ainsi que Taiwan qui n'est pas reconnue officiellement par au moins un État membre de l'UE[47], qui devront désormais recevoir une autorisation de voyage par l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (EU-Lisa) pour entrer sur le sol européen. Le système d'autorisation de voyage ne s'appliquera donc pas aux personnes titulaires de la nationalité d'un des États membres quand bien même ils seraient binationaux[48], ni aux ressortissants de pays tiers qui sont membres de la famille d'un citoyen de l'Union[49] en vertu de la directive sur les droits des citoyens[50]. Ce nouveau public concerne environ 1,4 milliards de personnes[51] à qui cette formalité préalable à l'entrée sur le territoire s'appliquera. Ce champ d'application est inédit car

---

[44] Sénat, Comptes rendus de la Commission des affaires européennes, « Audition de Mme Agnès Diallo, directrice exécutive de 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 (eu-LISA) » , 13 juillet 2023, https://www.senat.fr/compte-rendu-commissions/20230710/euros.html#toc8.

[45] MARIN, Luisa, « The Cooperation Between Frontex and Third Countries in Information Sharing: Practices, Law and Challenges in Externalizing Border Control Functions », *European Public Law,* vol 26, n°1, 2020, p.157-180.

[46] Règlement (CE) n°539/2001 du Conseil du 15 mars 2001 fixant la liste des pays tiers dont les ressortissants sont soumis à l'obligation de visa pour franchir les frontières extérieures des États membres et la liste de ceux dont les ressortissants sont exemptés de cette obligation

[47] Voir Annexe 3.

[48] Sénat, réponse du Ministère de l'Europe et des affaires étrangères publiée à la question écrite n°02657 de M. LECONTE Jean-Yves (sénateur des Français établis hors de France - SER), 11 mai 2023 (consulté le 20 février 2024 à 10h20). https://www.senat.fr/questions/base/2022/qSEQ220902657.html.

[49] Article 2 §2 du règlement 2018/1240 (ETIAS).

[50] Directive 2004/38/CE du Parlement européen et du Conseil relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) n° 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE, *JOUE* L 158/77.

[51] CESE, « Avis sur la proposition de règlement du Parlement européen et du Conseil ETIAS », 2017/C 246/28, p.2

aucun système d'information ne permettait jusqu'alors de cibler spécifiquement les voyageurs exemptés de visa.

6. *La mise en œuvre automatisée d'ETIAS*

Le système ETIAS consiste à délivrer une autorisation préalable de voyage accordée après un examen automatisé d'une demande. Cette autorisation sera un préalable nécessaire à l'entrée sur le territoire européen. Elle sera vérifiée en amont par les transporteurs aériens, maritimes, et autoroutiers[52], qui porteront, en cas de refus à l'entrée, la charge du retour du ressortissant étranger[53]. La demande devra être formulée en amont par les ressortissants étrangers de pays exemptés de visa désireux de voyager dans l'espace de sécurité, justice, liberté. Cette nouvelle exigence permet donc aux autorités européennes de cibler une catégorie de voyageurs qui était jusqu'à présent exemptée de telles formalités pour arriver sur le sol européen. Le système n'est ainsi pas seulement une nouvelle base de données européenne; il représente une étape cruciale dans la logique d'intégration de la politique migratoire et modifie en profondeur les voies d'accès au territoire européen[54].

Concrètement, les demandeurs d'autorisation devront remplir un formulaire sur un site hébergeur créé par EU-Lisa où leur seront demandées différentes informations (âge, sexe, nationalité, validité de passeport, etc.). Les demandeurs âgés de plus de 18 ans et moins de 70 ans devront ensuite s'acquitter du montant de 7 euros[55]. Les données seront ensuite collectées puis examinées par le logiciel mis en place par EU-Lisa. Celui-ci cherchera à vérifier s'il n'y a pas d'interférence entre la « liste de surveillance »[56] d'ETIAS tenue par Europol ainsi que les États membres et les règles de filtrage[57] établies par Frontex suivant les indicateurs de risques définis par un acte délégué de la Commission[58]. S'il n'y a pas de réponse positive à la suite de l'examen des informations remplies par le demandeur, alors celui-ci recevra une autorisation de voyage valable pour une durée n'excédant pas 90 jours sur une période de 180 jours[59]. Au contraire, si le logiciel rencontre une interférence entre les règles d'examen et les informations remplies par le demandeur, la demande

---

[52] Article 45 §1 du règlement 2018/1240 (ETIAS).

[53] Article 45 §8 du règlement 2018/1240 (ETIAS).

[54] MICHÉA, Frédérique, ROUSVOAL, Laurent, European Papers, « The Criminal Procedure Out of Itself: A Case Study of the Relationship Between EU Law and Criminal Procedure Using the ETIAS System », European Papers, Vol. 6, 2021, No 1, p.475-476.

[55] Article 18 du règlement 2018/1240 (ETIAS).

[56] Article 34 du règlement 2018/1240 (ETIAS).

[57] Article 33 du règlement 2018/1240 (ETIAS).

[58] Article 89 du règlement 2018/1240 (ETIAS).

[59] Article 44 du règlement 2018/1240 (ETIAS)

sera envoyée à l'Unité Nationale d'ETIAS - en France, il s'agit du Service National des Enquêtes d'Autorisation de Voyage[60] (SNEAV) au sein de la direction générale de la Police Nationale - responsable pour traiter manuellement la demande. En cas de doutes, l'Unité Nationale peut demander au demandeur de renseigner des informations complémentaires, de faire parvenir des documents justificatifs, voire de passer un entretien dans un consulat ou en visioconférence[61].

Si l'autorisation de voyage octroyée par EU-Lisa après l'examen de la demande d'un ressortissant étranger est décrite comme un « sésame »[62], elle ne constitue pas pour autant une garantie pour entrer sur le territoire européen. En effet, comme il est précisé dans le règlement, il s'agit d'une condition préalable à remplir avant d'entrer sur le sol européen. Ces autorisations de voyage devront être présentées avant la frontière, que ce soit dans les aéroports, les ports maritimes, les gares etc. Le règlement conserve la possibilité pour les gardes-frontières de refuser l'entrée à un ressortissant étranger exempté de visa.

III. La qualification juridique de l'algorithme ETIAS : l'utilisation présumée de l'intelligence artificielle

Si les algorithmes utilisés par ETIAS semblent entrer dans la définition large qui est donnée à l'IA, la question de l'utilisation d'IA dans ETIAS n'est pas encore résolue et la qualification juridique de ces algorithmes demeure incertaine.

7. *La définition extensive de l'intelligence artificielle*

L'utilisation d'IA au sein du règlement ETIAS est incertaine. En effet, le règlement ETIAS prévoit un cadre pour la mise en place du système d'autorisation de voyage, mais ne précise à aucun moment la façon dont le logiciel ETIAS sera créé ni s'il disposera d'IA. De plus, le terme d'intelligence artificielle est flou et protéiforme, ce qui laisse planer le doute sur une possible qualification des algorithmes mis en place par ETIAS d'intelligence artificielle. Le terme d' « intelligence artificielle » utilisé pour la première fois en 1956, lors de la conférence de Dartmouth[63] s'est démocratisé à la fin

---

[60] Décret n° 2021-1138 du 1er septembre 2021 portant création d'un service à compétence nationale dénommé « service national des enquêtes d'autorisation de voyage », JORF n°0204.

[61] Article 27 du règlement 2018/1240 (ETIAS).

[62] CHASSIN, Catherine-Amélie, « Un nouveau venu numérique : l'ETIAS », *Cahier de la recherche sur les droits fondamentaux*, 2023, p.67.

[63] MCCARTHY, J., MINSKY, M. L., ROCHESTER, N., & SHANNON, C. E., « A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence », August 31, 1955. *AI Magazine*, *27*(4), p.12.

du XXème siècle, pour devenir une expression incontournable du XXIe siècle. Elle est définie par la Commission Nationale de l'Informatique et des Libertés (CNIL) comme un « procédé logique et automatisé reposant généralement sur un algorithme et en mesure de réaliser des tâches bien définies »[64]. Il convient dès lors de distinguer les « IA faibles » des « IA fortes »[65]. Les premières sont des systèmes conçus pour effectuer une tâche spécifique, et ne possèdent donc pas de compréhension ou de conscience au-delà de cette tâche. Les secondes au contraire sont capables de comprendre, d'apprendre, de s'adapter à l'image de l'intelligence humaine. Par exemple, lorsque l'on demande à ChatGpt de quel type d'IA il s'agit, celui-ci rétorque : « Je suis une IA faible (…) je ne possède pas de conscience, de compréhension profonde ou d'adaptabilité au-delà des capacités spécifiques pour lesquelles je suis programmé ».

La qualification juridique d'un algorithme d'intelligence artificielle reste un sujet complexe dont s'est récemment emparé le droit. En 2021, le Parlement et le Conseil adoptaient ensuite une première proposition de règlement : l'IA Act[66], un texte ambitieux visant à encadrer et à réguler l'utilisation de l'intelligence artificielle sur le territoire européen. Ce règlement définit l'intelligence artificielle comme « un système automatisé conçu pour fonctionner à différents niveaux d'autonomie, qui peut faire preuve d'une capacité d'adaptation après son déploiement et qui, pour des objectifs explicites ou implicites, déduit, à partir des données d'entrée qu'il reçoit, la manière de générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels »[67]. En 2024, le projet de convention cadre du Conseil de l'Europe[68] la définissait comme « un système informatique qui déduit, à partir des données qu'il reçoit et en fonction d'objectifs explicites ou implicites, comment générer des résultats tels que des prévisions, des contenus, des recommandations ou des décisions susceptibles d'influer sur des environnements matériels ou virtuels ». Ces définitions sont donc si large pour certains experts, que n'importe quel programme informatique pourrait être qualifié d'IA au yeux des régulations

---

[64] CNIL, « Intelligence artificielle », https://www.cnil.fr/fr/definition/intelligence-artificielle (consulté le 4 mai 2024 à 12h11).

[65] SAENZ, Aaron, « We Live in a Jungle of Artificial Intelligence that will Spawn Sentience », *SingularityHub,* 10 août 2010, https://singularityhub.com/2010/08/10/we-live-in-a-jungle-of-artificial-intelligence-that-will-spawn-sentience/ (consulté le 4 mai à 13h04)

[66] Résolution législative du Parlement européen du 13 mars 2024 sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), *JOUE* T9-0138/2024.

[67] Article 3 (1) projet de législation sur l'intelligence artificielle du 13 mars 2024 (IA Act).

[68] Conseil de l'Europe, Projet de convention cadre sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'Etat de droit, 15 mars 2024, Document CM(2024)52-prov1.

européennes[69]. Il y a donc une forte présomption que les algorithmes utilisés par ETIAS puissent être qualifiés d'IA.

8. *La place présumée de l'intelligence artificielle dans ETIAS*

Interrogée par un groupe de chercheurs de l'Université Libres de Bruxelles sur la nature des algorithmes utilisés, l'agence EU-Lisa chargée de développer l'infrastructure ETIAS répondait qu'ils ne pouvaient transmettre d'informations liées aux algorithmes car rendre ces informations publiques impliquerait que le public puisse « exercer une pression inutile sur le processus en cours et compromettre la conception et le développement du système ». L'agence Frontex chargée de mettre en œuvre les règles d'examen ETIAS affirmait quant à elle qu'il serait préférable de parler d'algorithme de filtrage que d'intelligence artificielle car les algorithmes utilisés ne sont pas dotés de capacité d'analyse sophistiquée ou de capacité d'apprentissage pouvant s'apparenter à de « l'intelligence »[70]. Un algorithme, qui est terme générique englobant une large acception, peut être défini comme une séquence de commandes permettant à un ordinateur de transformer une entrée en sortie. Les algorithmes utilisés par ETIAS seraient ainsi de simples lignes de code permettant de traiter les données et de vérifier l'existence d'interférence avec la liste de surveillance ETIAS et les facteurs de risque dressés par Frontex. Cette affirmation a toutefois été largement remise en question, notamment par un rapport du Parlement européen[71] ainsi que par la littérature existante[72]. En tous les cas, si le système ETIAS n'utilise pas encore de dispositifs IA dans son logiciel, celui-ci voue à en intégrer[73]. En effet, l'agence chargée de mettre en œuvre ETIAS a créé une groupe de travail sur l'IA, afin d' « explorer les possibilités, les avantages et les limites de l'utilisation de l'IA dans ses principaux systèmes comme ETIAS »[74]. Ainsi, lors d'un entretien[75] avec quatre cadres de l'agence EU-Lisa, ceux ci confirmaient l'intention de l'agence d'intégrer prochainement des mécanismes d'intelligence artificielle au système ETIAS « dans la mesure ou l'IA Act le permettrait ». D'après un

---

[69] EBERS, Martin et al., « The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS) », *J,* Vol. 4, p.589-591.

[70] DERAVE, Charly, GENICOT, Nathan, HETMANSKA, Nina. op. cit, p.21.

[71] Parlement Européen, L'intelligence artificielle aux frontières de l'Union européenne: aperçu des applications et questions clés, 2021, p.21.

[72] VAVOULA, Niovi, « Tr-AI-nsforming Migration, Asylum and Border Management in the EU : the Roles of the AI Act, Interoperable Large-scale IT Systems and EU Migration Agencies », Article soumis pour publication, 2024, p.1-33 ou VELASCO RICO, Clara Isabel, « ETIAS System and new proposals to advance the use of AI in public services », Article soumis pour publication, 2023, p.1-16.

[73] EU-Lisa, « Artificial Intelligence in the Operational Management of Large-scale IT systems », Research and Technology Monitoring Report, July 2020, p30.

[74] EU-Lisa, « Single Programming Document 2023-2025 », Document 2022–414 REV 1, p.16.

[75] Voir Annexe 1.

rapport non-publié d'EU-Lisa[76], quatre options pour l'utilisation d'IA sont envisagées afin d'améliorer le fonctionnement du système ETIAS et atteindre les objectifs de ce dernier. Ainsi, l'IA pourrait être mis en place au sein d'ETIAS: pour contrôler et valider l'évaluation des règles d'examen faites par les agents d'EU Lisa en générant des résultats prédictifs sur l'impact de ces règles (1), pour identifier des corrélations parmi les profils risqués (2), pour analyser ces corrélations et proposer des améliorations dans les indicateurs de risques (3) et pour aider au traitement manuel en cas de réponse positive de l'algorithme (4). Si l'utilisation d'IA au sein d'ETIAS est avérée, celle-ci devra être régulée pour protéger les risques qui en découlent.

9. *Les régulations pionnières de l'Union en matière d'intelligence artificielle*

L'effervescence qu'a connu l'IA au cours de ces dernières années[77], illustrés par la révolution Chatgpt, a générée d'importants questionnements juridiques sur cette innovation protéiforme porteuse d'opportunités et de risques[78] notamment pour la politique de migration et d'asile de l'Union[79]. Ainsi, face au gigantesque nombre de données récoltées grâce aux systèmes d'information à grande échelle, se pose la question du traitement de ces données par des intelligences artificielles et les dangers qu'ils représentent pour la protection des données[80]. En effet, les agences européennes font appel à des algorithmes de plus en plus avancés permettant de traiter rapidement et efficacement ces données[81].

Aussi, les institutions ont du faire face à la question de comment encadrer la révolution à venir des IA afin de permettre le développement de ces puissants algorithmes tout en protégeant les droits de l'homme et les libertés fondamentales. Dans sa communication du 8 avril 2019[82], la Commission européenne avait déclaré que l'Union souhaitait renforcer la confiance dans l'IA : "la confiance est une condition préalable pour garantir une approche de l'IA centrée sur l'humain : l'IA est […] un outil qui doit servir les personnes dans le but ultime d'accroître le bien-être humain". Cette communication

---

[76] EU-Lisa, « AI in CSSR in the content of ETIAS and the revised VUS final report », 2022, Document non publié (cité dans VAVOULA, Niovi, *op. cit*, p. 17).

[77] GÉLIN, Rodolphe, « Dernières nouvelles de l'Intelligence artificielle », Flammarion, Paris, 2022, 160p.

[78] Commission européenne, « Opportunities and Challenges for the Use of Artificial Intelligence in Border Control », Migration and Security. vol. 1: Main Report, written by Deloitte, May 2020.

[79] YANG, Yiran, ZUIDERVEEN BORGESIUS, Frederik, BECKERS, Pascal, BROUWER, Evelien, « Automated Decision-making and Artificial Intelligence at European Borders and Their Risks for Human Rights », Article en préparation v1, 2024, p.1.

[80] Parlement Européen, L'intelligence artificielle aux frontières de l'Union européenne: aperçu des applications et questions clés, 2021, p.4.

[81] BROM, Frans, BESTERS, Michiel, *op. cit.,* p.457.

[82] Commission européenne, « Building Trust in Human-Centric Artificial Intelligence » (Communication) COM (2019) 168 final 1, 8 avril 2019, 10p.

s'inscrivait dans le cadre plus large de la stratégie de l'Union européenne (UE) en matière d'IA[83], selon laquelle l'homme est au coeur des avancées technologiques, afin que le progrès bénéficie à l'ensemble de la société. Aussi, la Commission affirmait dans son livre blanc sur l'IA[84] son souhait de construire un « écosystème de confiance » autour de l'intelligence artificielle, pour que la révolution technologique en cours s'accompagne d'une forte protection des droits fondamentaux et que l'Union devienne « le fer de lance » du développement de « nouvelles normes ambitieuses »[85] en la matière. Ces souhaits formulés ont trouvé une assise juridique dans le projet IA Act et le projet de convention cadre sur l'intelligence artificielle, qui devraient s'appliquer dès leur mise en vigueur au règlement ETIAS. Il est dès lors intéressant d'analyser la place qu'occupe l'intelligence artificielle au sein d'ETIAS afin d'envisager les risques qui en découlent, mais aussi les garanties que l'on devrait y apporter. Il convient donc de s'interroger dans le cadre de ce mémoire :

Dans quelle mesure l'utilisation de l'intelligence artificielle dans la mise en œuvre du règlement ETIAS engendre-t-elle des risques pour les droits fondamentaux des voyageurs étrangers exemptés de visa et requiert donc une mise en conformité accrue avec les normes européennes visant à protéger ces droits ?

Pour permettre un meilleur contrôle des flux migratoires au sein de l'espace de liberté, sécurité et justice, EU-Lisa utilise et développe des algorithmes intelligents afin de filtrer les demandes d'autorisations de voyage des ressortissants étrangers exemptés de visa. L'utilisation systématique de ces algorithmes pour le profilage de ces voyageurs est décolérée des risques générés par les voyageurs étrangers et va donc à l'encontre du principe de proportionnalité (**Partie I**). Cette utilisation est dommageable pour les droits reconnus par la Charte des droits fondamentaux[86] comme le droit à la vie privée et à la protection des données ainsi que le droit à la non-discrimination qui sont menacés (**Partie II**). Ce danger est exacerbée par les garanties incomplètes prévues par le règlement ETIAS qui ont toutefois été complétées par les nouvelles régulations en matière d'intelligence artificielle avec lesquelles ETIAS devra se mettre prochainement en conformité (**Partie III**).

---

[83] Commission européenne, « Un plan coordonné dans le domaine de l'intelligence artificielle » (Communication) COM (2018) 795 final, 25 avril 2018, 10p.

[84] Commission européenne, « White paper on Artificial Intelligence – A European approach to excellence and trust » COM (2020) 65 final, 19 février 2020, 26p.

[85] Commission européenne, « Favoriser une approche européenne en matière d'intelligence artificielle » (Communication) COM (2021) 205 final 4, 21 avril 2021, 11p.

[86] Charte des droits fondamentaux de l'Union européenne, version consolidée du 7 juin 2016, *JOUE* C 202/389.

Partie I. Un système automatisé disproportionné en faveur de la sécurisation de la politique migratoire de l'Union européenne

Le règlement ETIAS, en ce qu'il permet la collecte et la manipulation de données sensibles par des algorithmes est critiqué par une partie des universitaires qui y voient un outil sécuritaire dangereux pour les droits fondamentaux. La mise en œuvre formelle (**Chapitre 1**) et matérielle (**Chapitre 2**) de cet outil est donc contestée.

Chapitre 1. La mise en œuvre formelle du règlement ETIAS : la proportionnalité contestée du nouveau système d'information

La justification lacunaire de la Commission sur les risques existants et des outils déjà existants pour la lutte contre les risques sécuritaires (**Section I**), est corroborée par la mise en œuvre de moyens excessivement disproportionnés dans la mise en œuvre du règlement (**Section II**).

Section I. La justification lacunaire de la nécessité d'un nouveau système d'information pour la politique d'immigration

La nécessité de mettre en œuvre un nouveau système d'information visant un public jusqu'à présent exempté de visa n'a pas été justifiée par la Commission qui aurait du démontrer que le règlement ETIAS permettait une réelle amélioration contre les risques que les voyageurs étrangers provoquent.

10. *Le manque de preuve sur les risques générés par les ressortissants étrangers exemptés de visa*

À ce jour, aucune étude ne permet de démontrer un lien de causalité entre les flux migratoires provenant de pays exemptés de visa et un faible niveau de sécurité[87], Europol allant même jusqu'à affirmer dans une étude qu'il n'existe « aucun lien documenté entre l'immigration et le terrorisme »[88]. La mise en œuvre du règlement ETIAS s'explique avant tout par la volonté de

[87] VAVOULA, Niovi, « 'You (probably) Are Who I Say You Are' - ETIAS and the Fourfold Paradigm Shift in the Operationalisation of Information Systems » in Vavoula (dir) *Immigration and Privacy in the Law of the EU*, 2022, p.512.

[88] Europol, « European Union Terrorism Situation and Trend Report 2016 », 2016, p.7.

« réguler par les risques »[89]. Les voyageurs exemptés de visa sont ainsi désormais perçus comme des « suspects » qui devront prouver leur « bonne foi »[90] pour voyager sur le sol européen.

Pour justifier la nécessité d'adopter un tel règlement, la Commission soulignait l'existence d'un véritable « écart d'information »[91] entre les voyageurs provenant de pays-exemptés de visa et ceux provenant d'autres pays tiers. Cette analyse était exacerbée par les prévisions du nombre de voyageurs issus de pays exemptés de visa passant de 30 millions en 2014 à 39 millions en 2020[92]. La Commission ne relevait donc nullement l'existence d'un lien concret entre la hausse du nombre de voyageurs et le risque sécuritaire qui en découle. La nécessité de mettre en œuvre ETIAS se fondait également sur le fait que « des pays comme les États-Unis, le Canada et l'Australie utilisent déjà des systèmes similaires et les considèrent comme un élément essentiel de leur dispositif de sécurité et qu'en conséquence, beaucoup d'européens sont désormais familiers avec ces systèmes »[93].

Dans une étude pour la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement Européen[94], les professeurs Niovi Vavoula et Julien Jeandesboz rétorquaient que l'Australie, le Canada et les États-Unis n'étant pas soumis aux droits et libertés fondamentales reconnues par l'Union européenne, ni l'argument sur l'existence de tels systèmes dans d'autres pays, ni la familiarité présumée des européens avec ces systèmes ne pouvaient être légitiment reçus pour justifier la nécessité du règlement. Les auteurs appelaient ainsi à une révision du texte pour clarifier et préciser exactement à quelles fins les données collectées peuvent être utilisées ou réutilisées par ETIAS et les autres règlements du système d'interopérabilité à grande échelle.

11. *L'existence préliminaire de textes normatifs aux objectifs analogues*

La nécessité du règlement ETIAS a été largement contestée puisqu'il existait déjà des textes permettant de lutter contre les risques générés par les ressortissants étrangers. En effet, le règlement est particulièrement redondant avec le règlement EES qui vise également à contrôler les flux migratoires des voyageurs étrangers. Ainsi, EES, voté en 2017 et qui devrait entrer en vigueur en

---

[89] LATIL, Arnaud, « Le droit du numérique : une approche par les risques », *Lefebvre-Dalloz*, Paris, 2023.

[90] DERAVE, Charly, GENICOT, Nathan, HETMANSKA, Nina. *op. cit.* p. 27.

[91] Commission européenne, 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) n° 515/2014, (UE) 2016/399, (UE) 2016/794 et (UE) 2016/1624, COM (2016), 731 final, p. 2.

[92] *Ibid*.

[93] *Ibid*. spéc. p. 3.

[94] VAVOULA, Niovi, JEANDESBOZ, Julien, ALEGRE, Susie, « European Travel and Authorisation System (ETIAS) : Boarder management, fundamental rights and data protection », Étude pour la Commission des libertés civiles, de la justice et des affaires intérieures du parlement européen (LIBE), p.45.

octobre 2024, enregistrera le franchissement des frontières à l'entrée et à la sortie de tous les ressortissants de pays tiers admis pour un court séjour, y compris les ressortissants étrangers exemptés de visa[95]. Le texte vise tout comme ETIAS à prévenir et détecter des infractions terroristes ou d'autres infractions pénales graves en enregistrant des données alphanumériques liées au voyage des ressortissants étrangers comme la date, le lieu de franchissement des frontières, la durée du séjour ainsi que l'âge, le sexe et la nationalité[96]. Il prévoit également de collecter des données biométriques comme les empreintes digitales ou l'image faciale[97]. L'interopérabilité[98] entre les deux systèmes d'information, ainsi que le processus automatisé visant pour EES à compléter une fiche ETIAS[99], permettra la tenue d'un catalogue massif de données de ressortissants de pays tiers et la constitution d'un puissant outil de surveillance animé par la logique de la prévention des risques liés à l'immigration. Au vu de l'existence préalable d'un outil comme l'EES qui permet de collecter et de stocker des données relatives aux ressortissants étrangers, la nécessité d'adopter le règlement ETIAS est contestée.

De surcroît, deux autres directives précédant ETIAS permettent également de pallier les risques potentiels de l'immigration clandestine et de sécurité liés aux voyageurs étrangers exemptés de visa. En effet, la directive Advance Passenger Information (API)[100] adoptée le 29 avril 2004 prévoit d' « améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine, au moyen de la transmission préalable aux autorités nationales compétentes, par les transporteurs, de données relatives aux passagers »[101]. La directive Passenger Name Record (PNR)[102] adoptée le 27 avril 2016 prévoit quant à elle la collecte, le traitement et la conservation de données de passagers aériens des vols hors-UE et intra-UE à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité[103]. Le système API-PNR est géré par les « Unités Information Passagers » (UIP) dans chaque État membre[104], rattachée en France au ministère chargé des douanes,

---

95 Article 2 §1 (a) du Règlement 2017/2226.

96 Article 16 §1 du règlement 2017/2226 (EES).

97 Article 17 §1 b) et c) du règlement 2017/2226 (EES).

98 Article 8ter du règlement 2017/2226 (EES).

99 Article 8bis du règlement 2017/2226 (EES).

100 Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, *JOUE* L 261/24.

101 Article 1 de la directive 2004/82 (API).

102 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *JOUE* L 119/132.

103 Article 1 de la directive 2016/681 (EES).

104 Article 4 de la directive 2016/681 (PNR).

et rassemblent les informations transmises par les compagnies aériennes[105]. Ces unités sont ensuite chargées du traitement automatisé des données PNR en les confrontant « aux bases de données utiles aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité »[106].

Ces deux directives, qui s'appliquent à tous les passagers aériens, sont intégrées au cadre d'interopérabilité des bases de données[107]. Elles permettent donc, au même titre qu'ETIAS, de prévenir et contrôler les risques liés aux voyageurs entrants sur le sol européen[108]. Dans son étude sur la faisabilité du règlement ETIAS[109], la Commission relevait déjà l'existence d'API et PNR qui s'appliquent aux voyageurs étrangers exemptés de visa, soulignant que 84 % des voyages réalisés par des ressortissants étrangers aux frontières de l'Union le seraient par voie aérienne en 2025, soit 107 millions de voyages estimés. Ces directives ne traitent donc pas les données des seuls 16 % de voyageurs par voie terrestre (7 %) et maritime (9 %). Ayant constaté que ces directives s'appliquaient déjà aux voyageurs aériens, le règlement ETIAS aurait pu ne cibler que les voyages par voie terrestre et maritime, qui constituent par ailleurs la majorité des cas de refus à l'entrée[110]. Un tel champs d'application aurait permis d'éviter une réitération de la collecte de données personnelles des voyageurs étrangers, ce qui aurait rendu l'outil plus proportionnel à la conduite de ses objectifs. Si la nécessité de l'instauration du règlement ETIAS est donc encore à prouver, les outils mis en œuvre pour la réalisation de ses objectifs semblent également excessivement disproportionnés.

Section II. La proportionnalité contestée de la mise en œuvre du règlement ETIAS face aux risques

Outre la nécessité du système d'information, sa proportionnalité est contestée puisque ce dernier utilise des outils excessivement dangereux pour lutter contre des risques multiples et mal définis.

---

[105] CNIL, Le système API-PNR, que contient-il ?, https://www.cnil.fr/fr/cnil-direct/question/le-systeme-api-pnr-que-contient-il (consulté le 5 mai 2024 à 13h33).

[106] Article 6 §3 de la directive 2016/681 (PNR).

[107] DUMBRAVA, Costica, « Advance passenger information (API) to enhance border checks », The 'EU Legislation in Progress' Briefing, 2023, p.1-6.

[108] VAVOULA, Niovi, JEANDESBOZ, Julien, ALEGRE, Susie, *op. cit.*, p.44 ; PRIMORAC Zeljka, BOZENA, Bulum, PIJACA, Marija, « New European approach on passengers' digital surveillance through electronic platform (ETIAS) - Passengers' and carriers' perspective », *EU and comparative law issues and challenges series (ECLIC)*, p. 275-276.

[109] PwC, « Feasibility Study for a European Travel Information and Authorisation System (ETIAS) », Final Report, 16 novembre 2016, p.10.

[110] Ibid. p.9.

12. *L'utilisation disproportionnée de l'IA par ETIAS*

En vertu du principe de proportionnalité, des limitations des droits et libertés ne doivent être imposées que « si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui »[111]. La Cour de Justice est allée plus loin en affirmant que toute dérogation à la protection des données personnelles ne devait s'appliquer que « dans la mesure où cela est strictement nécessaire »[112]. La Commission affirmait ainsi en 2011[113] que « la contribution potentielle au renforcement de la sécurité des États membres ne pouvait justifier la collecte de données à caractère personnel à une telle échelle, ni le coût financier et l'impact sur les relations internationales ».

La création d'une demande d'autorisation de voyage préalable, qui collecte les données des voyageurs constitue une atteinte à la vie privée et la protection des données des voyageurs. Le spectre des données collectées est par ailleurs très important et constitue donc un réel danger pour les droits des voyageurs. La nécessité d'obtenir la multitudes de données collectées n'a toutefois pas été justifiée par la Commission européenne. Le nombre de données requises pourrait toutefois encore augmenter. En effet, la Commission a envisagé, dans un projet d'acte délégué, de demander davantage de données personnelles relatives aux membres de la famille, incluant les enfants, les grands-parents ou les amis, ce qui a été jugé particulièrement excessif par le Comité Européen de Protection des Données (CEPD)[114]. Cette autorisation de voyage constitue également aussi un alourdissement des démarches administratives pour voyager et entrer sur le sol européen. Celui-ci s'appliquera à 1,4 milliard de personnes originaires d'une soixantaine de pays, et aura donc aucun doute des conséquences diplomatiques mais aussi économiques et sociales pour de nombreux secteurs comme la mobilité professionnelle, la mobilité étudiante et universitaire ou le tourisme[115]. L'absence d'étude permettant de mesurer l'impact du règlement a d'ailleurs été soulignée par le Contrôleur européen de la protection des données[116], alors même que les « Better Regulation Guidelines » de 2015 imposent à la Commission d'établir des études pour mesurer l'impact d'« une initiative qui aura probablement des conséquences économiques, environnementales et sociales

---

[111] Article 52.1 de la Charte des Droits Fondamentaux de l'Union Européenne.

[112] Affaires jointes du 21 décembre 2016, C-203/15 Tele2 *Sverige AB v Post-och telestyrelsen* and others, *C-698/15 Secretary of State for the Home Department v Tom Watson and others*.

[113] Commission européenne, 2011, *op. cit.*, p. 7.

[114] CEPD, « Observations formelles du CEPD sur le projet de décision déléguée de la Commission visant à préciser le contenu et la forme des questions et à définir l'autre ensemble préétabli de questions », 3 août 2022, p.4.

[115] CESE, *op. cit.*, p.2-3.

[116] CEPD, 2017, *op. cit*., p.7.

significatives »[117]. Ce manque d'évaluation constitue une lacune importante qui remet en cause la proportionnalité du règlement.

La proportionnalité d'un tel texte est d'autant plus contestée que le système ETIAS utilise un mécanisme de décision automatisée, dont la question de s'avoir s'il devrait être qualifié d'intelligence artificielle n'est pas résolue, mais sa réponse fortement présumée[118]. L'utilisation d'un tel dispositif dans la politique d'immigration et d'asile est une nouveauté. En effet, la politique d'attribution des visas ne dispose pas d'algorithme d'aide à la décision, bien que cela ait déjà été proposé[119]. Compte tenu des interférences graves avec les risques fondamentaux que cela provoque, la régulation devrait répondre au critère de ce qui est strictement nécessaire dans une société démocratique[120]. Le CEPD soulignait ainsi qu'étant donné l'existence d'une liste de surveillance tenue par le règlement ETIAS, il n'y a pas d'éléments convaincants permettant d'attester la nécessité d'utiliser les outils de profilages prévues par ETIAS[121] qui pourtant portent atteinte aux droits fondamentaux. Le CEPD affirmait ainsi qu'il « n'est pas convaincu que la proposition prévoit des garanties (…) et qu'elle assure un niveau suffisant de protection des droits fondamentaux »[122]. Cela est d'autant plus problématique que le développement d'un tel outil numérique a nécessité l'investissement de plusieurs milliards d'euros[123].

L'utilisation de l'IA est donc disproportionnée et excessive, ce à qui s'ajoute au fait que le règlement ne revêt pas de finalités précises et suffisamment définies.

13. *La lutte contre différents risques décloisonnés*

Le système ETIAS prévoit de lutter contre des risques de nature très différentes et dont la définition est floue. En effet, le système a vocation à estimer si la présence de « ressortissants de pays tiers sur le territoire des États membres est susceptible de présenter un risque en matière de sécurité ou

---

[117] Commission européenne, « Staff Working Document: Better Regulation Guidelines », SWD (2015) 111 final, spéc. p.16.

[118] GUGLIOTTA, Lorenzo, ELBI, ABDULLAH, « Will AI 'subtly' take over decision-making in the EU migration context? Warnings and lessons from ETIAS and VIS », *2023 EULEN Conference on AI Systems and Enforcement: Between Effectiveness and the Rule of Law,* 2023, p.10-12.

[119] France Diplomatie « Propositions pour une amélioration de la délivrance des visas », Rapport Paul Hermelin, Mission Visas, Avril 2023, p32.

[120] GANDHI, Shrutika, *op. cit.*, p.8.

[121] CEPD, *op. cit.* p. 13

[122] *Ibid*.

[123] EU-Lisa, 2022, *op, cit.*, p.38.

d'immigration illégale ou un risque épidémique élevé »[124]. L'association de ces risques peut surprendre en ce qu'elle implique de récolter des informations personnelles très différentes (documents de voyage, nationalité, santé, etc.) qui seront traitées au sein du même système pour différentes fins[125]. Il existe donc un risque important que les données initialement collectées pour lutter contre les risques épidémiques le soit *in fine* pour lutter contre un risque sécuritaire ou d'immigration illégale et *vice versa*.

Ces préoccupations grandissantes ont été formulées par le Rapporteur spécial des Nations Unies qui soulignait dans un rapport[126] rendu en 2017 « [qu'il] est de plus en plus fréquent que les données personnelles se retrouvent mélangées à des données qui peuvent être utilisées et réutilisées à diverses fins, connues ou inconnues, ce qui soulève de graves questions, notamment pour ce qui est des critères appliqués pour collecter, stocker, analyser et, enfin, supprimer des données ». La collecte et le traitement de ces données diverses au sein d'un outil administratif de contrôle migratoire cacherait ainsi une forte dimension sécuritaire et criminelle[127]. En effet, les données collectées à des fins migratoires sont en l'espèce rendus accessibles aux autorités à des fins répressives, conduisant à une confusion des objectifs du règlement[128]. Ceux-ci sont pourtant difficilement conciliables : la lutte contre les risques sanitaires et sécuritaires, par exemple, étant fortement distincts. Cette confusion des objectifs s'analyse à travers la double nature que revêt le règlement : la création d'un outil migratoire pour contrôler administrativement les flux de ressortissants étrangers, mais aussi l'établissement d'un système de surveillance sécuritaire[129]. Le CEPD soulevait pourtant que la lutte contre l'immigration et contre l'insécurité sont deux objectifs d'ordre public différents qu'il faut traiter respectivement de façon cloisonnée[130]. En effet, en vertu d'une règle que les économistes connaissent bien[131], un instrument politique ne doit servir à atteindre qu'un seul objectif spécifique.

---

[124] Article 1 du règlement 2018/1240 (ETIAS). Il est d'ailleurs intéressant de noter que la volonté de l'Union de lutter contre les risques épidemiques est intervenu avant la survenue de l'épidémie de COVID-19.

[125] GAZIN, Fabienne, « Le développement de la "biométrisation" des migrants dans l'Union européenne : au mépris du principe de finalité et au service de la lutte contre l'immigration irrégulière », in Frédérique Berrod (dir) *Europe(s), droit(s) européen(s) : une passion d'universitaire*, Bruxelles, Bruylant, 2015, p. 209-221.

[126] Assemblée générale des Nations Unies, Rapport du Rapporteur spécial sur le droit à la vie privée, A/HRC/34/60, 6 septembre 2017.

[127] MICHÉA, Frédérique, ROUSVOAL, Laurent, *op. cit.*, p.474.

[128] VAVOULA, Niovi, « Consultation of EU Immigration Databases for Law Enforcement Purposes », *op. cit*. p.145.

[129] MICHÉA, Frédérique, ROUSVOAL, Laurent, *op. cit.* p.476.

[130] CEPD, « Avis 3/2017 du CEPD sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) », 6 mars 2017, p.9.

[131] Le théorème de Tinbergen ou « principe de cohérence » dans TINBERGEN, Jan, Techniques modernes de la politique économique, Paris, Dunod, 1961, 250p.

Il aurait donc été préférable que ETIAS se concentre sur un objectif afin de ne pas augmenter le risque d'interférence avec les droits fondamentaux.

La définition large des risques doit également être questionnée. Le règlement vise à lutter contre le terrorisme, l'immigration irrégulière ou les épidémies[132], mais ne précise pas précisément ce que sont ces menaces. Un tel flou autour de certaines notions comme le terrorisme implique d'associer des personnes à un risque terroriste, comme les manifestants Hongkongais qualifiés par la Chine de « terroristes » ou les défenseurs du président non-reconnu Juan Guaido au Vénézuela[133], au même titre que d'individus réellement dangereux pour l'Europe. Cette association est particulièrement préoccupante au regard de la grande nécessité pour ces personnes persécutées d' exercer leur droit d'asile sur le sol européen. Cette préoccupation va de pair avec la qualification des zones de guerre et de conflit par la Commission. Cette dernière a dressé une liste de 45 pays tiers désignés comme étant des « zones de guerre et de conflit »[134] dont certains pays, comme la Chine ou la Turquie ont par ailleurs conclu des accords de partenariat avec l'UE. La définition extensive du terrorisme ou des conflits risque de mener à un traitement malvenu de l'algorithme qui ne pourra saisir les subtilités des situations personnelles des voyageurs[135].

Chapitre 2. La mise en œuvre matérielle du règlement ETIAS : l'automatisation préoccupante de l'examen des demandes d'autorisation de voyage

Matériellement, le règlement ETIAS se concrétise par un logiciel permettant d'évaluer les risques perçus d'une demande d'autorisation de voyage et de les comparer aux règles d'examen du système (**I**). Cette comparaison est menée par un algorithme qui débouche sur une décision automatisée pouvant être réexaminée manuellement (**II**).

---

[132] CRASSEGGER Céline, « Comment l'Union européenne fait-elle face aux défis que représente la lutte contre le terrorisme et la radicalisation ? », *Cahiers de la sécurité et de la justice*, 2022, p. 86-87.

[133] GUILD, Elspeth, VAVOULA, Niovi, « Travel Authorization in the EU : Automated Processing and Profiling », *Open Democracy,* 12 octobre 2020, <https://www.opendemocracy.net/en/can-europe-make-it/travel-authorization-eu-automated-processing-and-profiling/>(consulté le 9 mai 2024 à 22h47)

[134] Décision déléguée (UE) 2023/2424 de la Commission du 28 juillet 2023 précisant le contenu et la forme des questions et définissant l'autre ensemble préétabli de questions pour le système européen d'information et d'autorisation concernant les voyages (ETIAS) conformément à l'article 17, paragraphes 5 et 6, du règlement (UE) 2018/1240 du Parlement européen et du Conseil, *JOUE* C/2023/4972, spéc. Annexe II.

[135] Comité Européen de la Protection des Données, « Observations formelles sur le projet de décision déléguée de la Commission visant à préciser les risques en matière de sécurité ou d'immigration illégale ou le risque épidémique élevé », 7 juin 2021, p.2.

Section I. L'évaluation automatisée des demandes d'autorisation de voyage

L'algorithme ETIAS fonctionne en évaluant les demandes d'autorisation de voyage sous la forme d'un profilage dont le profil est ensuite comparé aux règles d'examen établies par l'unité centrale du système.

14. *L'évaluation des risques sur la base des données personnelles transmises*

Pour octroyer les autorisations de voyage, ETIAS prévoit d'apprécier les différents risques que pourraient causer les voyageurs exemptés de visa. Ces risques seront ensuite comparés aux « règles d'examen » du règlement qui déterminent si le demandeur pourra recevoir une autorisation de voyage. En effet, les règles d'examen ETIAS « prennent la forme d'un algorithme permettant un profilage (…) par la comparaison (…) entre les données enregistrées dans un dossier de demande du système central ETIAS et les indicateurs de risques spécifiques établis par l'unité centrale ETIAS »[136]. Les profils des demandeurs d'autorisation de voyage seront établis par le traitement des données personnelles transmises par les voyageurs.

Ainsi, en remplissant le formulaire numérique sur le site internet pour les demandes d'autorisation de voyage, les demandeurs devront transmettre les données suivantes[137] : leur nom(s), prénom(s), date de naissance, lieu de naissance, sexe, nationalité(s), adresse du domicile, adresse électronique, numéro de téléphone, niveau d'études, profession actuelle, l'adresse du premier séjour envisagé, le prénom(s) et le pays de naissance des parents, le type de document de voyage, le numéro et le pays de délivrance du document, la date de délivrance et d'expiration du document. L'adresse IP du demandeur sera également relevée. Par ailleurs, le demandeur devra répondre aux questions de savoir « s'il a été condamné au cours des vingt-cinq dernières années pour infraction terroriste ou au cours des quinze dernières années pour une autre infraction pénale mentionnée dans la liste (…); s'il a séjourné dans une zone de guerre ou de conflit particulière au cours des dix années précédentes, en précisant les raisons du séjour; s'il a fait l'objet d'un ordre de quitter le territoire d'un État membre (…) ou d'une décision de retour au cours des dix dernières années ». S'il répond par la positive à une de ces questions, une nouvelle liste de questions avec des réponses préétablies que la Commission doit adopter par acte délégué[138] lui seront alors posées. Une fois la collecte de données effectuées,

---

[136] Article 33 du règlement 2018/1240 (ETIAS).

[137] Article 17 du règlement 2018/1240 (ETIAS).

[138] Article 89 du règlement 2018/1240 (ETIAS).

l'algorithme traite celle-ci puis compare le profil du demandeur aux règles de filtrages établies par EU-Lisa.

15. *La conception de règles d'examen par l'Unité Centrale ETIAS*

Les règles d'examen sont conçues par un algorithme sur la base d'une combinaison de données résultant d'un calcul statistique complexe. Celui-ci compare les indicateurs de risques spécifiques et les données transmises par le demandeur. Les indicateurs de risques sont précisés par la Commission via un acte délégué, sur la base de nombreuses données[139] fournies par les États membres et des organisations internationales comme l'OMS, mais aussi de statistiques générées par EES indiquant des taux anormaux de durée de séjour ou d'ETIAS et VIS indiquant des taux anormaux de refus d'autorisation de voyage. Regroupés au sein du CRRS, ces statistiques pourront être traitées par des outils d'intelligents afin d'améliorer la conception des indicateurs de risques en identifiant plus précisément les caractéristiques des individus qui doivent être associés à des risques[140] (le fait d'être jeune, de ne pas avoir d'emploi, d'être issu d'un pays pauvre etc.).

Là encore, l'amplitude de l'utilisation d'IA pour déterminer les risques est inconnue, mais de nombreux indices comme la feuille de route d'EU-Lisa pour 2023-2025 ou l'étude de la Commission européenne sur les opportunités liés à l'IA[141] mentionnent explicitement les possibilités d'inclure des modèles automatisés d'apprentissage en profondeur (« deep learning ») dans la mise en œuvre de l'algorithme ETIAS.

À partir de ces indicateurs risques, l'unité centrale ETIAS établit une « grille d'analyse »[142] qui comprend les risques spécifiques, adoptés par acte d'exécution, sur la base de l'âge, le sexe, la nationalité, le pays et la ville de résidence, le niveau d'études et la profession actuelle[143]. Cette grille d'analyse va permettre à l'algorithme de donner une réponse positive ou négative à la demande d'autorisation de voyage. L'algorithme ETIAS s'auto-nourrit ensuite des données qu'il produit. Ainsi, s'il refuse souvent un certain type de profil avec des caractéristiques communes - la donnée taux anormaux de refus d'autorisation de voyage - celui-ci va intégrer cette statistique qui conduira dès lors à un refus encore plus systématique de ces profils, malgré la singularité de chaque voyageurs.

---

[139] Article 33 §2 du règlement 2018/1240 (ETIAS).

[140] EU-Lisa, 2022, *op. cit.*, p.73

[141] Commission européenne, « Opportunities and Challenges for the Use of Artificial Intelligence in Border Control », *op. cit.*

[142] CHASSIN, Catherine-Amélie, *op. cit.*, p.69.

[143] Article 33 §4 du règlement 2018/1240 (ETIAS).

Section II. L'évaluation excessivement automatisée de la conformité des demandes d'autorisations de voyage

Cet examen automatisée des demandes ETIAS est particulièrement excessive car le traitement par un algorithme des demandes pour les comparer aux règles de filtrage est insuffisamment suppléée par un humain.

16. *La recherche de correspondances entre le profil des demandeurs et les règles d'examen*

Afin d'octroyer les autorisations de voyage aux demandeurs, l'algorithme ETIAS va chercher des correspondances entre les données du demandeur et les règles d'examen. L'examen des demandes est un processus minutieux qui implique la comparaison des données du demandeur avec les indicateurs de risques établis par la Commission européenne sur la base des calculs d'ETIAS, mais aussi la consultation sur l'ESP des systèmes d'information SIS II, EES, VIS II, Eurodac, ECRIS-TCN et des bases de données d'INTERPOL Stolen and Lost Travel Document (STLD) et Travel Document Associated with Notices (TDAWN)[144] et d'une liste de surveillance propre à ETIAS[145].

L'algorithme va donc rechercher si le demandeur n'a pas été signalé dans une autre base de données, et si son document de voyage n'a pas été signalé dans un registre comme le VIS, le STLD ou le TDAWN. Il va également vérifier que le demandeur n'est pas inscrit sur sa liste de surveillance ETIAS. Cette dernière se compose de « données relative à des personnes soupçonnées d'avoir commis une infraction terroriste ou une autre infraction pénale grave (…) ou à des personnes pour lesquelles il existe des indices concrets ou des motifs raisonnables permettant de croire (…) qu'elle commettront une infraction terroriste ou une infraction pénale grave »[146]. Cette liste est tenue par Euopol et peut être alimentée par l'unité centrale ETIAS et les États membres. Une autorisation de voyage est délivrée lorsque'à la suite de l'examen, l'algorithme indique qu'il n'y a « aucun indice concret ni aucun motif raisonnable (…) permettant de conclure que la présence de la personne sur le territoire des États membres présente un risque »[147].

En cas de réponse négative à l'examen de la demande, c'est-à-dire si ETIAS ne trouve aucune correspondance entre les règles d'examen et les données du demandeur, une autorisation de voyage

---

144 Article 20 §2 du règlement 2018/1240 (ETIAS).

145 Article 34 du règlement 2018/1240 (ETIAS).

146 *Ibid*.

147 Article 36 du règlement 2018/1240 (ETIAS).

sera délivrée avec laquelle le voyageur devra se présenter aux frontières de l'Union. Dans la majorité des cas, ETIAS impliquera une prise de décision automatisée dans laquelle une autorisation de voyage sera délivrée automatiquement, sans participation humaine au processus d'examen. Toutefois, en cas de réponse positive à l'examen de la demande, celle-ci sera transmise à l'unité nationale chargée de réexaminer manuellement la demande. La réévaluation de la demande est alors censée préserver les droits fondamentaux et intérêts légitimes du demandeur en éliminant les biais et erreurs de l'algorithme, grâce à l'examen par un humain de la demande, ce qui ne semble pas garanti en l'état.

17. *Le traitement manuel subsidiaire insuffisant de la demande ETIAS*

Lorsque le traitement automatisé conduit à une réponse positive sur la correspondance des données les bases de données européennes consultées par ETIAS, la demande est transférée aux unités nationales créées par les États membres. Le système central envoie alors une notification à l'unité nationale de l'État membre responsable, qui est celui qui a introduit ou fournit les données ayant déclenché la réponse positive par l'algorithme[148]. Si plusieurs États membres ont introduit des données; c'est celui qui les a fournies le plus récemment qui est déclaré responsable. L'unité nationale est alors chargée du réexamen de la demande. Elle a un accès direct aux systèmes d'information de l'UE ainsi qu'aux casiers judiciaire nationaux et aux données transmises par le demandeur[149]. L'unité nationale procède alors à une réévaluation des risques générés par le demandeur dans les 4 jours suivant la transmission du dossier. En cas de doutes ou d'éléments manquants, elle peut être amenée à lui poser de nouvelles questions et à demander des documents justificatifs (certificat médical, attestation de participation à une association, etc.), ce qui peut allonger le délai de réponse jusqu'à 30 jours. Lorsque des doutes subsistent encore, l'unité nationale dispose de la possibilité de proposer un entretien, dans un consulat situé à moins de 500 kilomètres de la résidence du demandeur, ou à défaut via des moyens de communication audiovisuels à distance[150]. Si l'intéressé ne répond pas à la demande d'information complémentaire ou ne se présente pas à l'entretien, celui-ci verra sa demande rejetée. Si celui-ci répond, l'unité nationale délivre ou refuse l'autorisation de voyage à l'issue de l'évaluation humaine[151]. Ce réexamen est

[148] Article 25 du règlement 2018/1240 (ETIAS).

[149] Article 25bis du règlement 2018/1240 (ETIAS).

[150] Article 27 §4 du règlement 2018/1240 (ETIAS).

[151] Article 26 du règlement 2018/1240 (ETIAS).

censé apporter une garantie suffisante que la décision ne résulte pas seulement du traitement des données par un algorithme.

Il est toutefois incertain que le traitement manuel subsidiaire en l'espèce suffise à considérer que les demandes sont convenablement et entièrement réexaminés par un humain. En effet, dans son arrêt *Ligue des Droits Humains*[152] au sujet de la conformité de la directive PNR au RGPD, la Cour affirmait la nécessité de respecter le critère d'un « contrôle humain clair et précis » dans la prise de décision automatisée. Aucune information ne permet d'affirmer qu'ETIAS est conforme à ce critère dans la prise de décision automatisée, puisque le règlement en lui-même ne contient pas d'indications à ce sujet[153]. Par ailleurs, Il y a de grandes chances que le réexamen manuel soit influencé par la décision automatisée. Celui-ci interviendra en effet après la réponse positive de l'algorithme aux règles d'examen ETIAS ce qui ne sera sûrement pas sans conséquences pour la décision humaine. Enfin, les unités nationales ont été autorisées à mettre en place des outils numériques d'aide au traitement des données ce qui réduit la portée de l'évaluation humaine.

[152] CJUE, C-817/19, *Ligue des droits humains*, 21 juin 2022.

[153] THONNES, Christian, VAVOULA, Novi, « Automated predictive threat detection after Ligue des Droits Humains : Implications for ETIAS and CSAM », *Verfassungsblog*, 12 mai 2023, <https://verfassungsblog.de/pnr-threat-detection-ii/ > (consulté le 2 février 2024 à 23:35).

Partie II. Les menaces substantielles de l'utilisation d'intelligence artificielle pour les droits fondamentaux

Bien que le règlement ETIAS rappelle le nécessaire respect du principe de non-discrimination et de la protection des droits fondamentaux[154], l'utilisation d'IA par le règlement ETIAS demeure une atteinte aux droits consacrés par l'Union européenne à sa travers sa Charte des droits fondamentaux. Ainsi, la collecte et la rétention de données constitue une menace directe au droit à la vie privée et à la protection des données (**Chapitre 3**), tandis que la prise de décision automatisée menace le droit à la non-discrimination (**Chapitre 4**).

Chapitre 3. Les atteintes manifestes au droit à la vie privée et à la protection des données : l'utilisation compromettante des données

Les atteintes au droit à la vie privée et à la protection des données des demandeurs d'autorisation de voyage interviennent au cours de la collecte et du traitement des demandes (**Section I**), mais également après, lors de la conservation et de la réutilisation des données (**Section II**).

Section I. L'utilisation de données personnelles protégées à des fins de surveillance

La protection des données et la vie privée des voyageurs sont menacées par le profilage réalisé par l'algorithme, mais aussi par la liste de surveillance établie par le système d'information qui fait peser une épée de Damoclès sur les demandeurs d'autorisation de voyage.

18. *Le profilage systématique des voyageurs par l'algorithme ETIAS*

Les données collectées par ETIAS pour le traitement des demandes sont personnelles et sensibles. Elles permettent à l'algorithme d'effectuer un « profilage » au sens du Règlement Général sur la Protection des Données[155] (RGPD), c'est-à- dire « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains

[154] Article 14 du règlement 2018/1240 (ETIAS).

[155] Règlement (UE) 2016/679 du Parlement européen et 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), *JOUE* L 119/1.

aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique »[156]. En effet, les données collectées servent à l'établissement de profils qui qui seront ensuite comparées aux indicateurs de risques établis par l'unité centrale ETIAS.

Ce profilage, qui constitue une prise de décision automatisée d'après la jurisprudence de la Cour[157], va à l'encontre d'un principe posé par le RGPD[158] qui consacre le droit de la personne à « ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ». Ce profilage, ainsi que la collecte de données personnelles constitue en effet une véritable atteinte aux articles 7 et 8 de la Charte des droits fondamentaux qui reconnaissent respectivement un droit au respect de la vie privée et familiale ainsi qu'un droit à la protection des données à caractère personnel. Cette atteinte est d'autant plus importante qu'une grande partie des données concerneront les enfants qui doivent bénéficier d'une protection décuplée compte tenu de leur vulnérabilité[159]. Le point suivant du RGPD prévoit cependant une dérogation au principe : le profilage qui « prévoit des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée » saurait être accepté[160]. Le règlement ETIAS doit donc en vertu du RGPD[161] prendre mesures appropriées pour la sauvegarde des droits fondamentaux. Ces mesures sont notamment la création d'un comité d'orientation sur les droits fondamentaux[162] chargé d'évaluer l'incidence du règlement sur les droits fondamentaux ou le traitement subsidiaire des demandes. Il est toutefois très incertain qu'elles suffisent pour contrebalancer les risques générés par ETIAS.

Par ailleurs, l'article 8 de la Charte des droits fondamentaux relatif à la protection des données précise que les « données doivent être traitées loyalement, à des fins déterminées ». Les fins d'utilisations des données par le système d'information ETIAS ne semblent pas strictement déterminées, étant donné la multiplicité des risques par ailleurs mal définis contre lesquels ETIAS voue à lutter. Cet argument est amplifié par le fait que les données seront échangées avec les autres

---

156 Article 4 §4 du règlement 2016/679 (RGPD).

157 CJUE, C-634/21, *SCHUFA Holding*, 7 décembre 2023.

158 Article 22 du règlement 2016/679 (RGPD).

159 (38) du règlement 2016/679 (RGPD).

160 Article 22 §2 point b) du règlement 2016/679 (RGPD).

161 VAVOULA, Niovi, « You (Probably) Are Who I Say You Are », *op. cit.* p.515.

162 Article 10 du règlement 2018/1240 (ETIAS)

systèmes d'information dans le cadre de l'interopérabilité. Il y a donc de fortes chances que le profilage effectué ne remplisse pas la condition de « minimisation des données » consacrée par le RGPD, selon laquelle la collecte de données à caractère personnel doit être « limitée à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »[163]. Il est donc nécessaire que les finalités du règlement soient limitées et mieux définies, afin que la collecte et le traitement de données soient strictement circonscrits à ce qui est nécessaire à l'exécution du règlement.

19**.** *L'élaboration d'une liste de surveillance d'individus à potentiels risques*

En sus du profilage des voyageurs, le règlement prévoit l'élaboration d'une liste de surveillance[164] qui concentre des informations relatives aux personnes suspectées d'avoir commis un acte terroriste ou une autre infraction pénale grave, ainsi que des personnes pour lesquels il existe des indices concrets ou des motifs raisonnables basés sur une évaluation globale que la personne de commette de tels actes.

Cette liste concerne uniquement des suspects. En effet, la liste ne comprendra pas d'informations relatives aux personnes ayant commis de telles infractions, bien que le Conseil ai tenté d'inclure cette catégorie dans le spectre de la liste de surveillance[165]. Elle contiendra donc les données alphanumériques des personnes suspectes, leurs informations de voyage ainsi que leurs contacts[166]. Tenue par l'unité centrale sur la base de la directive 2017/541 pour la lutte contre le terrorisme[167], la liste sera complétée par Europol et les États membres[168]. Les informations transmises devront être « adéquates, exactes et suffisamment importantes »[169] et seront réévalués chaque année par Europol et les États membres. Toutefois, il n'y a aucune mesure visant à limiter ou à contrôler l'entrée d'informations par les différentes autorités disposant de cette prérogative[170], si ce n'est la responsabilité de ces dernières à l'égard de l'exactitude des informations entrées. L'absence de limitation de ces données est donc contraire au principe de minimisation, mais aussi au principe

---

163 Article 5 §1 point c) du règlement 2016/679 (RGPD).

164 Article 34 §1 du règlement 2018/1240 (ETIAS).

165 Conseil de l'Union, Document 8247/17, 24 avril 2017, p.35.

166 Article 34 §4 du règlement 2018/1240 (ETIAS).

167 Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, *JOUE* L 88/6.

168 Article 34 §3 du règlement 2018/1240 (ETIAS).

169 Article 35 §1 du règlement 2018/1240 (ETIAS).

170 VAVOULA, Niovi, *op. cit*, p.525.

d'autodétermination de l'information consacré par un arrêt de la Cour allemande en 1983[171], et donc le juge droit commun pourrait tirer le principe de l'article 8 de la Charte des droits fondamentaux, permettant à tout un chacun d'être maître des informations le concernant.

Le fait que cette liste contiendra des informations relatives à des personnes n'ayant pas commis d'infraction est particulièrement problématique. Cela montre qu'il y a une « normalisation des approches prédictives »[172] dans la politique de l'Union européenne, qui consiste en l'espèce à prêter des intentions à des individus sur la base de données récoltées. Cette approche prédictive ne semble pas compatible avec le droit à la présomption d'innocence consacré par l'article 48 de la Charte des droits fondamentaux[173]. La CJUE avait ainsi souligné le fait que les mesures de surveillance devaient respecter les tests de proportionnalité tels que développés par sa jurisprudence[174]. Il faut alors que des motifs « raisonnables et concrets » permettent de suspecter un individu. Ce critère est issu des conclusions de la CEDH dans son arrêt *Roman Zakharov contre Russie*[175] dans lesquelles les juges avaient affirmé qu'il devait y avoir une suspicion raisonnable contre une personne pour qu'une autorité puisse surveiller une personne. Ainsi, bien que le règlement ETIAS ne prévoit aucune disposition en ce sens, l'atteinte au droit à la vie privée résultant du traitement et de la conservation de données personnelles d'un individu devra être justifiée par un motif raisonnable que les États membres et Europol devront appliquer scrupuleusement pour compléter la liste de surveillance.

Section II. La conservation et l'utilisation compromettante des données dans le système d'interopérabilité

Les données sur les voyageurs étrangers sont collectées puis conservées pour les fins du système ETIAS, mais pourront également être utilisées par d'autres systèmes dans le cadre du système d'interopérabilité dont fait partie ETIAS.

20. *La conservation inquiétante des données par ETIAS*

---

171 BVerfG, Census Acte case,15 décembre 1983.

172 *Ibid*.

173 BRIGANT, Jean-Marie, « Les risques accentués d'une justice pénale prédictive », *Archives de philosophie du droit,*Vol. 60, 2018, p.249.

174 CJUE, C-293/12 et C-594/12, *Digital Rights Ireland Ltd v Minister for Communications*, *Marine and Natural Resources and Others* et *Ka¨rntner Landesregierung and Others*, 8 April 2014, para 42

175 CEDH, *Roman Zakharov c/ Russie*, Grande chambre, Requête n° 47143/06, 4 décembre 2015, para 260.

Une fois les demandes traitées par l'algorithme ETIAS, les données sont conservées dans le système central ETIAS pour la durée de validité de l'autorisation de voyage ou pendant cinq ans à compter de la dernière décision de refus, d'annulation ou de révocation de l'autorisation de voyage[176]. Si le demandeur l'accepte au moment de remplir le formulaire, ses données pourront également être conservées pendant trois ans à compter de l'autorisation de voyage, afin de faciliter une future demande. A l'expiration des délais de conservation, les données sont automatiquement effacées du système central ETIAS.

La période de rétention des données de cinq ans est critiquée car elle est particulièrement longue et est sans doute disproportionnée au regard de la finalité du traitement[177]. Par ailleurs, le principal danger provient du fait que les données conservées accessibles à des fins étrangères à la fonction administrative d'ETIAS[178]. Elles sont en effet utilisées pour la formation et l'entrainement de l'algorithme ETIAS qui s'auto-nourri des statistiques de demandes d'autorisation[179] pour établir des indicateurs de risques liés aux demandeurs[180]. Les données sont également accessibles sous certaines conditions aux transporteurs, aux autorités frontalières, aux autorités chargées de l'immigration, aux agences de l'union compétentes, aux autorités nationales compétentes. Le stockage de ces données par EU-Lisa génère par ailleurs un risque important de cyberattaques qui pourrait mener à d'importantes fuites de données, ce qui aurait des conséquences désastreuses pour le respect du droit à la protection des données des ressortissants étrangers compte tenu de la sensibilité des informations en jeux. Ce danger est d'autant plus important que les données seront échangées par différents systèmes d'information à travers différents portails ce qui augment la vulnérabilité de ces dernière/

21. *L'interopérabilité excessive des données dans les systèmes d'information*

En effet, un élément essentiel dans la mise en œuvre du règlement ETIAS est son interconnexion avec les autres systèmes d'information via l'interopérabilité des données[181]. Cette interopérabilité s'articule autour du portail de recherche européen (ESP) qui permet d'interroger simultanément les différents systèmes d'information, du service partagé d'établissement de correspondances biométriques (BMS partagé) qui permet de rechercher et comparer les données biométriques contenues dans les systèmes d'information, du répertoire de données d'identité (CIR) qui facilite

[176] Article 54 §1 du règlement 2018/1240 (ETIAS).

[177] VAVOULA, Niovi, JEANDESBOZ, Julien, ALEGRE, Susie, *op. cit.*, p.12.

[178] MICHÉA, Frédérique, ROUSVOAL, Laurent, *op. cit.*, p.474.

[179] Article 84 du règlement 2018/1240 (ETIAS).

[180] Article 33 §2 b) et c) du règlement 2018/1240 (ETIAS).

[181] Voir Annexe 5 et 6.

l'identification des personnes en stockant les informations biographiques et biométriques, et du détecteur d'identité multiples (MID) qui vérifie si les données existent dans plusieurs systèmes afin de détecter des identités multiples. Cette interopérabilité traduit davantage « un choix politique que technique » d'après le CEPD[182], car elle permet l'accès des services répressifs visés par le règlement 2019/817[183] (Europol, services de police des États-membres) aux systèmes à finalité non répressive (SIS, VIS, EES, ETIAS, Eurodac). Les systèmes d'information ainsi que les services répressifs pourront y accéder via les différents portails mis en place par l'Union.

Les données stockées dans ETIAS pourront donc servir à différentes autorités, sans que le demandeur d'autorisation de voyage n'y soit informé le cas échéant. Le manque d'information du voyageur à ce sujet enfreint le principe de légalité selon lequel les individus devrait être mis au courant de la manière dont leurs données sont utilisées et les fins pour lesquelles elles le seront[184]. Cette interopérabilité constitue une atteinte majeure à la protection des données[185] et constitue un risque de violation du principe de limitation du traitement des données à des fins déterminées[186] prévue par le RGPD[187]. En effet, comme le rappelle le CEPD, chacun des systèmes d'information a été créé pour une finalité spécifique qui ne devrait donc pas être combiné avec celle d'ETIAS[188]. Ce risque encouru est renforcé par le fait que ces bases de données centralisées contiennent des informations à caractère personnel sur des millions de ressortissants de pays tiers. Le CEPD en conclut la possibilité de consulter la base de données centralisée devrait être formulée de manière plus claire. Il en appelle à la « mise en place de garanties réelles pour préserver les droits fondamentaux des ressortissants de pays tiers » face au cadre d'interopérabilité. Ces garanties ont notamment vu le jour avec l'article 52 du règlement ETIAS durcissant les conditions d'accès aux données du système ETIAS. Cette disposition précise que la consultation d'autres bases de données doit être nécessaire aux fins de prévention et de détection d'une infraction terroriste ou d'une infraction pénale grave, proportionné au cas spécifique, et qu'il doit exister des preuves ou motifs raisonnables permettant de considérer que la consultation des données contribueras aux fins visées.

---

[182] CEPD, « Avis 4/2018 sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE » , 16 avril 2018, p.3.

[183] Article 20 du règlement 2019/817 (Interopérablitié).

[184] VAVOULA, Niovi, JEANDESBOZ, Julien, ALEGRE, Susie, *op. cit*. p.37.

[185] FRA, « Fundamental rights and the interoperability of EU information systems: borders and security », 2017, 50p.

[186] MICHÉA, Férédrique, « Les finalités des systèmes d'information européens à vocation migratoire », in Sandrine Turgis (dir.), *Les données numériques des migrants et des réfugiés sous l'angle du droit européen*, 2020, p. 37-63.

[187] Article 5 §1 b) du règlement 2016/679 (RGPD).

[188] CEPD, 2017, *op.cit.,* p.13.

Là encore, l'appréciation de ce qui est strictement nécessaire devra être contrôlé par des organes indépendants afin de limiter l'utilisation des données à la finalité pour laquelle elle a été collectée.

Chapitre 4. Les atteintes potentielles au droit à la non-discrimination : le refus automatisé des autorisations de voyage

Outre les dangers pour la vie privée, le règlement ETIAS a également été critiqué pour les risques de discrimination qu'il génère envers les ressortissants étrangers. En effet, l'algorithme utilisé manipule des données personnelles fortement discriminantes (**Section I**) alors même que celui-ci est intrinsèquement sujet à des biais algorithmiques qui augmentent le risque de potentielles discriminations dans le traitement des demandes (**Section II**).

Section I. L'utilisation de données personnelles discriminantes dans la prise de décision automatisée

Les données collectées par ETIAS concernent des informations très personnelles à haut potentiel discriminant et font donc craindre le risque d'une éviction de certains groupes sociaux lors du traitement automatisé des demandes.

22. *La collecte de données hautement discriminantes par l'algorithme ETIAS*

Le règlement ETIAS, en collectant autant de données à caractère personnel, menace fortement le droit à la non discrimination garanti aux ressortissants étrangers par la Charte des droits fondamentaux[189], qui dispose qu'est « interdite, toute discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. ». Le règlement ETIAS précise ainsi que les indicateurs de risques ne devront en aucun cas révéler la couleur d'une personne, sa race, son ethnie, son origine sociale, des éléments génétiques, sa langue, sa religion, ses convictions politiques, son appartenance à un syndicat, à une minorité, sa propriété, son handicap ou son orientation sexuelle[190]. Il interdit de surcroît les indicateurs de risques qui

[189] Article 21 de la Charte des droits fondamentaux.

[190] Article 35 §5 de la régulation 2018/1240 (ETIAS).

seraient uniquement fondés sur le sexe ou l'âge. Une personne ne pourra donc pas être refusée seulement parce qu'elle a 25 ans ou parce que c'est une femme. Toutefois, même lorsque les marqueurs d'identité et les catégories d'informations protégées sont supprimés d'un ensemble de données, des résultats discriminatoires peuvent néanmoins survenir[191]. Ainsi, cette même personne pourra toutefois être refoulée si c'est une femme de 25 ans et que les indicateurs de risques précisent que ce profil est particulièrement risqué. Une discrimination fondée sur l'intersection entre plusieurs critères discriminants pourrait donc apparaître[192], ce qui est particulièrement dangereux notamment pour les groupes les plus vulnérables[193].

En outre, le Comité européen pour la protection des données souligne que les données sur lesquelles se fonderont les indicateurs de risques des règles d'examen seront très proches des informations personnelles protégées[194], ce qui rendrait ETIAS directement ou indirectement discriminant. En effet, couplée à un traitement fondé sur les statistiques, une donnée personnelle pourra souvent révéler une information discriminante. L'adresse postale, par exemple, sera souvent utilisée comme substitut pour déterminer l'origine ethnique[195]. Le sexe d'un individu pourra indiquer son orientation sexuelle. Son âge pourrait révéler sa richesse, ses convictions politiques et son état physique. Sa ville de résidence, manifester son ethnie ou sa couleur. Sa nationalité, révéler son ethnie, sa religion, ses convictions politiques. Son emploi (salarié, travailleur indépendant, chômeur, sans emploi, retraité, étudiant), laisser transparaitre sa richesse et sa potentielle appartenance syndicale[196]. Ainsi, en raison des liens étroits qui existent entre les données collectées et les informations protégées, comme le lien entre la nationalité et l'ethnie ou la profession et le syndicat, le profilage ETIAS constitue un risque important de discrimination[197]. Les refus d'autorisation de voyages auraient en effet de grandes chances d'être fondés sur des caractéristiques interdites par la Charte des droits fondamentaux et par la Convention des Nations Unies[198]. Ainsi, le résultat de la décision automatisée pourrait mener à l'éviction systématique de personnes appartenants à certains groupes sociaux, par exemple les chômeurs ou les membres de tels syndicats, sans qu'un tel risque généré par ces profils soit avéré.

---

191 LEPRI, Bruno et al. « Fair, Transparent, and Accountable Algorithmic Decision-Making Processes. », *Philosophy & Technology,* n°31, 2018, p.616.

192 DERAVE, p.36

193 Bien que la CJEU ait refusé un recours fondé sur une discrimination intersectionnelle dans C-443/15 *David L Parris v Trinity College Dublin*, 24 novembre 2016, para 80.

194 CEPD, 2017, *op. cit*., p.12.

195 CJUE, C-83/14, *CHEZ Razpredelenie Bulgaria*, 16 juillet 2015

196 VAVOULA, Niovi, *op. cit.*, p.529.

197 CEPD, *op. cit.*, p.14.

198 Convention des Nations Unies pour l'élimination de toutes les formes de discriminations raciales de 1965.

Une telle discrimination remettrait en cause la liberté d'expression, d'association ou de culte des personnes reconnus par la charte qui se verraient persécutées pour l'exercice de certaines libertés fondamentales. Ce danger est décuplé par le fait que les individus évincés seraient très probablement des profils déjà très vulnérables. Une fois ces données révélant des information protégées collectées, elle seront traitées automatiquement par un algorithme qui décidera d'octroyer les demandes d'autorisation de voyage sur la base d'un traitement statistique.

23. *L'inquiétant traitement statistique des données personnelles par un algorithme*

Le traitement des données à caractère personnel par un algorithme statistique est particulièrement alarmant. D'abord, parce que pour que l'algorithme fonctionne, il faut que l'algorithme puisse convenablement traiter les données. Pour cela, les données doivent être complètes et de bonne qualité. Il est toutefois possible que ce ne soit pas le cas, car peuvent subsister des erreurs matérielles, un manque de documentation ou de transcription ainsi qu'une traduction ou translittération incorrecte. Les données issues du système d'interopérabilité peuvent également être endommagées. Par exemple, lorsqu'une empreinte digitale retrouvée sur une scène de crime est inscrite par Eurodac dans BMS partagé[199], mais est incomplète ou de mauvaise qualité. Cela conduirait à un grand nombre de correspondances avec des individus[200], et impliquerait un grand nombre de rejet d'autorisations de voyages. Par conséquent, si les données enregistrées dans le système d'information sont de mauvaise qualité, il y a de grande chance que l'algorithme conduise à un refus de l'autorisation de voyage. Cela aurait une répercussion importante un grand nombre de ressortissants étrangers illégitimement associés à des données parcellaires.

De surcroit, l'algorithme ne pourra probablement pas comprendre certaines explications subtiles données par le demandeur, et conduira très certainement à un rejet automatique de la demande dès lors qu'une correspondance sera établie entre une donnée et les indicateurs de risques. Ainsi, un individu ayant séjourné dans un pays en guerre à l'occasion d'un voyage humanitaire sera probablement caractérisé par l'algorithme comme un individu à haut risque, conduisant à une décision mal fondée. Ensuite, la prise de décision automatisée est préoccupante car la logique probabiliste qui guide le fonctionnement de l'IA, c'est-à-dire le raisonnement déductif fait sur la base des probabilités et de statistiques[201], est particulièrement déconnectée de la réalité complexe de la

---

[199] THIERY, Sylvain, « La place grandissante des outils numériques en matière migratoire à la lumière de la réforme du règlement Eurodac », in Bertrand Brunessen (dir.), *La politique européenne du numérique,* Bruylant, Bruxelles, p. 457-472.

[200] VAVOULA, Niovi, « Consultation of EU Immigration Databases for Law Enforcement Purposes », *op. cit*., p. 173.

[201] JOHN NILSSON, Nils, « Probabilistic Logic », *Artificial Intelligence*, Vol. 28, 1986, p. 71–88.

situation des individus. En effet, les modèles prédictifs ne sont basés que sur des propensions et des corrélations qui biaisent toutes réflexions sur la réalité du risque encouru. Les décisions ne sont alors plus basées sur des critères juridiques stables mais sur des « caractéristiques » et des « corrélations » liées à des modèles qui reproduisent des propensions observés dans les données[202]. Cela mène à des décisions qui omettent l'individualité et la singularité des personnes pour générer des « clusters » (ou « groupes spécifiques de voyageurs »)[203]. Ces groupes rassemblent des individus qui ne sont que provisoirement liés entre eux sur la base d'informations collectées associées à un risque défini par des statistiques. L'acceptation ou non d'une demande relève alors uniquement de la prospection des risques que pourrait représenter un ressortissant étranger, ceux-ci devenant de véritables « suspects » aux yeux de la politique migratoire de l'Union dès lors qu'ils disposent d'une caractéristique associée à une risque. Le traitement statistique mène donc à une discrimination des individus au même titre que le phénomène de « contrôle au faciès »[204], et constitue donc un danger majeur pour les individus. Ce danger est en outre décuplé par l'existence de biais intrinsèques aux données et à l'intelligence artificielle, qui vont jusqu'à influencer la décision humaine.

Section II. Le risque de biais discriminants consubstantiel à l'utilisation de l'intelligence artificielle

L'utilisation de l'IA dans le règlement ETIAS mène à de nombreux biais qui sont difficiles à détecter et à limiter[205]. La science comportementale a ainsi permis de reconnaître différents biais auxquels fait face une IA, permettant de souligner les dangers générés par un tel dispositif.

24. *Les biais inhérents aux données statistiques utilisées*

Un biais se définit comme une « déviation dans le traitement cognitif d'une information ». Il implique, en l'espèce, une décision injuste et discriminante. Ils sont inhérents au fonctionnement de l'algorithme et aux données utilisées, ce qui augmente le risque de discrimination lors de la décision automatisée. L'IA peut être biaisée dès sa formation à cause des données utilisées pour créer

---

[202] *Ibid*. p.111.

[203] PETERSMANN, Marie, VAN DEN MEERSSCHE, Dimitri, « On phantom publics, clusters, and collectives: be(com)ing subject in algorithmic times », *AI & SOCIETY,* 2024, p.109.

[204] JOHANNÈS, Frank, « En France, « le contrôle d'identité au faciès est un problème systémique, structurel, institutionnel », Le Monde, 1er août 2023 < https://www.lemonde.fr/societe/article/2023/08/01/police-le-controle-d-identite-au-facies-est-un-probleme-systemique-structurel-institutionnel_6184039_3224.html> (consulté le 19 mai 2024 à 23:45).

[205] FRA, « #BigData: Discrimination in data-supported decision-making », 2018, p. 3

l'algorithme[206]. En effet, les données qui sont utilisées pour entraîner un algorithme peuvent être affectées par de multiples biais cognitifs. Ainsi, le « biais de l'échantillon » est apparaît en sélectionnant des types spécifiques de données au dépens d'autres données représentatives, ce qui conduit à une conceptualisation du monde non représentative de la réalité. En effet, les statistiques ne sont pas forcément représentatives des personnes demandant une autorisation de voyage. Le « biais d'attribution » est également particulièrement présent dans la décision ETIAS. Il s'agît du fait que des comportements soient associés à une caractéristique spécifique. Ainsi, l'algorithme est programmer pour associer certains risques (migratoires, sécuritaires, sanitaires) à des caractéristiques (âge, sexe, emploi etc.) qui reviennent souvent corrélés. L'algorithme conclura alors systématiquement au refus d'une personne liée à la caractéristique visée, ce qui est contraire au principe de non-discrimination. Enfin, il existe un « biais de capture »[207] dans la phase d'entrainement et de formation de l'algorithme, qui intervient lorsque des ensembles de données sont créés en utilisant des substituts au lieu de valeurs réelles. Par exemple, le taux d'arrestation est souvent utilisé comme substitut au taux de criminalité, les visites chez le médecin et les médicaments achetés le sont comme indicateurs de santé. Cela conduit au traitement trompeur des informations qui sera ensuite retranscrit dans la décision de l'algorithme chargée de refuser automatiquement les individus associés à un risque.

Par ailleurs, il existe une marge d'erreur importante relative aux données statistiques utilisés par ETIAS dont la fiabilité n'est pas encore avérée[208]. En effet, l'algorithme utilisera dès son lancement des statistiques issues d'EES, VIS et ETIAS alors même que ces systèmes débuteront leur opérations et la qualité des données n'aura pas été évaluée. Les données seront également apportées par les États membres dont certains pourraient souhaiter promouvoir des contrôles extrêmement strictes[209] pour renforcer leur bilan sécuritaire et migratoire, ce qui renforcerait la dimension politique d'ETIAS.

25. *Les biais dans la prise de décision de l'intelligence artificielle*

---

[206] SRINIVASAN, Ramya, CHANDER, Ajay, « Biases in AI systems », *Commun* ACM 64, 8, 2021, p.44–49.

[207] TORRALBA, Antonio, EFROS, Alexei, « Unbiased Look at Dataset Bias », *IEEE Conference on Computer Vision and Pattern Recognition* (CVPR), 2011, p.1522.

[208] VAVOULA, Niovi, *Immigration and Privacy in the Law of the European Union*, Leiden, Brill, 2022, p.444.

[209] VAVOULA, Niovi, « Tr-AI-nsforming Migration, Asylum and Border Management in the EU », *op. cit.*, p.19.

En-dehors des biais relatifs aux données, il existe des biais inhérents aux machines qui apparaissent dans au moment du codage des algorithmes. Il y a ainsi un fort risque de biais de transfert[210], c'est-à-dire une situation dans laquelle il y a « transfusion » d'un préjugé humain à la machine. Ainsi, une IA peut retranscrire directement un préjugé de nature humaine. Ces biais ne sont pas corrigés par les machines et faussent donc la prise de décision optimale. Ils représentent ainsi un danger inhérent à la décision automatisée et font craindre le risque d'une discrimination pour les ressortissants étrangers. En effet, une étude menée sur les logiciels de reconnaissance faciale (utilisés par Amazon notamment) a montré que les machines prenaient systématiquement une décision défavorable aux femmes noires[211]. Une autre étude effectuée par des chercheurs américains[212] avait pu démontrer que les algorithmes utilisés par la justice américaine dans différents États pour mesurer le risque de récidive de criminels évaluaient constamment les personnes noires comme ayant plus de risques de récidiver. L'utilisation de facteurs « neutres » en apparence tels que le code postal ou l'emploi peut, dans la pratique, servir de substitut à des critères raciaux, exacerbant les préjugés raciaux, conférant une fausse légitimité aux modèles de profilage et sapant la présomption d'innocence dans le système de justice pénale[213]. Ce biais est conforté par la dimension objective et rationnelle qui est souvent associé aux IA et qui camoufle les discriminations qui découlent de la décision automatisée.

Subsidiairement à la décision automatisée, ETIAS prévoit une analyse humaine des demandes d'autorisation de voyage supposée limiter les erreurs des algorithmes. En effet, la jurisprudence de la Cour impose pour éviter les mesures discriminatoires une ré-examination entièrement manuelle d'une décision automatisée[214]. Il y a toutefois de grandes chances que la décision manuelle soit l'objet de biais. Celle-ci risque en effet d'être influencée par le résultat de la décision automatisée qui aura conclu à un risque représenté par le ressortissant étranger car les résultats présentés par les algorithmes sont souvent présentés comme objectifs et rationnels[215], d'autant plus que des algorithmes seront progressivement mis en place pour « aider » l'humain à la décision[216]. Il faudrait

---

[210] FERRER, Xavier et al. « Bias and Discrimination in AI : A Cross-Disciplinary Perspective », *Computers and Society*, 2020, p.2.

[211] SRINIVASAN, Ramya, CHANDER, Ajay, *op. cit.*, p.46.

[212] Julia ANGWIN, Jeff LARSON, Surya MATTU, Lauren KIRCHNER, « Ethics of Data and Analytics », *ProPublica*, 2016,<https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> (consulté le 10 mai 2024 à 17:15)

[213] SHAPIRO, Aaron, « Reform predictive policing » *Nature,* 25 January 2017, <https://www.nature.com/articles/541458a> (consulté le 11 mai 2024 à 17h21).

[214] CJUE, C-511/18 - *La Quadrature du Net and Others*., 6 octobre 2020, para 182.

[215] Woody Allen disait que « L'intelligence artificielle se définit comme le contraire de la bêtise naturelle ».

[216] ZANDSTRA, Timo, BROUWER, Evelien, « Fundamental Rights at the Digital Border : ETIAS, the Right to Data Protection, and the CJEU's PNR judgment », *Verfasssungsblog*, 24 juin 2022, <https://verfassungsblog.de/digital-border/> (consulté le 14 avril 2024 à 16:35).

donc des mesures permettant d'assurer que l'humain adopte un regard sceptique et distant face au résultat de l'IA. Des outils ont été créés dans cette optique pour évaluer le degré d'équité dans un système[217], comme « Aequitas » ou « AI Fairness 360 »[218]. Ils sont censé aider les ingénieurs à développer des modèles d'apprentissages équitables afin de s'éloigner des pratiques discriminatoires, bien qu'ils ne présentent pas encore de garanties fiables.

Partie III. Le renforcement nécessaire des garanties pour la protection des droits fondamentaux face à l'utilisation de l'intelligence artificielle

L'utilisation prévue de l'IA dans le règlement ETIAS menace donc au moins cinq droits fondamentaux reconnus par la Charte des droits fondamentaux : le principe de proportionnalité, le droit à la vie privée, le droit à la protection des données, la protection des enfants, le droit à la non-discrimination. Le règlement prévoit ainsi qu'il est « nécessaire que les personnes physiques bénéficient d'un droit d'accès, de rectification, de limitation du traitement et d'effacement, ainsi que du droit de faire compléter des données, et d'un droit de recours en ce qui concerne les données à caractère personnel, en particulier du droit à un recours juridictionnel, et que le contrôle des opérations de traitement soit assuré par des autorités publiques indépendantes ». Toutefois, si ces garanties existent, elles semblent incomplètes et limitées (**Chapitre 5**). Les nouveaux textes en matière de régulation de l'intelligence artificielle constituent dès lors des gardes-fous bienvenus pour l'utilisation d'algorithmes dans le système ETIAS et devraient permettre de compléter les garanties prévues par le règlement (**Chapitre 6**).

Chapitre 5. Les garanties incomplètes d'ETIAS : les failles du règlement dans la protection des droits fondamentaux face aux risques de l'intelligence artificielle

Bien que le règlement ETIAS prévoit l'instauration d'un Comité des droits fondamentaux visant à faire cesser toutes atteintes aux droits fondamentaux, les garanties mises en place par ETIAS demeurent limitées et incomplètes. Ainsi, le règlement reste opaque dans le traitement des données (**Section I**) tandis que l'effectivité des voies de droits est incertaine (**Section II**).

---

[217] MEHRABI, Ninareh, et al. « A Survey on Bias and Fairness in Machine Learning », *ACM Computing Surveys,* Volume 54, 2021, p.1–35.

[218] KADIRESAN, A., BAWEJA, Y., OGBANUFE, O, « Bias in AI-Based Decision-Making », *Bridging Human Intelligence and Artificial Intelligence*, 2022, p. 280.

Section I. L'utilisation nébuleuse de l'intelligence artificielle dans le règlement ETIAS : un manque à l'obligation de transparence

En l'état, le règlement ETIAS manque à l'obligation de transparence qui découle du droit à l'information, car les informations sur les algorithmes utilisés sont difficilement accessibles et compréhensibles pour les voyageurs, et que l'explication de la décision sur l'autorisation de voyage est lacunaire.

26. *L'utilisation opaque d'algorithmes intelligents dans ETIAS*

Dans une étude de l'université de Toronto[219] sur l'utilisation d'algorithme dans la politique migratoire du Canada, des chercheurs concluaient : « Le défi n'est pas d'utiliser les nouvelles technologies pour perpétuer d'anciens problèmes, mais plutôt de mieux comprendre comment nous pouvons utiliser cette opportunité pour imaginer et concevoir des systèmes plus transparents, plus équitables et plus justes. ». En effet, la transparence liée à l'utilisation algorithmique doit être une garantie fondamentale accordée aux usagers que sont les voyageurs, sans quoi la prise de décision automatisée devient un véritable danger pour les droits fondamentaux. Le règlement ne précise pourtant pas comment l'algorithme devrait être conçu et utilisé pour trier les demandes[220]. Il affirme seulement que celui-ci effectuera un profilage dans l'objectif de chercher des correspondances avec les règles de filtrage établies. Ces demandes seront refusées si le demandeur présente un risque ou si ses documents font l'objet d'un signalement[221], sans plus de précision. Ce manque d'informations s'explique par des contraintes techniques liées au développement de l'algorithme[222], mais aussi par une volonté politique cherchant discrètement à entreprendre le développement d'un système d'information massif pour collecter les données des ressortissants étrangers[223]. Il résulte également de l'impossibilité pour des observateurs humains externes d'identifier, de comprendre et de reproduire les schémas de raisonnement choisis par les algorithmes qualifiés de « boîte noire »[224],

---

[219] MOLNAR, Petra, GILL, Lex,, « Bots at the Gate : A human rights analysis of Automated decision-making in Canada's immigration and refugee system », *University of Toronto and the Citizen Lab-Munk School of Global Affairs and Public Policy*, 2018, p.7.

[220] GANDHI, Shrutika, *op. cit*., p.9.

[221] Article 37 du règlement 2018/1240 (ETIAS).

[222] MICHÉA, Frédérique, ROUSVOAL, Laurent, *op. cit*, p.476.

[223] Sandrine Turgis, *Les données numériques des migrants et des réfugiés sous l'angle du droit européen*, Presses Universitaires de Rennes, 2020.

[224] LEESE, Mathias, « The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-Discriminatory Safeguards in the European Union », *Security Dialogue*, 2014, p.494.

compromettant donc la conformité d'ETIAS aux obligations en matière de droits fondamentaux comme le droit à l'information.

Le CEPD soulignait en ce sens que « les 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 ». En effet, une utilisation opaque de l'IA exacerbe les asymétries[225] qui existent entre les demandeurs d'autorisations de voyage, qui n'ont alors aucune visibilité sur la façon dont seront traitées leurs données, et les concepteurs de l'algorithme, c'est-à-dire EU-Lisa et Frontex, qui décident discrétionnairement des indicateurs de risques appliqués aux demandes sans qu'il n'y ai de quelconque limite technique à leur élaboration[226]. Le risque principal est alors que les ressortissants étrangers qui voient leur demande d'autorisation de voyage refusée ne pourront pas intenter un recours effectif, puisqu'il ne sauront pas suffisamment d'information sur la façon dont l'algorithme fonctionne et dont les indicateurs de risques déterminent la décision automatisée[227]. Cette opacité dans le fonctionnement de l'algorithme est exacerbée par le manque de justification liée au refus d'autorisation de voyage.

27. *L'explication lacunaire du refus d'autorisation de voyage*

Si l'algorithme ETIAS fonctionne de façon nébuleuse, ce qui nuit au droit à l'information des usagers; les raisons conduisant au refus, à l'annulation ou à la révocation de l'autorisation de voyage le sont tout autant. Ainsi, le règlement prévoit que lorsqu'une demande est refusée, annulée ou révoquée, le demandeur reçoit la notification via messagerie électronique, accompagnée de la mention claire des motifs refus de l'autorisation de voyage, les coordonnées de l'unité nationale qui a refusé la demande et des informations quant au droit au recours[228]. Il convient toutefois de s'intéresser aux motifs de rejet d'une demande. Ces motifs sont les suivants : le fait de présenter un risque en matière de sécurité, d'immigration illégale ou d'épidémie, le fait de faire l'objet d'un signalement, ou l'existence de doutes raisonnables et sérieux quant à l'authenticité des données[229]. L'exposition des motifs est donc très laconique et n'est pas suffisante. La Commission a toutefois

---

[225] LEPRI, Bruno, *op. cit.*, p.618.

[226] Musco Eklund, Amanda, « Rule of Law Challenges of 'Algorithmic Discretion' & Automation in EU Border Control A Case Study of ETIAS Through the Lens of Legality », *European Journal of Migration and Law,,* Vol. 25*,* 2023, p.261.

[227] BROUWER, Evelien, « Schengen and the Administration of Exclusion: Legal Remedies Caught in between Entry Bans, Risk Assessment and Artificial Intelligence », *European Journal of Migration and Law*, Vol. 23, n°4, 2021, p.505

[228] Article 38 §2 du règlement 2018/1240 (ETIAS).

[229] Décision d'exécution (UE) 2022/102 de la Commission du 25 janvier 2022 établissant des formulaires de refus, d'annulation ou de révocation d'une autorisation de voyage, *JOUE* L 17/59.

ajouté la possibilité pour l'Unité nationale de préciser ces réponses dans le cadre d'une zone de texte permettant d'exposer « des faits pertinents et motivation supplémentaire »[230].

Les réponses préparées par la Commission, limitées et peu élaborées, ne semblent par apporter de motif suffisamment clair au demandeur, notamment lorsque le motif invoqué est l'existence d'un risque en matière d'immigration irrégulière ou sur un doute quant à l'authenticité des données[231]. Le CEPD recommandait ainsi d'apporter davantage de précisions suite au rejet d'une autorisation, notamment si ce dernier résulte d'une réponse positive de l'algorithme liée à une donnée obtenue dans un autre système d'information. En effet, la Cour avait déjà pu affirmer que pour garantir un droit de recours juridictionnel effectif, il est nécessaire que la personne ayant reçu une décision automatisée puisse connaître les motifs précis sur lesquels se fonde la décision à son égard[232]. Grâce à ces informations plus précises, le demandeur pourra déterminer le système d'information dans lequel il devrait exercer son droit d'accès aux données à caractère personnel le concernant, et potentiellement son droit de rectification ou d'effacement en cas d'erreur ou de traitement illicite de ses données. Il pourra également plus facilement activer son droit au recours en contestant les motifs précis invoqués. Une réponse précise et motivée écrite par un humain serait donc favorable à l'exercice d'un droit au recours juridictionnel effectif par le demandeur.

Le manque de transparence et d'explication dans la prise de décision ETIAS sont des atteintes aux droits fondamentaux puisqu'ils affaiblissent la responsabilité des autorités au regard de la décision automatisée et la possibilité pour les demandeurs d'exercer un recours effectif[233].

Section II. Le droit au recours effectif incertain dans le règlement ETIAS

Deux recours peuvent être effectués par les ressortissants étranger susceptibles de subir une atteinte à leurs droits fondamentaux : le recours contre le refus de l'autorisation de voyage et la réclamation pour le traitement des données à caractère personnel.

28. *Le droit à procès juridictionnel équitable limité par à la nature extraterritoriale d'ETIAS*

[230] *Ibid*. spéc. Annexe 1 de la décision d'exécution.

[231] CEPD, *op. cit.*, p.21.

[232] CJUE, Joined cases C-225/19 and C-226/19, *RNNS and KA*, 24 novembre 2020

[233] ROBLES CARILLO, Margarita, « Artificial intelligence: From ethics to law », *Telecommunications Policy,* vol 44, 2020.

Le droit au recours face à un refus, une révocation ou une annulation d'autorisation de voyage[234], bien qu'explicitement mentionné par le règlement ETIAS[235], demeure incertain. En effet, le règlement précise que « Les recours sont intentés dans l'État membre qui s'est prononcé sur la demande et conformément au droit national de cet État membre ». Ce sont donc les unités nationales qui sont chargées de mettre en œuvre les voies de recours disponibles, conjointement avec les autorités judiciaire nationales. La première difficulté pour effectuer un recours effectif est la limite de la langue. En effet, les demandes ETIAS doivent être effectuées dans l'une des 24 langues de l'Union[236], tout comme le sera la réponse délivrée par l'algorithme ETIAS. Ainsi, un ressortissant japonais pourra donc avoir accès au formulaire en estonien ou en bulgare mais pas dans sa langue natale. Le refus d'autorisation notifié par courriel le sera tout autant.

En outre, une seconde difficulté, et non des moindre, tient à la nature extraterritoriale du règlement ETIAS[237]. Celui-ci s'applique aux ressortissants étrangers en dehors des frontières de l'Union. Les demandeurs remplissent en effet leur demande d'autorisation de voyage alors qu'ils ne sont pas sur le territoire de l'Union. Cela a des conséquences importantes sur l'accès de ces demandeurs aux tribunaux européens[238]. En effet, ceux-ci seront nécessairement en position de faiblesse[239] pour intenter un recours contre les Unités nationales dans le droit national de ces dernières. En France, les ressortissants étrangers devront exercer un recours administratif préalable obligatoire[240] auprès du sous-directeur des visas[241] dans un délai de trente jours à compter de la notification de la décision de refus d'autorisation de voyage. En cas de réponse négative au RAPO, le demandeur peut saisir le tribunal de Nantes d'un recours contentieux dans un délai de deux mois à partir de la notification du refus[242]. Cette procédure complexe, qui varie de surcroît selon les États-membres, semble à l'antipode de l'exigence d'un recours approprié et accessible[243] tenant compte de la situation

---

234 En vertu de l'article 47 de la Charte des droits fondamentaux.

235 Article 37 § 3 du règlement 2018/1240 (ETIAS).

236 Article 16 du règlement 2018/1240 (ETIAS).

237 VAVOULA, Niovi, « The "Puzzle" of EU Large-Scale Information Systems for Third-Country Nationals », *op. cit*., p.14.

238 DEN HERTOG, Leonhard, « Fundamental Rights and the Extra-Territorialisation of E.U. Border Policy : a contradiction in terms ? », in Didier Bigo, Sergio Carrera, Elspeth Guild (dir.), *Foreigners, Refugees or Minorities ? Rethinking People in the Context of Border Controls and Visas*, Ashgate, Farnham, 2013, p. 205-226.

239 VAVOULA, Niovi, « You (Probably) Are Who I Say You Are », *op. cit.*, p.533.

240 Article L411-2 du Code des relations entre le public et l'administration.

241 Article D312-7 du Code de l'entrée et du séjour des étrangers et du droit d'asile instauré par Décret n°2022-963 du 29 juin 2022 relatif aux modalités de contestation des refus d'autorisations de voyage et des refus de visas d'entrée et de séjour en France *JORF* n°0151.

242 Article R421-1 du Code de justice administrative.

243 CEDH, *Çelik et İmret c.Turquie*, 2004, §5.

personnelle des requérants[244] garanti par la Convention EDH[245]. En effet, il semble par exemple extrêmement compliqué pour un ressortissant coréen de porter un recours devant les juridictions françaises et dans une autre langue. Le droit à un recours effectif, bien qu'existant en théorie, ne semble donc pas garanti par la pratique.

29. *Le droit de réclamation pour le traitement des données menacé par la dimension sécuritaire d'ETIAS*

Le demandeur bénéficie d'un droit d'accéder à ses données à caractère personnel stockées, de les rectifier, les effacer et de limiter leur traitement. Cette faculté est précisée par le règlement ETIAS[246], qui prévoit d'informer le demandeur lors de la notification de la décision d'autorisation de voyage en vertu de l'article 15 du RGPD. La notification de la décision sera ainsi accompagnée des coordonnées du délégué à la protection des données de Frontex, du Contrôleur européen de la protection des données et de l'autorité de contrôle nationale de la protection des données, en France la CNIL.

Compte tenu de l'importance des données personnelles collectées pour mener à bien le système d'information liés aux voyageurs et la liste de surveillance ETIAS, il y a fort à parier que l'unité centrale ETIAS oppose un refus à l'effacement ou à la rectification de données personnelles. Une telle réclamation devra être minutieusement justifiée et témoigner d'une absence de proportionnalité entre les données conservées et les risques engendrés par le demandeur d'autorisation de voyage. La garantie consacrée par le RGPD est alors limitée par la nature même du règlement ETIAS, instauré à des fins répressives et de surveillance[247].

Cette garantie est de surcroît amoindrie par la dimension extraterritoriale du règlement qui implique des difficultés pour le demandeur de faire valoir ses droits à distance. En effet, en cas de refus lié à une réclamation auprès d'une autorité de contrôle, le demandeur devra exercer un recours contentieux devant les juridictions de l'État membre sur lequel l'autorité de contrôle est établi[248]. En France, c'est donc le Conseil d'État qui est compétent en premier et dernier ressort pour connaître des recours suite au refus d'une réclamation sur le traitement des données[249]. Ainsi, les difficultés liées à la langue, à la singularité de chaque système juridique et à la complexité de la procédure font

---

[244] CEDH, *Akdivar et autres c. Turquie*, 1996, § 69.

[245] Article 13 de la CEDH.

[246] Article 71 q) du règlement 2018/1240 (ETIAS).

[247] MICHÉA, Frédérique, ROUSVOAL, Laurent, *op. cit.*, p.481.

[248] Article 78 du règlement 2016/679 (RGPD).

[249] Article R311-1 du Code de justice administrative.

ainsi craindre que beaucoup de ressortissants étrangers renoncent à l'exercice de cette garantie pourtant fondamentale pour contrebalancer les atteintes faites aux droits fondamentaux. La protection des des données et le respect de la vie privée, y compris le « droit à l'autodétermination en matière d'information »[250] des voyageurs, est ainsi particulièrement menacée[251]. De nouvelles garanties pour limiter les atteintes aux droits fondamentaux provoqués par l'utilisation de l'IA dans ETIAS seraient donc les bienvenues.

Chapitre 6. L'amélioration attendue d'ETIAS : la mise en conformité nécessaire du règlement avec les nouveaux garde-fous pour l'utilisation de l'intelligence artificielle

Face aux risques inhérents à l'utilisation de l'IA, l'Union européenne a érigé un ensemble de régulation pour limiter les atteintes aux droits fondamentaux[252]. Ces régulations bienvenues ont permis de compléter les garanties dans l'utilisation de l'IA (**Section 1**), et nécessitent désormais une mise en conformité stricte du règlement ETIAS (**Section 2**).

Section 1. L'adoption de régulations protectrices bienvenues pour la complétude des garanties face aux risques de l'intelligence artificielle

Deux projets de régulations sur l'IA portent des garanties pionnières pour la protection des droits fondamentaux dans ETIAS : la Convention cadre du Conseil de l'Europe qui consacre des grands principes et le projet de règlement du Parlement et du Conseil dont les applications sont plus concrètes.

30. *Les exigences renforcées de l'utilisation éthique de l'intelligence artificielle par la Convention cadre du Conseil de l'Europe*

---

[250] ROBUSTELLI, Ludovica, «Le droit à l'autodétermination informationnelle en droit européen», RDLF 2023 thèse n°02, https://revuedlf.com/theses/le-droit-a-lautodetermination-informationnelle-en-droit-europeen/#note-8260-6 (consulté le 21 mai 2024 à 15h47).

[251] DE TERWANGNE, Cécile, « Les droits fondamentaux à la vie privée et à la protection des données personnelles des migrants et des réfugiés », in Sandrine Turgis (dir.), *Les données numériques des migrants et des réfugiés sous l'angle du droit européen*, Presses universitaires de Rennes, 2020, p. 97-116.

[252] POULLET, Yves, BRONTIDDER, Noémie, « Intelligence artificielle et services publics – le rôle des autorités publiques au service de la « troisième voie » dessinée par la Commission européenne », *Revue générale du droit*, 2022, p. 3-5.

La Convention du Conseil de l'Europe couvre les activités menées dans le cycle de vie des systèmes d'intelligence artificielle qui sont susceptibles de porter atteinte aux droits de l'homme, à la démocratie et à l'État de droit[253]. Si la Convention ne mentionne pas explicitement ETIAS, elle apporte des exigences importantes pour l'utilisation éthique de celle-ci. Ainsi, elle vise à inscrire dans le marbre plusieurs principes pour la protection des droits de l'homme[254] face à l'IA. Nombre de ces principes ont vocation à s'appliquer à ETIAS et peuvent être regroupés au sein de 4 principaux axes.

Ainsi, pour une utilisation éthique de l'IA dans ETIAS au regard de la Convention cadre, il faudrait établir un cadre juridique qui prévoie une procédure à suivre par les autorités publiques pour évaluer l'impact sur les droits de l'homme (1). L'utilisation des systèmes d'IA ne devrait pas seulement être rendue publique en des termes clairs et accessibles, mais aussi que les personnes soient capables de comprendre les décisions prises et la vérification de celles-ci (2). Il faudrait prévoir un cadre indépendant permettant de surveiller la conformité des systèmes aux droits de l'homme et notamment prévenir les risques de discrimination en accordant une protection particulière à certains groupes pour lequel le risque est accru (femmes, enfants, personnes âgées, LGBTI, personnes handicapées, groupes ethniques et religieux…) et assurer la protection des données et le respect de la vie privée, y compris le droit à l'autodétermination de l'information lors du développement, l'apprentissage, la phase d'essai et l'utilisation des systèmes IA (3). Il est également nécessaire garantir le droit de ne pas être soumis à une décision automatisée les affectant de manière significative ainsi que le droit de recours effectif devant une instance nationale, qui implique que les plaintes soient examinées avec un scepticisme approprié à l'égard de la décision automatisée (4). Cette convention récente impose donc de nouvelles exigences à l'utilisation de l'IA, permettant une application éthique et fiable de l'IA dans le règlement ETIAS.

31. *Les garanties pionnières de l'IA Act pour l'utilisation de l'intelligence artificielle*

L'IA Act est une autre régulation visant à assurer une utilisation « sûre, fiable et éthique » de l'IA[255]. Fondé sur l'article 16 du TFUE, le règlement prévoit des garde-fous essentiels pour une utilisation plus tempérée des algorithmes dans la politique de migration et sécurité de l'Union européenne.

---

[253] Article 3 du projet de convention cadre du Conseil de l'Europe.

[254] Commissaire aux droits de l'homme du Conseil de l'Europe, « Décoder l'intelligence artificielle : 10 mesures pour protéger les droits de l'homme », 2019, 26p.

[255] Point (3) du projet de règlement sur l'IA (IA Act).

Pour ce faire, la législation se fonde sur une approche par les risques. Ainsi, l'IA Act distingue les Intelligences Artificielles par les risques qu'elles génèrent - soit "la combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci »[256] - de faible à fort, et prévoit une forte régulation en conséquence, prohibant en son chapitre II les dispositifs les plus dangereux en matière de droits fondamentaux. Il met ainsi en place une approche par les risques qui permet d'adapter le type et le contenu des règles applicables en matière d'IA. Le règlement prévoit donc que les systèmes d'IA utilisés dans la politique de migration, d'asile et de gestion des contrôles au frontières pour évaluer un risque pour la sécurité, pour l'immigration irrégulière ou la santé posé par une personne qui à l'intention d'entrer sur le territoire d'un État membre sont qualifiés de systèmes à haut risque[257]. Le règlement ETIAS entre donc à tout point de vue dans la qualification d'IA à haut risque posée par l'IA Act[258].

À ces systèmes à haut risque s'appliquent des exigences particulières que doivent respecter les concepteurs et déployeurs des IA[259]. La conception et le développement des systèmes d'IA doivent ainsi permettre un contrôle effectif par des personnes physiques visant à réduire les risques pour les droits fondamentaux[260] des utilisateurs. Il faut alors que les personnes effectuant le contrôle des demandes aient conscience de la tendance à se fier automatiquement aux résultats produits par l'IA (biais d'automatisation) et puissent décider de ne pas utiliser le système d'IA[261].

Section 2. La mise en conformité du règlement ETIAS avec les nouveaux garde-fous des régulations européennes

Suite à l'adoption du projet IA Act le 13 mars 2024[262] par les députés européens, et de la Convention cadre sur l'intelligence artificielle le 17 mai 2024[263], EU-lisa travaille pour déceler les

---

[256] Article 3 2) du projet de règlement sur l'IA (IA Act).

[257] Annexe III §7 b) du projet de règlement sur l'IA (IA Act).

[258] Article 6 du projet de règlement sur l'IA (IA Act).

[259] Article 8 du projet de règlement sur l'IA (IA Act).

[260] Article 14 §2 du projet de règlement sur l'IA (IA Act).

[261] Article 14 §4 b) et d) du projet de règlement sur l'IA (IA Act).

[262] Parlement européen, « Intelligence artificielle: les députés adoptent une législation historique » le 13 mars 2024 <https://www.europarl.europa.eu/news/fr/press-room/20240308IPR19015/intelligence-artificielle-les-deputes-adoptent-une-legislation-historique> (consulté le 1er avril 2024 à 10:11).

[263] Conseil de l'Europe, « Le Conseil de l'Europe adopte le premier traité international sur l'intelligence artificielle » le 17 mai 2024 <https://www.coe.int/fr/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence> (consulté le 18 mai 2024 à 9:30).

incompatibilités entre l'utilisation de l'IA par ETIAS et les régulations européennes qui prévoient une mise en conformité du règlement.

32. *De lege lata, l'incompatibilité patente entre ETIAS et les garde-fous des régulations européennes*

L'IA Act et la Convention cadre sur l'utilisation de l'IA ont donc fait ressortir les incompatibilités flagrantes entre une utilisation éthique de l'intelligence artificielle et la mise en œuvre des algorithmes de proflilage des ressortissants étrangers dans le règlement ETIAS.

D'abord, les régulations rappellent que le déploiement d'IA nécessite une étude d'impact des risques pour les droits fondamentaux *ex-ante*[264], ce qui n'a pas été fait avant l'adoption d'ETIAS. De surcroît, il est incertain qu'ETIAS réponde en l'état aux exigences sur la protection des droits fondamentaux[265] comme le droit au respect à la vie privée, la protection des données[266] et la non-discrimination[267] et sur les garanties apportées comme la transparence de l'utilisation d'algorithme[268], le réexamen manuel des demandes d'autorisation de voyage[269], le droit au recours effectif[270] ou le droit de recevoir une explication claire et pertinente sur la décision[271]. En effet, l'algorithme permettant l'établissement d'indicateurs de risques sur la base de statistiques, et le profilage effectué pour comparer les données des demandeurs aux règles de filtrages permettant la prise de décision automatisée sont des systèmes informatiques techniques dont la conformité avec les régulations européennes devra être analysée dans une étude approfondie. Plusieurs indices semblent montrer que ces algorithmes ne sont pas conformes à l'usage éthique et fiable de l'IA.

Ainsi, la première version de l'IA Actl datant de 2021 prévoyait que ses dispositions ne s'appliqueraient pas au règlement ETIAS[272]. Le fait qu'ETIAS soit exempté de mise en conformité à l'IA Act constituait donc un élément important pour penser que le règlement utilise bien de l'intelligence artificielle. Finalement, la dernière version de l'IA Act exige la mise en conformité

---

264 Article 16 du projet de convention cadre du Conseil de l'Europe ; article 27 du projet de règlement sur l'IA (IA Act).

265 Article 82 du projet de règlement sur l'IA (IA Act).

266 Article 4 du projet de convention cadre du Conseil de l'Europe ; article 10 projet de règlement sur l'IA (IA Act).

267 Article 10 du projet de convention cadre du Conseil de l'Europe.

268 Article 8 du projet de convention cadre du Conseil de l'Europe ; article 13 du projet de règlement sur l'IA (IA Act).

269 Article 14 du projet de règlement sur l'IA (IA Act).

270 Article 14 du projet de convention cadre du Conseil de l'Europe.

271 Article 86 du projet de règlement sur l'IA (IA Act).

272 Article 83 de la proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'union du 21 avril 2021, 2021/0106(COD).

d'ETIAS[273]. Les points précis de cette mise en conformité ne sont toutefois pas abordées. EU-Lisa sera donc tenue d'étudier la législation pour faire en sorte que la mise en œuvre d'ETIAS respecte la législation européenne en matière d'IA. Cette injonction laisse donc une place importante à la prospection pour repenser l'utilisation de l'IA dans le règlement.

33. *De lege ferranda, la nécessaire mise en conformité d'ETIAS pour une utilisation éthique de l'IA*

Face à aux nouvelles exigences de l'utilisation de l'IA, le règlement ETIAS devra être mis en conformité sous peine de ne pas respecter le droit en vigueur et d'être sanctionné par les juridictions européennes comme la CJUE et la CEDH. Le projet IA Act de mars 2024 précise que les composantes du système d'information à grande échelle devront se mettre en conformité avec cette régulation avant le 31 décembre 2030. Cette nécessaire mise en conformité vient drastiquement diminuer les possibilités de mises en œuvre d'intelligence artificielle au sein d'ETIAS. Toutefois, d'après Jonas Grimheden, chef du bureau des droits fondamentaux de Frontex interrogé sur l'IA Act, le règlement ne devrait pas modifier en profondeur la mise en service immédiate d'ETIAS qui ne serait en l'état pas doté de tels outils « intelligents »[274].

En effet, les régulations ne devraient pas avoir d'impact immédiat sur le lancement du système ETIAS puisque l'entrée en vigueur de l'IA Act est prévu pour 2026[275], tandis que la mise en conformité des systèmes d'information l'est pour 2030. L'entrée en vigueur de la convention cadre sur l'IA n'a quant à elle pas de date indicative. L'Union dispose donc encore d'années précieuses pour développer des modèles d'IA, mais aussi évaluer la conformité de ses règlements aux nouvelles normes et les ajuster à la marge. La chronologie est donc regrettable compte tenu de l'imminence du danger que représente l'IA pour les droits fondamentaux[276].

Étant donné les tensions qui existent entre ces droits et garanties et la prise de décision automatisée d'ETIAS, il est fort probable d'après la professeure Niovi Vavoula, que différents litiges apparaissent dès la mise en application du règlement. En effet, des recours contentieux seront très probablement menés par des associations de protection des droits de l'Homme ou des ressortissants étrangers victime d'une violation de leurs droits, et pourraient aboutir à des questions préjudicielles devant la Cour de l'Union, comme dans les affaires *Ligue des droits humains* et *Quadrature du net*, qui devra

---

[273] Article 111 du projet de règlement sur l'IA (IA Act).

[274] Voir Annexe 2.

[275] Conseil de l'Union, Chronologie - Intelligence artificielle, 11 janvier 2024 < https://www.consilium.europa.eu/fr/policies/artificial-intelligence/timeline-artificial-intelligence/> (Consulté le 12 mai 2024 à 18h09).

[276] VAVOULA, Niovi, « Tr-AI-nsforming Migration, Asylum and Border Management in the EU », *op. cit.*, p. 24.

alors se prononcer sur les différents points de tension. La CEDH pourrait également sanctionner les États membres dans leur application du règlement, si les garanties qu'il apportent pour le réexamen manuel des demandes ou l'accès aux tribunaux ne sont pas jugées suffisantes.

CONCLUSION GÉNÉRALE

Les États membres ont de grandes attentes envers le renforcement des « Smart Borders » qu'ETIAS est censé apporter. Cependant, ce règlement représente une menace sérieuse pour plusieurs droits fondamentaux protégés par l'Union européenne, tels que le principe de proportionnalité, le droit à la vie privée, la protection des données et le droit à la non-discrimination. Les garanties prévues pour protéger ces droits, comme le traitement manuel subsidiaire des demandes ou la possibilité de faire un recours, semblent insuffisantes au regard des menaces. Pour compléter ces garanties et prévenir les risques générés pour des millions de voyageurs étrangers, une étude consacrée à l'évaluation de l'impact de l'utilisation de l'IA dans le système ETIAS serait la bienvenue.

Une autre interrogation est de savoir dans quelle mesure les algorithmes utilisés dans le système ETIAS pourraient, en l'état et dans le futur, être qualifiés d' « intelligences artificielles » au regard des régulations européennes. Certains signaux vont dans ce sens. La nouvelle version de l'IA Act dispose ainsi qu'ETIAS doit se mettre en conformité avec ses exigences en matière de protection des droits fondamentaux. Si la présomption est donc grande pour faire entrer le règlement ETIAS dans le spectre des régulations sur l'IA, il faudra attendre une telle qualification juridique par des un acte la Commission ou un arrêt de la Cour de justice. Au regard des incompatibilités manifestes entre le règlement et les garde-fous européens, cette qualification devrait être suivie d'une révision partielle du règlement afin de le mettre en conformité avec les normes européennes.

Compte tenu de l'effervescence de l'IA et de ses applications directes notamment à la politique de migration et d'asile, il est nécessaire de surveiller de près les régulations en la matière d'IA. En effet, l'IA Act prévoit que la Commission réexaminera[277] chaque année la régulation afin de permettre le développement des nouvelles technologies tout en régulant les risques engendrés. L'utilisation de l'IA dans le règlement ETIAS, et plus généralement dans la politique de migration et d'asile de l'Union, est donc un sujet complexe sujet à des mutations dans les années à venir, pour lequel la recherche aura un rôle déterminant à jouer en faveur de la protection des droits fondamentaux.

[277] Article 112 du projet de règlement sur l'IA (IA Act).

ANNEXES

Annexe 1 : Entretien avec Théofanis Syrigos, Joris Vankeerberghen, Sasha Madzar, Athanasia Papavasileiou (EU-Lisa) le 29 avril 2024 de 11h à 11h50 via Teams, retranscrit à la main.

[Marc Naro] Do you think it's relevant to talk about AI in ETIAS, or should I say « algorithm » or another word ?

[Théofanis Syrigos] First of all, there is no AI in ETIAS. We did not implement that. We had the intention to, but we did not implement it. As a result, AI has not been implemented. The intention was to use anonymized information from a different system. So ETIAS is fed with anonymized information from the CRRS, the Common Repository for Reporting and Statistics.

And on that basis, we could use AI technologies to support the exercise of risk definition that is feeding into the screening rules of ETIAS. We have done, let's say, we have analyzed this topic. But at the end of the day, we did not proceed because it was not good enough.
We wanted to have more information coming, feeding the technology, in order to support the screening rules. We didn't have this information, so it came directly from the system. We didn't have a legal basis, in fact, to do that.

So AI was not implemented in ETIAS. So that was the previous status. Now, of course, there are discussions at the legal level to see whether we could use more information to feed the technology and therefore the definition of the screening rules. If this regulation will allow us to do that, then indeed, it will make more sense. And then, indeed, we could envisage the implementation. I'd like to give the floor to my colleagues now.

[Joris Vankeerberghen] Well, we are looking at if we implement it, what algorithms we could use, and, indeed, what would be the consequences on the legal aspects. But that is one of the reasons why we are also studying and looking around.

[Sasha Madzar] The ETIAS regulation was obviously adopted before the artificial intelligence regulation came into existence. So you'll see in Article 33 that the ETIAS screening rules are an algorithm, and the algorithm is profiling as defined by the GDPR. Now, in the regulation itself, if

you notice Article 6.3, the last subparagraph, which says an AI system referred to in Annex 3 shall always be considered to be a high risk where the AI system performs profiling of natural persons,. And then, in Annex 3, we have the purpose that ETIAS serves. We're assessing the risk of illegal immigration or something else. Now, the conclusion from that might be that the profiling done by ETIAS is, in fact, something under this limit, but it might also not be. It depends. We need to do further analysis of this in order to actually reach a conclusion on that part. That would be my opinion, but we are very much in the process of analyzing the Artificial Intelligence Act. So we need to go into further detail in order to provide conclusive answers.

[Joris Vankeerberghen] Actually, we will provide statistics. And based on these statistics, the Commission will set, if I understood it well, a delegating or implementing act that says which are the risk factors. So very concretely, if we have for a certain set of travelers, for example, that they are overstaying more than the average, say by 5%, then they will consider this a risk factor. And based on that, Frontex will start using this risk factor in the screening of the ETIAS applications that come in over the Internet. So there are actually a lot of human steps involved. We'll have to investigate a bit deeper, but at this stage it most probably won't be considered AI.

[Théofanis Syrigos] Yes, I confirm. In fact, the Commission already designed those implementing and delegated acts, if I may be more precise. Because any act touching sensitive human information that has to do with fundamental rights, screening, risks, and all these things is considered a delegated act. It goes for approval through a different process. Let's put it this way. And indeed, this act is defining how and why Frontex exists.

Frontex will be chairing the screening, or so-called screening board. As you have seen in the ETIAS regulation, it will be the same in the revised regulation. This board will, in fact, address the screening aspects of these two systems, ETIAS and revised. It will be composed by the Member States, and I think the Fundamental Rights Agency will be consulted as well. And they will consolidate the information coming either from us, through statistics and reporting, or from different other sources. And on that basis, for example, they consult the World Health Organization.

So they will consolidate feedback from different sources. They will set the different risk indicators, and on that basis, through the software that we give them, they will set the screening rules into ETIAS and, in the future, into this. As you can see, this process involves human intervention rather

than the use of artificial intelligence. It's not AI at all, at least not now. Yes, we do want to design and implement such a technology. So the way the regulations were constructed didn't allow us to properly use the technology. Technology wouldn't do anything because there is missing information, which we're not legally allowed to assess. For instance, assessing the city of residence is prohibited.So AI couldn't do that much, even if we had it.

[Marc Naro] So according to you, why is there an article in the new AI Act, Article 111, that requires ETIAS regulations to comply with the new rules of the AI Act?

[Théofanis Syrigos] We are currently conducting an assessment.. As Sasha mentioned, we have a thorough understanding of the Act and are currently evaluating its potential impact.. So, in this case, we clearly need to comply with the AI Act. So in the future, if the other regulations that will allow us to, in fact, allow the agency and the technology to use information—more information, sorry—than the one we have now, then we clearly, yes, have to comply with the provisions of the AI Act.

[Marc Naro] How would you comply with the IA Act? There will be changes to the ETIAS regulation.

[Joris Vankeerberghen] Indeed, if you read the ETIAS regulation today, it has already, in some way, taken into account all the potential risks associated with the implementation of AI algorithms. And that's why you have screening boards that can consult the fundamental rights body. So there are steps in there to, I mean, you mentioned bias. So if we start using these algorithms, they should be taken up, or at least detected, by the different bodies that are created. Therefore, an algorithm will never make a direct decision. That's also clearly written in the basis. Even if we use algorithms to assist individuals at the border in making decisions, we can identify any potential bias or issues early in the process, before we implement them in real-world scenarios.

[Athanasia Papavasileiou] The idea behind using an AI in ETIAS was not further explored until the future. We were also waiting for the AI to set the constraints. In order to have the Frontex and the ETIAS central unit define the screening rules, the way to analyze the various statistics and results from the database might employ an AI. So that the AI could more easily identify trends. see certain risks, and propose certain valid screening rules for Frontex to evaluate and see if they are indeed valid and can be verified and then introduced in the system.

If they were to be introduced in the system, then the system would employ some filtering of persons that fall under a specific screening rule that says, If you are under this nationality and you are of this age, etc., you might produce a hit because it has been verified and we have set this screening rule. But nothing would mean that it would come directly from an AI that this person is considered a risk.

[Marc Naro] So, as you've said, there are still things to be adjusted in order to implement ETIAS. Will ETIAS be available in 2025 and what are the main issues with implementing ETIAS? What are the issues that made it take so much time to implement ?

[Théofanis Syrigos] First of all, this year we implemented Entry-exit. For ideas, by the end of the year, we will only declare technical readiness. The actual entry into operation, as you rightly said, is spring next year, and it's not our decision. The Member States, together with the Commission, will decide on that. And indeed, this year, EU-Lisa will deliver entry-exit. In fact, we will declare readiness in July, a few months from now. But indeed, as you rightly said, because of the Olympics and other events, it's up to the community, the Member States, and the Commission to decide when exactly entry-exit will enter operations. This will happen in October or November of this year.

We will be technically ready by the end of the year. What does "technically ready" mean? That we are ready at the central level, that we have done testing with the Member States, with the central unit also, testing of the system, of the processes, of various things. However, the actual entry into operation will be determined by the Commission. And it will happen in spring, somewhere in spring next year. The reason that we had delays was in fact that ETIAS, as a system, needs information from entry-exit in order to function. For example, it needs the overstayer information or other information stored in entry-exit, exactly for the risk definition screening rules, for the automated process as well. And that's why there must be a distance between the entry into operation of the two systems. So first comes Entry-exit, which collects a lot of information, and after a while, ETIAS will start receiving this information via the interoperable systems to use it for its own processes.

Therefore, the issue is not with ETIAS itself, but rather with the need to establish a first entry-exit system. ETIAS implementation goes well. In fact, as we speak, we are in the process of conducting extensive testing at the central level. Very, very soon; in fact, as we speak, we are doing pilot testing

with some of the member states. And in the summer, we will do compliance testing with them. And we will continue, of course, with business end-to-end testing and all these things.

[Marc Naro] What is the exact role of EU-Lisa ? Does it have a political role in the negotiation of the implementation ? Is ETIAS a European ESTA ?

[Théofanis Syrigos] In fact, we are not part of the negotiations when the co-legislators, who are in fact the Member States, are at different levels: the Commission and the institutions. Except for the Commission, Council, Parliament, and so on. So, during that process, they negotiate the provisions of each system. The various articles, the system's actions, etc. I believe that during this process, indeed, they take into account what is happening in other countries, like the US, Canada, or Australia.

I believe they do that, but they also do so because they identify the gap. The very existence of ETIAS is, in fact, to close the information gap and add more value to the concept of freedom of movement, security, etc. You know, in the past, what is happening now is that we didn't have systems at the European level to manage the entry and exits. It was based on passport stamps, as well as, of course, national implementations. Of course, we had central systems to individually check some elements, like the visa. Or at the national level, borders or other authorities were checking against the SIS, the Schengen Information System.

But there was no system to capture the actual entry and exit, calculate the remaining stay, and, therefore, create an overstayor thing. So, now, this system is coming. The entry-exit is coming. And then, ETIAS is coming in order to cover the visa-exempt spectrum of third-country nationals. It has similarities. Of course, you will have a website to log in to and provide information on in order to apply for ETIAS. It has a payment service similar to ESTA.

It will have a mobile app. There will be automation in the background. You know, a lot of activities have similarities. But, in fact, we at EU-LISA were simply given the regulation and the implementing acts, and they told us to do it. As a result, you know, we are not consulted as member states. We do not go further.

[Marc Naro] Regarding the importance of the data you will manage, how do you prepare for cyberattacks or cybercrime?

[Joris Vankeerberghen] This is, of course, a bit of a broader context, but, I mean, we apply; in general, we do risk analysis. Then, based on the risk, we take potential countermeasures to minimize it. But, very concretely, we have to see that we do not go too far to disclose too many things. But we basically isolate as much as we can the entire database from all the rest.

So, only member states have access, and then only authorized persons within the member states. So, that's one of the biggest measures we take. Besides, there are all the normal IT security measures taken, like simple things like firewalls, authentication, identity and access management, and encryption. So, there's a whole set of measures we take to prevent any cyberattacks, and they're all, let's say, put together in our security plans. They are looked at by our political masters, NGOs, and member states. So, everybody has a say in that, but it's a big topic, I mean, it's not something we can clarify in one minute.

[Marc Naro] At EU-LISA, what are the measures your unit takes to protect the data and the right to privacy?

[Joris Vankeerberghen] Yeah, so we have indeed had a security unit involved all along the way. So, for example, I'm more on the IT side of things, so we do security by design. In every step of the system we develop, we ensure that there are security controls in place. Besides that, our security unit will look at security requirements and security plans. For example, if we have an issue, there are plans and procedures in place to mitigate it as quickly as possible. We need to ensure the data, because one of the cyber attacks that could happen is that they try to make the data unavailable, which could have very serious effects on the border controls.

We also make sure that we have, for example, a secondary site. So, in case we have issues on the primary site, we immediately fall back to the secondary site. So, we look at availability, we look at the integrity of the data to make sure it's not manipulated, and we look at ensuring it stays confidential as well. These are typically the three big axes in cybersecurity. And at all levels of the IT system, both technical and procedural, we make sure that there are things in place to prevent any malicious cyber attacks against our data and systems.

[Marc Naro] What are the relations between EU-Lisa and ETIAS national units ? Because I know there will be different implementations of central national units.For instance, in France, it's the SNEAV that will be inside the Minister for Internal Affairs, while it could be for the Minister of Foreign Affairs. So, how are you discussing this with national units so that ETIAS will apply uniformly in all European Union countries ?

[Athanasia Papavasileiou] Yes, of course. So, the requirements for how the ETIAS national units manage workflows and do manual processing are set up in the regulations, so we cannot deviate from them. Of course, over the years, we haven't simply read the text of the legal base, but we have had multiple meetings with member states and Frontex, who is also coordinating an effort to provide processes and align the ETIAS national units among them.

So, this is a preparation that has started for many years and continues until the entry into operation. The legal basis does allow for different setups of the ETIAS national units. It can be divided into different ministries. It can be under different buildings. In any case, the way that the ETIAS has been implemented allows, from a technical perspective, to accommodate all the different configurations that the member states have decided to follow. There are some general rules that are respected, and after that, it is a national competency and the decision to organize themselves in one way or another.

[Marc Naro] I read that some professors in the literature said that ETIAS and EES are serving the same role. What are the links between the two regulations?

[Théofanis Syrigos] First of all, the EES is exactly as the word says, capturing the entry and the exit. EES is not there to be consulted in order to give information to a visa holder, a person who is requesting a visa, or, in the future, a person who is visa exempt and therefore is requesting ETIAS.

Therefore, there is no such equation as whether EES is there, so we don't need ETIAS. EES is there to ensure that the border guards and, of course, other authorities are there, but let's focus now on the borders. We have the right tool in place in order to capture the entry and exit, the right tool in order to allow them to calculate the authorized stay, whether it is for a visa exempt or for the visa exempt crossings, or it will consult, as it does, with VIS, the visa information system, in order to receive

information for the visa holders. Therefore, when we discuss whether a responsible authority or competent authority needs to take a decision on granting a visa, they will go to the VIS.

Imagine a consulate of France in the US; they will follow the procedures as they do today. The big difference with entry-exit is that when somebody applies for a visa, the consulate will send the request to the French national system. They will do the standard proceedings, but also, at the central level, VIS will consult entry-exit and see if this person asking for a visa still has authorized remaining time in the Schengen Area. If not, it will inform. If yes, it means you still have a few days to spend. Same with ETIAS. When the automated processing is done, there is information on whether the person consumed or not; they are allowed to stay within Europe, within Schengen. Both regulations play a different role.

[Marc Naro] Ok, but ETIAS will use EES information, so they are really linked, even if ETIAS doesn’t target visa travelers.

[Théofanis Syrigos] EES doesn't have screening rules. EES doesn't have risk indicators. EES doesn't have a watch list, for example. Those things are not in entry-exit. ETIAS is more than an IT system. We have all of the national units that do a sort of consultation before granting travel authorization in case of a hit. They populate the watch lists. They work with ETIAS in the background. Entry-exit doesn't do that.

[Marc Naro] Regarding the transparency of screening rules and decisions, I know that the Commission and Frontex will establish the risk indicators. I don't think that the public will be able to know what the risk indicators are, so do you think that we should implement more transparency ?

[Joris Vankeerberghen] At the end of the day, EU Lisa provides the technology in accordance with the regulations. We are not the ones setting the screening rules or the risk indicators. This is done by the screening board, and I believe within the screening board there are procedures in place to cover the elements that you just mentioned. In fact, it's not that much on us. I believe the European Data Protection Supervisor is also involved. On our side, indeed, we make sure that we design systems that respect privacy and all data protection matters.

And concerning transparency, I believe that, indeed, it is a topic to be covered under the Frontex and screening board with the parties involved there on how they publicly inform and how they set the different rules in the system. I don't think they can do everything because some of the elements are very sensitive, in particular when it comes to the risks of terrorism. However, we are not involved in this topic. We are service providers. If you allow me to use this expression, we deliver the system; they do what they have to do.

[Marc Naro] And, as a service provider, are you collaborating with Frontex to implement ETIAS?

[Théofanis Syrigos] We have governance in place. The regulation clearly defines the procedures for the advisory group and the program management board. Indeed, the management board of EU-LISA is the ultimate decision body. Frontex is present on our management board. And now, if you go a level lower to the governance bodies, in the advisory group itself, Frontex is present. So, I am chairing the entry-exit ideas advisory group. In all of our meetings, we have Frontex colleagues present. Furthermore, when they organize meetings to analyze aspects between the central unit and the national unit, we are also invited. On the program management board, also established by the regulation, Frontex is present. So, we have the member states, Frontex, and the commission chairing. So, the collaboration is clearly regulated and well-functioning.

Annexe 2 : Échanges de courriels avec Jonas Grimheden (Frontex) le 12, 17 et 18 avril 2024.

[Marc Naro] ETIAS regulation was scheduled to enter into law in 2020. Now, we are talking about 2025. According to you, what are the reasons why the implementation of the ETIAS Regulation take some much time. Furthermore, Article 111 of IA Act provides that ETIAS (Annex 10) should comply with the new guarantees implemented by IA Act. Thus, could ETIAS it be postponed again ? Will it be rewritten ? If so, which articles should/will be rewritten ?

[Jonas Grimheden] The reasons for the delays have been technical, in terms of development of the required IT tool at an EU level, concerns to be ready on time by Member States, and most recently, the risk of rolling out the system just before the Paris Olympics. I do not think it will be delayed further. The AI Act sets requirements that ETIAS will have to comply with should they apply AI. So far, there are no such technology in place. So in that sense, I don’t see any likelihood or postponement or redrafting of any sort.

[Marc Naro] I would like to emphasize in my Master thesis the extraterritorial nature of this regulation, which will be applied before the travel of passengers towards Europe. According to you, is it realistic to believe that foreigners will have an effective judicial remedy as they will be far away from jurisdiction ?

[Jonas Grimheden] There should be an effective judicial remedy (something we discussed at the meeting mentioned above earlier this week, and something we have a Guidance Note under development on). This is easy in theory but could very well cause problems at national level, where national rules set limitations on how complaints may be made. The ETIAS Fundamental Rights Guidance Board will with the forthcoming Guidance Note stress the risks involved here. ETIAS has conducted a overview of the available complaints mechanisms, which will be helpful in this regard.

[Marc Naro] Do you think ETIAS comply with the « clear and precise » human review criteria posed by CJEU with C-817/19 - *Ligue des droits humains* ?

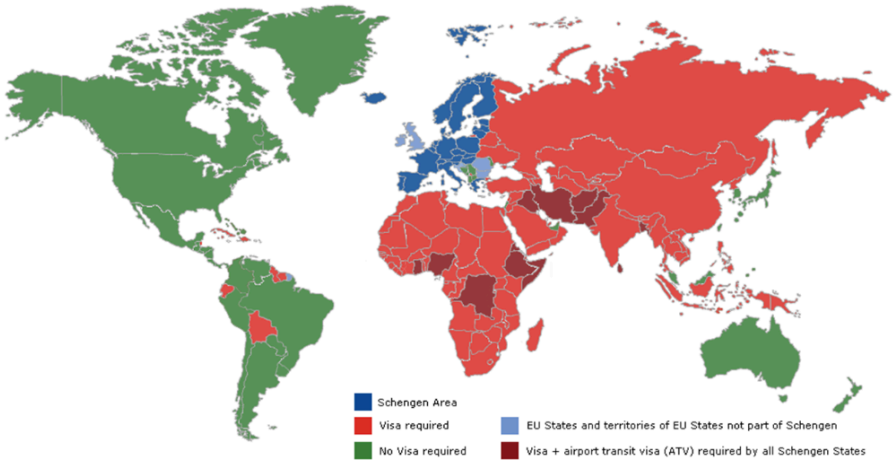
[Jonas Grimheden] I don't expect the clear and precise criteria to be an issue with ETIAS. It is fairly clear what the fundamental rights issues are and the Guidance Board can further clarify this if needed.

[Marc Naro] Frontex has been condemned couple of times for violation of human rights. Which measures are or should be granted to insure that there will be no interferences between Fundamental Right board and ETIAS Regulation ?

[Jonas Grimheden] Condemned by a court no, but criticised by a range of different actors, yes. And there have been many problems. What I can see from three years of intensive work (65 staff members, some 2,000 days in the field, 100 return flights directly monitored and much more), Frontex involvement in fundamental rights violations are indirect, and where possible the Agency is quick to adjust. The issue is rather with the national authorities in the countries where Frontex is operating. Here I have much less jurisdiction and surely much less leverage. As for ETIAS specifically, it is rather clear to me that with the mandate of the Guidance Board as well as my direct mandate, any fundamental rights issues should be resolvable. There may still be challenges with the

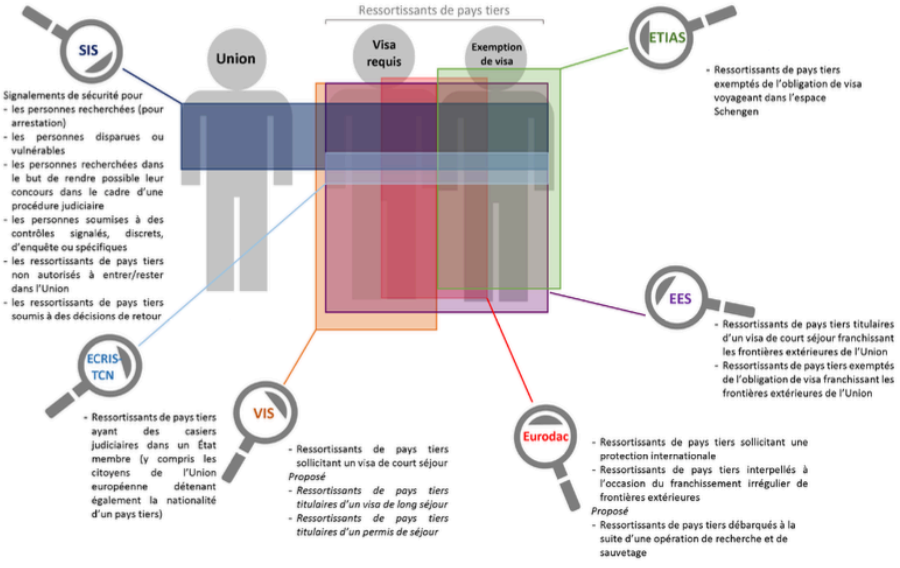
Member States, such as with access to remedy or attempts to use the system in an incorrect way, but also here I would think the safeguards are sufficient to be able to redress these.

<u>Annexe 3</u> : Cartographie des pays d'origines des ressortissants étrangers exemptés de visa.



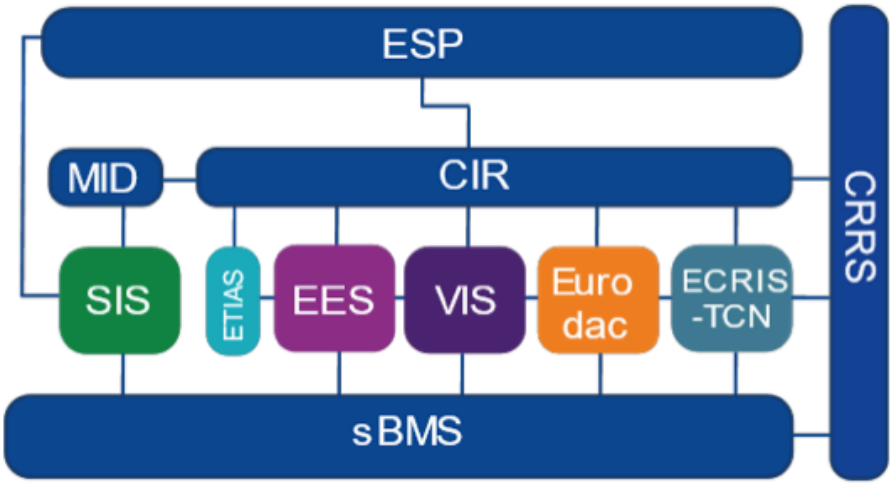
Source : PwC « Feasibility Study for a European Travel Information and Authorisation System (ETIAS) », Final Report, 16 novembre 2016, 281p.

<u>Annexe 4</u> : Représentation des différents systèmes d'information collectant des données sur les ressortissants étrangers.



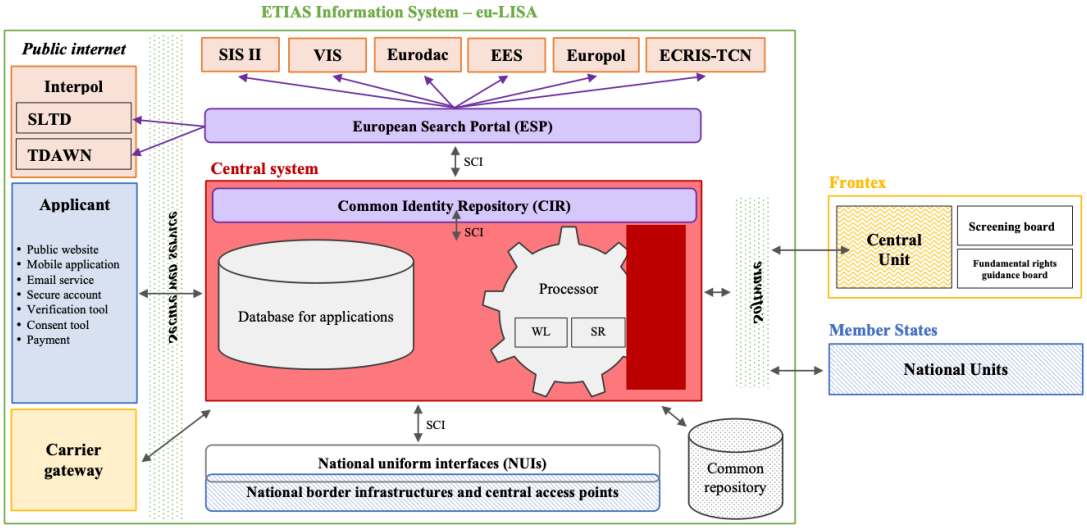
Source : PwC, Feasibility Study for a European Travel Information and Authorisation System (ETIAS), Final Report, 16 novembre 2016, 281p.

Annexe 5 : Schématisation de l'architecture du système interopérabilité de l'Union européenne.



Source : Eu-Lisa, Identity Management at eu-LISA eu-LISA Industry Roundtable, 16th June 2022, 26p < https://eulisaroundtable.eu/eulisa_content/uploads/2022/06/4_Istvan-Racz-FINAL.pdf>.

Annexe 6 : Schématisation du fonctionnement interopérable d'ETIAS.



Source : DERAVE, Charly, GENICOT, Nathan, HETMANSKA, Nina, « The risks of trustworthy AI - The case of ETIAS », *European journal of risk regulation*, 13, 3, 2022, p. 399.

BIBLIOGRAPHIE

Chapitre 1 : Documentation officielle

I. Documentation officielle internationale

A. Nations Unies

1. Convention

Convention internationale des Nations Unies pour l'élimination de toutes les formes de discrimination raciale, résolution 2106, 21 décembre 1965.

2. Rapports et études

Haut Commissariat des Droit de l'Homme des Nations Unies, « Digital Border Governance : a Human Rights Base Approach », Université d'Essex 2023, 25p.

B. Conseil de l'Europe

1. Projet de convention

Conseil de l'Europe, Projet de convention cadre sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'Etat de droit du 15 mars 2024, CM(2024) 52-prov1.

2. Rapports et études

Conseil de l'Europe, « Guide on Article 8 of the European Convention on Human Rights – Right to Respect for Private and Family Life, Home and Correspondence », 2019, p.150p.

Conseil de l'Europe, « Discrimination, Artificial Intelligence, and Algorithmic Decision-Making », 2018, 75p.

Commissaire aux droits de l'homme du Conseil de l'Europe, « Décoder l'intelligence artificielle : 10 mesures pour protéger les droits de l'homme », 2019, 15p.

3. Jurisprudence de la CEDH

Roman Zakharov c/ Russie, Requête n° 47143/06, 4 décembre 2015.

Çelik et İmret c.Turquie, Requête n° 44093/982004, 26 octobre 2004.

Akdivar et autres c. Turquie, Requête n°21893/93, 18 décembre 1996.

C. États non membres de l'Union européenne

Parlement canadien, règlement modifiant la loi sur l'immigration et la protection des réfugiés (LIPR), Section 11 (1.01), 30 juin 2017.

Congrès américain, Act to provide for the implementation of the recommendations of the National Commission on Terrorist Attacks Upon the United States, Public Law 110-53, 3 août 2007.

II. Documentation officielle de l'Union européenne

A. Droit primaire

Traité sur le fonctionnement de l'Union Européenne, version consolidée du 7 juin 2016, *JOUE* C 202.

Traité sur l'Union Européenne, version consolidée du 26 octobre 2012, *JOUE* C 326.

Charte des droits fondamentaux de l'Union européenne, version consolidée du 7 juin 2016, *JOUE* C 202/389.

B. Droit dérivé

2. Directives européennes

Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, *JOUE* L 88/6.

Directive (EU) 2016/680 du Parlement Européen et du Conseil du 27 April 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, *JOUE* L 119/89.

Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, *JOUE* L 261/24.

1. Règlements européens

Règlement (UE) 2021/1152 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (CE) no 767/2008, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861 et (UE) 2019/817 en ce qui concerne l'établissement des conditions d'accès aux autres systèmes d'information de l'UE aux fins du système européen d'information et d'autorisation concernant les voyages, *JOUE* L 249/15.

Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) no 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil, *JOUE* L 135/27.

Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006, *JOUE* L 312/14.

Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) no 1077/2011, (UE) no 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226, *JOUE* L 236/1.

Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) no 767/2008 et (UE) no 1077/2011, *JOUE* L 327/20.

Règlement (UE) 2016/679 du Parlement européen et 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), *JOUE* L 119/1.

Règlement (UE) No 603/2013 du Parlement 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), *JOUE* L180/1.

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), *JOUE* L 218/60.

3. Propositions de règlements européens

Résolution législative du Parlement européen du 13 mars 2024 sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), *JOUE* T9-0138/2024.

Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union du 21 mars 2021, 2021/0106 (COD).

4. Actes délégués

Décision déléguée (UE) 2023/2424 de la Commission du 28 juillet 2023 précisant le contenu et la forme des questions et définissant l'autre ensemble préétabli de questions pour le système européen d'information et d'autorisation concernant les voyages (ETIAS) conformément à l'article 17, paragraphes 5 et 6, du règlement (UE) 2018/1240 du Parlement européen et du Conseil, *JOUE* C 2023/4972.

5. Actes exécutifs

Décision d'exécution (UE) 2022/102 de la Commission du 25 janvier 2022 établissant des formulaires de refus, d'annulation ou de révocation d'une autorisation de voyage, *JOUE* L 17/59.

6. Avis

a) Comité Européen de la protection des données

Comité Européen de la Protection des Données, « Observations formelles du CEPD sur le projet de décision déléguée de la Commission visant à préciser le contenu et la forme des questions et à définir l'autre ensemble préétabli de questions », 3 août 2022, 5p.

Comité Européen de la Protection des Données, « Observations formelles sur le projet de décision déléguée de la Commission visant à préciser les risques en matière de sécurité ou d'immigration illégale ou le risque épidémique élevé », 7 juin 2021, 3p.

Comité Européen de la Protection des Données, « Avis du CEPD sur l'AIPD de l'ETIAS », Dossier 2021-0640, 13 septembre 2021, 16p.

Comité Européen de la Protection des Données, « Avis 4/2018 sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE » , 16 avril 2018, 38p.

Comité Européen de la Protection des Données, « 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) », 6 mars 2017, 30p.

b) Comité Economique et Social Européen

Comité Economique et Social Européen, « Avis sur la proposition de règlement du Parlement européen et du Conseil ETIAS », 2017/C 246/28, 6p.

C. Communication

Commission européenne, « Favoriser une approche européenne en matière d'intelligence artificielle » (Communication) COM (2021) 205 final 4, 21 avril 2021, 11p.

Commission européenne, « White paper on Artificial Intelligence – A European approach to excellence and trust » COM (2020) 65 final, 19 février 2020, 26p.

Commission européenne, « Building Trust in Human-Centric Artificial Intelligence » (Communication) COM (2019) 168 final 1, 8 avril 2019, 10p.

Commission européenne, « Un plan coordonné dans le domaine de l'intelligence artificielle » (Communication) COM (2018) 795 final, 25 avril 2018, 10p.

Commission européenne, 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) n° 515/2014, (UE) 2016/399, (UE) 2016/794 et (UE) 2016/1624, COM (2016), 731 final, 90p.

Commission européenne, « Frontières intelligentes: options et pistes envisageables », COM (2011) 680 final, 25 octobre 2011, 16p.

Commission européenne, «Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne » COM (2008) 69 final, 13 février 2008, 10p.

E. Document de travail des services de la Commission

Commission européenne, « Staff Working Document: Better Regulation Guidelines », SWD (2015) 111 final, 89p.

F. Rapports et études émanant des institutions

1. Agence des droits fondamentaux de l'Union Européenne :

European Union Agency for Fundamental Rights,, « Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement », 2019, 34p.

European Union Agency for Fundamental Rights,, « #BigData: Discrimination in data-supported decision-making », 2018, 12p.

European Union Agency for Fundamental Rights, « Fundamental rights and the interoperability of EU information systems: borders and security », 2017, 50p.

2. EU-Lisa

EU-Lisa, « Single Programming Document 2023-2025 », Document 2022–414 REV 1, 135p.

EU-Lisa, « Artificial Intelligence in the Operational Management of Large-scale IT systems », Research and Technology Monitoring Report, July 2020, 36p.

EU-Lisa, « AI in CSSR in the content of ETIAS and the revised VUS final report », 2022, Document non publié.

3. Europol

Europol, « European Union Terrorism Situation and Trend Report 2016 », TE-SAT Report, 2016, 60p.

G. Rapports et études d'experts pour le compte des institutions:

1. Commission européenne

Deloitte, « Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security » . vol. 1: Main Report, 2020, 128p.

PwC, « Feasibility Study for a European Travel Information and Authorisation System (ETIAS) », Final Report, 16 novembre 2016, 238p.

2. Parlement européen

DUMBRAVA, Costica, « L'intelligence artificielle aux frontières de l'Union européenne: aperçu des applications et questions clés », *European Parliamentary Research Service* 2021, 50p.

DUMBRAVA, Costica, « Advance passenger information (API) to enhance border checks », The 'EU Legislation in Progress' Briefing, 2023, 6p.

VAN MOENSEL Lieve, et NEVIL, Nissy, « What if your emotions were tracked to spy on you ? », *European Parliamentary Research Service*, mars 2019, 2p.

VAVOULA, Niovi, JEANDESBOZ, Julien, ALEGRE, Susie, « European Travel and Authorisation System (ETIAS) : Boarder management, fundamental rights and data protection », Étude pour la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, 60p.

D. Jurisprudence de la CJUE

OQ v SCHUFA Holding, C-634/21, 7 décembre 2023.

Ligue des droits humains ASBL v Conseil des ministres, C-817/19, 21 juin 2022.

La Quadrature du Net and Others v Premier Ministre, C-511/18, 6 octobre 2020.

Opinion 1/15 of the Court (Grand Chamber) on the EU/CANADA PNR Agreement, 26 July 2017.

Tele2 *Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and others,* C-203/15 et C-698/15, 21 décembre 2016.

David L Parris v Trinity College Dublin, C-443/15, 24 novembre 2016.

CHEZ Razpredelenie Bulgaria v Anelia Nikolova, C-83/14, 16 juillet 2015.

Digital Rights Ireland Ltd v Minister for Communications, *Marine and Natural Resources and others and Ka¨rntner Landesregierung and others*, C-293/12 et C-594/12, 8 April 2014.

E. Jurisprudence nationale

Census Acte case, BVerfG 209/83, 15 décembre 1983.

III. Documentation officielle nationale:

A. Actes juridiques

Décret n°2022-963 du 29 juin 2022 relatif aux modalités de contestation des refus d'autorisations de voyage et des refus de visas d'entrée et de séjour en France *JORF* n°0151.

Décret n° 2021-1138 du 1er septembre 2021 portant création d'un service à compétence nationale dénommé « service national des enquêtes d'autorisation de voyage », *JORF* n°0204

B. Rapports d'experts

France Diplomatie « Propositions pour une amélioration de la délivrance des visas », Rapport Paul Hermelin, Mission Visas, Avril 2023, 36p.

Chapitres 2. Doctrine

I. Ouvrages intégraux

GÉLIN, Rodolphe, « Dernières nouvelles de l'Intelligence artificielle », Flammarion, Paris, 2022, 160p.

LATIL, Arnaud, *Le droit numérique une approche par les risques*, Lefebvre-Dalloz, Paris, 2023, 276p.

MEHDI, Rostane (dir.), L'Agenciarisation de la politique d'immigration et d'asile, collection confluences, 2020, 153p.

TINBERGEN, Jan, Techniques modernes de la politique économique, Paris, Dunod, 1961, 250p.

VAVOULA, Niovi, *Immigration and Privacy in the Law of the European Union*, Leiden, Brill, 2022, 780p.

II. Contributions d'ouvrages

DE TERWANGNE, Cécile, « Les droits fondamentaux à la vie privée et à la protection des données personnelles des migrants et des réfugiés », in Sandrine Turgis (dir.), *Les données numériques des migrants et des réfugiés sous l'angle du droit européen*, Presses universitaires de Rennes, 2020, p. 97-116.

DEN HERTOG, Leonhard, « Fundamental Rights and the Extra-Territorialisation of E.U. Border Policy : a contradiction in terms ? », in Didier Bigo, Sergio Carrera, Elspeth Guild (dir.), *Foreigners, Refugees or Minorities ? Rethinking People in the Context of Border Controls and Visas*, Ashgate, Farnham, 2013, p. 205-226.

GAZIN, Fabienne, « Le développement de la "biométrisation" des migrants dans l'Union européenne : au mépris du principe de finalité et au service de la lutte contre l'immigration irrégulière », in Frédérique Berrod (dir) *Europe(s), droit(s) européen(s) : une passion d'universitaire*, Bruxelles, Bruylant, 2015, pp. 209-221.

JEANDESBOZ Julien, « Logiques et pratiques de contrôle et de surveillance des frontières de l'Union européenne », in Amandine Scherrer, Emmanuel-Pierre Guittet et Didier Bigo (dir.) *Mobilités sous surveillance: Perspectives croisées UE-Canada, Athéna éditions*, Balma, 2009, p. 149-164.

MICHÉA, Férédrique, « Les finalités des systèmes d'information européens à vocation migratoire », in Sandrine Turgis (dir.), *Les données numériques des migrants et des réfugiés sous l'angle du droit européen*, Presses universitaires de Rennes, 2020, p. 37-63.

PESCH, Paulina, DIMITROVA, Diana, BOEHM, Franziska, « Data Protection and Machine-Learning-Supported Decision-Making at the EU Border: ETIAS Profiling Under Scrutiny », in Gryszczyńska, A., Polański, P., Gruschka, N., Rannenberg, K., Adamczyk, M. (eds) *Privacy Technologies and Policy*. APF 2022, p. 50-72.

TURGIS, Sandrine, « Les systèmes d'information à grande échelle au carrefour de la politique du numérique et des politiques en matière d'asile, d'immigration et de contrôle des frontières », in Bertrand Brunessen (dir.), *La politique européenne du numérique,* Bruylant, Bruxelles, p. 442-456.

THIERY, Sylvain, « La place grandissante des outils numériques en matière migratoire à la lumière de la réforme du règlement Eurodac », in Bertrand Brunessen (dir.), *La politique européenne du numérique,* Bruylant, Bruxelles, p. 457-472.

VAVOULA, Niovi, « You (Probably) Are Who I Say You Are– ' ETIAS and the Fourfold Paradigm Shift in the Operationalisation of Information Systems », in Niovi Vavoula (dir.) *Immigration and Privacy in the Law of the European Union*, Leiden, Brill, 2022, p. 467-539.

III. Articles de revue

A. Articles publiés

BEDUSCHI, Ana, « International migration management in the age of artificial intelligence », *Migration Studies*, Vol. 9, 2021, p. 576-596.

BIGOT, Didier, « Sécurité et immigration : vers une gouvernementalité par l'inquiétude ? », *Cultures & Conflits*, Vol. 32, 1998, p.13-38.

BIGOT, Didier, « L'immigration à la croisée des chemins sécuritaires », *Revue européenne des migrations internationales*, Vol. 1, 1998, p.25-46.

BROM, Frans, BESTERS, Michiel, « ‘Greedy’ Information Technology: The Digitalization of the European Migration Policy, » *European Journal of Migration and Law,* Vol. 12, 2010, p.455–470.

BRIGANT, Jean-Marie, « Les risques accentués d’une justice pénale prédictive », *Archives de philosophie du droit,* Vol. 60, 2018, p.237-251.

BROUWER, Evelien, « Schengen and the Administration of Exclusion: Legal Remedies Caught in between Entry Bans, Risk Assessment and Artificial Intelligence », *European Journal of Migration and Law*, Vol. 23, 2021, p.485-507.

CHASSIN, Catherine-Amélie, « Un nouveau venu numérique : l’ETIAS », *Cahier de la recherche sur les droits fondamentaux*, 2023, p.61-71.

CRASSEGGER Céline, « Comment l’Union européenne fait-elle face aux défis que représente la lutte contre le terrorisme et la radicalisation ? », *Cahiers de la sécurité et de la justice*, 2022, p. 86-97.

DERAVE, Charly, GENICOT, Nathan, HETMANSKA, Nina, « The risks of trustworthy AI - The case of ETIAS », *European journal of risk regulation*, 2022, Vol. 13, p. 389-420.

DELMAS-MARTY, Mireille, « L’ambivalence des nouvelles technologies », *Droit, sciences et techniques, quelles responsabilités ?*, *LexisNexis*, 2011, pp. 8-9.

EBERS, Martin et al., « The European Commission’s Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS) », *J,* Vol. 4, p.589-603.

FERRER, Xavier et al. « Bias and Discrimination in AI : A Cross-Disciplinary Perspective », *Computers and Society*, Vol. 40, 2020, p.72-78.

GANDHI, Shrutika, « Frontex as a hub for surveillance and data sharing: Challenges for data protection and privacy rights », *Computer Law & Security Review:The International Journal of Technology Law and Practice*, Vol. 53, 2024, p.1-10.

GUGLIOTTA, Lorenzo, ELBI, ABDULLAH, « Will AI ‘subtly’ take over decision-making in the EU migration context? Warnings and lessons from ETIAS and VIS », *2023 EULEN Conference on AI Systems and Enforcement: Between Effectiveness and the Rule of Law,* 2023, p.1-26.

GREMSL, Thomas, HODL, Elisabeth, « Emotional AI : Legal and Ethical Challenges », Information polity, Vol. 27, 2022, p.163-174.

JOHN NILSSON, Nils, « Probabilistic Logic », *Artificial Intelligence*, Vol. 28, 1986, p.71–88.

KADIRESAN, A., BAWEJA, Y., OGBANUFE, O, « Bias in AI-Based Decision-Making », *Bridging Human Intelligence and Artificial Intelligence*, 2022, p.279-301.

KOULISH, Robert, « Immigration Détention in the Risk Classification Assessment Era », *Connecticut Public Interest Law Journal*, Vol. 16, 2016, p.1-35.

LEPRI, Bruno et al. « Fair, Transparent, and Accountable Algorithmic Decision-Making Processes. », *Philosophy & Technology,* Vol. 31, 2018, p.611-627.

MARIN, Luisa, « The Cooperation Between Frontex and Third Countries in Information Sharing: Practices, Law and Challenges in Externalizing Border Control Functions », *European Public Law,* Vol. 26, 2020, p.157-180.

MCCARTHY, J., MINSKY, M. L., ROCHESTER, N., & SHANNON, C. E., « A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence », *AI Magazine*, Vol. 27, 1955, 14p.

MEHRABI, Ninareh, et al. « A Survey on Bias and Fairness in Machine Learning », *ACM Computing Surveys,* Vol. 54, 2021, 35p.

MICHÉA, Frédérique, ROUSVOAL, Laurent, European Papers, « The Criminal Procedure Out of Itself: A Case Study of the Relationship Between EU Law and Criminal Procedure Using the ETIAS System », *European Papers*, Vol. 6, 2021, p. 473-492

Musco Eklund, Amanda, « Rule of Law Challenges of 'Algorithmic Discretion' & Automation in EU Border Control: A Case Study of ETIAS Through the Lens of Legality », *European Journal of Migration and Law,,* Vol. 25*,* 2023, p.249-274.

PETERSMANN, Marie, VAN DEN MEERSSCHE, Dimitri, « On phantom publics, clusters, and collectives: be(com)ing subject in algorithmic times », *AI & Society,* Vol. 39, 2024, p.107–124.

POULLET Yves, BRONTIDDER, Noémie, « Intelligence artificielle et services publics – le rôle des autorités publiques au service de la « troisième voie » dessinée par la Commission européenne », *Revue générale du droit*, 2022, p. 1-43.

PRIMORAC Zeljka, BOZENA, Bulum, PIJACA, Marija, « New European approach on passengers' digital surveillance through electronic platform (ETIAS) - Passengers' and carriers' perspective », *EU and comparative law issues and challenges series (ECLIC)*, Vol. 7, 2022, p. 273-294.

RAPTIS, George et al., « Using Eye Gaze Data and Visual Activities to Infer Human Cognitive Styles : Method and Feasibility Studies. » *Proceedings of the ACM conference on User Modeling, Adaptation and Personalization (UMAP'17)*, ACM Press, 2017, p.164-173.

ROBLES CARILLO, Margarita, « Artificial intelligence: From ethics to law », *Telecommunications Policy,* Vol. 44, 2020, p.78-87.

RODIER, Claire et al. « Pour une autre vision de la frontière », *Revue projet*, n°335, 2013, p.60-66.

SRINIVASAN, Ramya, CHANDER, Ajay, « Biases in AI systems », *Commun* ACM 64, Vol. 8, 2021, p.44–49.

TORRALBA, Antonio, EFROS, Alexei, « Unbiased Look at Dataset Bias », *IEEE Conference on Computer Vision and Pattern Recognition* (CVPR), 2011, p.1521-1528.

VAVOULA, Niovi, « The "Puzzle" of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection », *European Law Review*, Vol. 45, 2020, p. 348-372.

VAVOULA, Niovi, « Consultation of EU Immigration Databases for Law Enforcement Purposes: a Privacy and Data Protection Assessment », *European Journal of Migration and Law,* Vol. 22, 2020, p.139-177.

B. Articles à venir

VAVOULA, Niovi, « Tr-AI-nsforming Migration, Asylum and Border Management in the EU : the Roles of the AI Act, Interoperable Large-scale IT Systems and EU Migration Agencies », Article soumis pour publication, 2024, p.1-33.

VELASCO RICO, Clara Isabel, LAUKYTE, Migle, « ETIAS System and new proposals to advance the use of AI in public services », Article soumis pour publication, 2023, p.1-16.

YANG, Yiran, ZUIDERVEEN BORGESIUS, Frederik, BECKERS, Pascal, BROUWER, Evelien, « Automated Decision-making and Artificial Intelligence at European Borders and Their Risks for Human Rights », Article en préparation, 2024, p.1-37.

IV. Rapports universitaires

DUSHI, Desara, « The use of facial recognition technology in EU law enforcement: Fundamental rights implications », *Global Campus of Human Rights,* 2020, 10p.

ISRAEL, Tamir, « Facial recognition at a crossroads : Transformation at our Borders and Beyond », *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)*, 2020, 189p.

MOLNAR, Petra, GILL, Lex,, « Bots at the Gate : A human rights analysis of Automated decision-making in Canada's immigration and refugee system », *University of Toronto and the Citizen Lab-Munk School of Global Affairs and Public Policy*, 2018, 88p.

RUIZ BENEDICTO, Ainhoa, FRAILE MORENO Maria, LADAN, Sani, « Who watches the watchman ? Border violence and Impunity at Frontex », *Centre delas Estudias por la Paz,* 2024, 34p.

VAVOULA, Niovi, « European Travel Information and Authorisation System (ETIAS): A Flanking Measure of the EU's Visa Policy with Far Reaching Privacy Implications », *Queen Mary School of Law Legal Studies*, 2017, p. 1-8.

Chapitre 3 : Ressources numériques

I. Ressources émanant d'institutions internationales

Conseil de l'Europe, « Le Conseil de l'Europe adopte le premier traité international sur l'intelligence artificielle » le 17 mai 2024 <https://www.coe.int/fr/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence> (consulté le 18 mai 2024 à 9:30).

II. Ressources émanant d'institutions européennes

Parlement européen, « Les députés approuvent le nouveau pacte sur la migration et l'asile » (Communiqué de presse), 10 avril 2024 < https://www.europarl.europa.eu/news/fr/press-room/

20240408IPR20290/les-deputes-approuvent-le-nouveau-pacte-sur-la-migration-et-l-asile> (consulté le 25 avril 2024 à 12:33).

Parlement européen, « Intelligence artificielle: les députés adoptent une législation historique » le 13 mars 2024 <https://www.europarl.europa.eu/news/fr/press-room/20240308IPR19015/intelligence-artificielle-les-deputes-adoptent-une-legislation-historique> (consulté le 1er avril 2024 à 10:11).

Conseil de l'Union, Chronologie - Intelligence artificielle, 11 janvier 2024 <https://www.consilium.europa.eu/fr/policies/artificial-intelligence/timeline-artificial-intelligence/> (Consulté le 12 mai 2024 à 18h09).

Commission européenne, « Union de la sécurité: la Commission propose de créer un système européen d'autorisation et d'information concernant les voyages », 16 novembre 2016 <https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_18_4362> (consulté le 8 mars 2024 à 15:05).

III. Ressources émanant d'institutions nationales

A. Sénat

Sénat, Comptes rendus de la Commission des affaires européennes, « Audition de Mme Agnès Diallo, directrice exécutive de 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 (eu-LISA) » , 13 juillet 2023, <https://www.senat.fr/compte-rendu-commissions/20230710/euros.html#toc8> (consulté le 24 février 2024 à 17:10)

Sénat, réponse du Ministère de l'Europe et des affaires étrangères publiée à la question écrite n°02657 de M. EPR Jean-Yves (sénateur des Français établis hors de France - SER), 11 mai 2023 <https://www.senat.fr/questions/base/2022/qSEQ220902657.html> (consulté le 24 février 2024 à 17:30).

B. CNIL

CNIL, « Intelligence artificielle », <https://www.cnil.fr/fr/definition/intelligence-artificielle> (consulté le 4 mai 2024 à 12h11).

CNIL, « Le système API-PNR, que contient-il ? », <https://www.cnil.fr/fr/cnil-direct/question/le-systeme-api-pnr-que-contient-il> (consulté le 5 mai 2024 à 13h33).

IV. Articles en ligne

ANGWIN, Julia et al., « Ethics of Data and Analytics », *ProPublica*, 2016,<https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> (consulté le 10 mai 2024 à 17:15)

BOFFEY, Daniel, « EU Border 'Lie Detector' System criticized as Pseudoscience », The Guardian, 2 Novembre 2018, <https://www.theguardian.com/world/2018/nov/02/eu-border-lie-detection-system-criticised-as-pseudoscience> (consulté le 10 mars 2024 à 18:15).

CHARMEIL, Thimothée, « George Orwell's Dystopian World Is Coming To Life And The European AI Act Will Not Stop It : The Collection Of Emotional Data By AI - HKS Student Policy Review », *HKS Student Policy Review*, 10 mars 2024 <https://studentreview.hks.harvard.edu/george-orwells-dystopian-world-is-coming-to-life-and-the-european-ai-act-will-not-stop-it-the-collection-of-emotional-data-by-ai/> (consulté le 11 mars 2024 à 12:08).

EKLUND, Amanda Musco. « Frontex and 'Algorithmic Discretion' (Part I) : The ETIAS Screening Rules and the Principle of Legality », *Verfassungsblog*, 10 septembre 2022 <https://verfassungsblog.de/frontex-and-algorithmic-discretion-part-i/> (consulté le 2 février 2024 à 22:56).

GUILD, Elspeth, VAVOULA, Niovi, « Travel Authorization in the EU: Automated Processing and Profiling », *Open Democracy,* 12 octobre 2020, <https://www.opendemocracy.net/en/can-europe-make-it/travel-authorization-eu-automated-processing-and-profiling/> (consulté le 9 mai 2024 à 22h47).

JOHANNÈS, Frank, « En France, « le contrôle d'identité au faciès est un problème systémique, structurel, institutionnel », Le Monde, 1er août 2023 < https://www.lemonde.fr/societe/article/2023/08/01/police-le-controle-d-identite-au-facies-est-un-probleme-systemique-structurel-institutionnel_6184039_3224.html> (consulté le 19 mai 2024 à 23:45).

PROUST, Jean-Marc, «Surveiller et punir» est devenu surveiller, punir et jouir », *Slate*, publié le 4 février 2016 (consulté le 22 avril 2024 à 19h39) < https://www.slate.fr/story/113619/surveiller-punir-jouir#> (consulté le 31 mars 2024 à 15:11).

OBUSTELLI, Ludovica, «Le droit à l'autodétermination informationnelle en droit européen», RDLF 2023 thèse n°02, <https://revuedlf.com/theses/le-droit-a-lautodetermination-informationnelle-en-droit-europeen/#note-8260-6> (consulté le 21 mai 2024 à 15h47).

SAENZ, Aaron, « We Live in a Jungle of Artificial Intelligence that will Spawn Sentience », *SingularityHub,* 10 août 2010, <https://singularityhub.com/2010/08/10/we-live-in-a-jungle-of-artificial-intelligence-that-will-spawn-sentience/> (consulté le 4 mai à 13h04).

SHAPIRO, Aaron, « Reform predictive policing » *Nature,* 25 January 2017, <https://www.nature.com/articles/541458a> (consulté le 11 mai 2024 à 17h21).

THONNES, Christian, VAVOULA, Novi, « Automated predictive threat detection after Ligue des Droits Humains : Implications for ETIAS and CSAM », *Verfassungsblog*, 2023. <https://verfassungsblog.de/pnr-threat-detection-ii/> (consulté le 2 février 2024 à 23:35).

ZANDSTRA, Timo, BROUWER, Evelien, « Fundamental Rights at the Digital Border : ETIAS, the Right to Data Protection, and the CJEU's PNR judgment », *Verfasssungsblog*, 24 juin 2022 <https://verfassungsblog.de/digital-border/> (consulté le 14 avril 2024 à 16:35).

TABLE DES MATIÈRES