Page: 1857-1888 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.224

THE EU AI ACT AND THE RIGHT TO ASYLUM: ARE "HIGH-RISK" SAFEGUARDS ENOUGH FOR ASYLUM, VISA, AND RESIDENCE DECISIONS?

Prabin Acharya[1]

I. ABSTRACT

This paper examines whether the EU AI Act's "high-risk" framework adequately protects the right to asylum when artificial intelligence assists asylum, visa, and residence decisions. It situates AI within EU migration governance, where automated screening, document analysis, risk indicators, country-of-origin research, and credibility tools may influence access to protection before a human officer gives reasons. The paper argues that the AI Act marks an important regulatory advance because it expressly classifies several migration, asylum, and border-control AI systems as high-risk and subjects them to duties of risk management, data governance, transparency, human oversight, accuracy, and fundamental rights assessment. Yet these safeguards remain incomplete if they operate only as technical compliance standards. Asylum law demands individualised assessment, meaningful reasons, effective remedy, and strict respect for non-refoulement under the EU Charter, the Refugee Convention, and the Common European Asylum System. The paper further contends that opacity, automation bias, weak disclosure, and predictive profiling may convert AI assistance into disguised determinative decision-making. It therefore proposes a rights-centred model requiring notice, explainability, independent audit, case-file traceability, and stronger limits on AI tools that affect credibility, evidence reliability, or removal outcomes. Its central claim is that technology must remain subordinate to protection and due process.

II. KEYWORDS

EU AI Act, Right to Asylum, Non-Refoulement, High-Risk AI Systems, Algorithmic Migration Governance.

[1] Advocate licensed to practice in Nepal Legal Researcher and Immigration Law Professional; LL.M., University of California, Davis School of Law (2025). Email: pracharya@ucdavis.edu

 (ISSN: 2583-7753)

III. INTRODUCTION

A. Background: Artificial intelligence in EU migration governance

Artificial intelligence has entered EU migration governance through quiet administrative routes. It does not always appear as a final decision-maker. It often appears as a screening aid, a database tool, a document analyser, a biometric verifier, or a risk indicator. Yet these tools may influence how authorities see the migrant before any legal hearing begins. In asylum, visa, and residence procedures, this early influence has serious force. It may shape suspicion, eligibility, credibility, and the pace of access to protection. The EU AI Act therefore becomes relevant not because it replaces asylum law, but because it regulates the digital systems that increasingly touch asylum administration.[2]

The EU's migration architecture already depends on large-scale information systems. Visa authorities, border agencies, asylum offices, and law-enforcement bodies work through connected databases and automated checks. ETIAS, for example, uses automated processing and screening rules to assess whether an applicant may present security, illegal immigration, or high epidemic risks. These rules rely on indicators, databases, and comparison of applicant data. Such tools may help administrate speed. They may also produce hidden disadvantage where correlation turns into suspicion, especially for applicants from conflict zones, irregular routes, or document-poor backgrounds.[3]

AI also appears in border surveillance and risk analysis. Frontex and Member State authorities operate within a security-oriented border framework that values early detection, situational awareness, and operational forecasting. This creates institutional demand for predictive tools. These tools may process movement patterns, biometric data, travel routes, vessel images, document traces, or country-risk signals. The problem is not

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 1, 2024 O.J. (L 2024/1689) 1.
[3] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 Establishing a European Travel Information and Authorisation System (ETIAS), art. 33, 2018 O.J. (L 236) 1.

technology itself. The problem is the legal weight given to its output. A risk flag may begin as an operational tool. It may later influence detention, refusal, transfer, or credibility assessment. That movement from intelligence to adjudication is legally delicate.[4]

The European Parliament's research has identified AI-related border uses such as biometric identification, automated risk assessment, border monitoring, and experimental lie-detection or emotion-recognition tools. These applications show why migration governance is not a normal administrative field. It involves foreign nationals who may lack language access, legal support, stable documents, or knowledge of EU systems. Many are vulnerable because they seek protection from persecution or serious harm. Therefore, any AI tool used in this field must be measured against asylum, non-refoulement, dignity, privacy, equality, and effective remedy.[5]

The EU AI Act responds through a risk-based legal model. It classifies several migration, asylum, and border-control AI systems as "high-risk." Annex III covers systems used to assess risks posed by people entering or present in the territory, systems assisting asylum, visa, and residence applications, and systems evaluating the reliability of evidence. This classification is important. It recognises that AI may affect the substance of migration decisions even when it only "assists" an officer. It also rejects a narrow view that only fully automated refusals threaten rights.[6]

B. Research Questions

1. How does the EU AI Act regulate AI systems used in asylum, visa, residence, and border-control decision-making under its "high-risk" framework?

[4] Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard, arts. 28–29, 2024 O.J. (L 295) 1.
[5] European Parliamentary Research Service, Artificial Intelligence at EU Borders: Overview of Applications and Key Issues 1–4 (2021), https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf (last visited June 21, 2026).
[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, annex III, pt. 7, 2024 O.J. (L 2024/1689) 1.

2. Are the EU AI Act's high-risk safeguards sufficient to protect the right to asylum, non-refoulement, and effective remedy under EU and international refugee law?
3. How can AI-assisted screening, risk assessment, document analysis, evidence-reliability evaluation, and credibility indicators affect procedural fairness and individualised assessment in migration decisions?
4. What additional legal and procedural safeguards are necessary to ensure that AI remains an accountable administrative aid rather than a hidden or determinative decision-maker in EU asylum and migration governance?

C. Research Objectives

1. To examine the regulatory framework of the EU AI Act in relation to high-risk AI systems used in asylum, visa, residence, migration, and border-control decision-making.
2. To analyse whether the EU AI Act's safeguards on transparency, data governance, human oversight, risk management, and accuracy adequately protect the right to asylum and the principle of non-refoulement.
3. To evaluate the impact of AI-assisted tools on procedural fairness, individualised assessment, credibility determination, evidence reliability, and access to effective remedies in EU migration procedures.
4. To propose a rights-centred model for the use of AI in EU asylum and migration law, with stronger safeguards for disclosure, explainability, auditability, judicial review, and protection against discriminatory or opaque algorithmic decision-making.

D. Research Methodology

This research adopts doctrinal and analytical legal research methodology. It is based on a close examination of primary legal materials, including the EU AI Act, the Charter of Fundamental Rights of the European Union, the Common European Asylum System, the

Refugee Convention, the 1967 Protocol, the GDPR, and relevant decisions of the Court of Justice of the European Union and the European Court of Human Rights. The study also relies on secondary sources such as academic articles, institutional reports, EU policy materials, UNHCR guidance, and expert commentary on artificial intelligence, asylum adjudication, algorithmic governance, and human rights protection. The research follows a rights-based approach to assess whether the EU AI Act's high-risk safeguards sufficiently protect asylum seekers, visa applicants, and residence applicants from opaque, biased, or automated decision-making. It further uses comparative and critical analysis to evaluate the gap between technical AI compliance and substantive refugee-law obligations.

IV. THE EU AI ACT FRAMEWORK FOR MIGRATION, ASYLUM, VISA, AND RESIDENCE DECISIONS

A. Legislative purpose and risk-based regulatory design

The EU AI Act builds horizontal legal architecture for artificial intelligence. It does not regulate asylum law as a separate migration statute. Yet it enters asylum decision-making through its control of AI systems used by public authorities and Union agencies. Its legislative purpose is twofold. First, it seeks to improve the internal market through harmonised rules. Secondly, it promotes human-centric and trustworthy AI while protecting health, safety, fundamental rights, democracy, rule of law, and the environment. This dual-purpose matters in migration governance. Asylum, visa, and residence decisions are not ordinary service decisions. They may decide liberty, family unity, protection from persecution, and access to lawful presence. Therefore, a market-based AI statute becomes a rights-sensitive administrative law instrument when its systems assist immigration authorities.[7]

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 1, 2024 O.J. (L 2024/1689) 1.

The Act adopts a risk-based design. It places AI uses into graded categories. Some practices face prohibition. Some systems fall within high-risk control. Some systems attract transparency duties. General-purpose AI models face a separate regime. The high-risk category remains the most important for asylum and migration decisions because it does not ban such systems outright. Instead, it allows their use if providers and deployers satisfy strict obligations. These include lifecycle risk management, data governance, technical documentation, record keeping, transparency to deployers, human oversight, accuracy, robustness, and cybersecurity. The model is regulatory rather than abolitionist. It assumes that AI may assist public administration, but only under measurable legal discipline.[8]

Article 6 supplies the gateway for high-risk classification. It covers AI used as safety components in regulated products and, more importantly for migration, AI systems listed in Annex III. The Act also creates a limited derogation for certain Annex III tools if they do not pose a significant risk of harm to health, safety, or fundamental rights. This includes tools performing narrow procedural tasks or preparatory tasks. However, that exception cannot protect systems which profile natural persons. This distinction is crucial in asylum and residence administration. A document-sorting tool may look harmless. But a risk score, credibility flag, or evidence-reliability indicator may materially influence the official mind. In that setting, the system does more than assist. It shapes the legal pathway of the applicant.[9]

B. Classification of migration, asylum, and border-control AI systems as "high-risk"

Annex III, point 7 expressly places migration, asylum, and border-control management within the high-risk field. It identifies four clusters. The first covers polygraphs and similar tools. The second covers AI systems used to assess security, irregular migration,

[8] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, arts. 9–15, 2024 O.J. (L 2024/1689) 1.
[9] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 6, 2024 O.J. (L 2024/1689) 1.

or health risks posed by people entering or present in a Member State. The third covers systems assisting authorities in examining asylum, visa, and residence permit applications, including associated complaints and assessments of evidence reliability. The fourth covers systems used to detect, recognise, or identify natural persons in migration, asylum, or border-control management, except mere verification of travel documents. The classification is broad, and rightly so. It captures not only final decision engines but also tools that influence eligibility and proof.[10]

Recital 60 explains the normative reason behind this special treatment. It recognises that people affected by migration, asylum, and border-control AI are often in a vulnerable position and depend on the action of public authorities. It then stresses accuracy, non-discrimination, and transparency because the affected rights include free movement, private life, personal data, international protection, and good administration. The same recital adds a strict warning. Member States and Union bodies must not use AI to circumvent their obligations under the 1951 Refugee Convention and the 1967 Protocol. Nor may they use it to infringe non-refoulement or deny safe and effective legal avenues into the Union, including access to international protection.[11]

The classification must also be read with the Charter of Fundamental Rights of the European Union. Article 18 guarantees the right to asylum with due respect for the Geneva Convention and the Protocol. Article 19 prohibits collective expulsions and protects against removal to a serious risk of death penalty, torture, or inhuman or degrading treatment. Article 47 protects the right to an effective remedy and a fair hearing. These provisions transform high-risk compliance into constitutional compliance. A technically valid AI system can still produce an unlawful asylum process if the applicant cannot understand, contest, or correct the system's role in the decision.[12]

[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, annex III, pt. 7, 2024 O.J. (L 2024/1689) 1.
[11] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, recital 60, 2024 O.J. (L 2024/1689) 1.
[12] Charter of Fundamental Rights of the European Union arts. 18, 19, 47, 2012 O.J. (C 326) 391.

The Court of Justice has already rejected administrative convenience where it endangers fundamental protection. In Joined Cases C-411/10 and C-493/10, N.S. v. Secretary of State for the Home Department, ECLI:EU:C:2011:865, the Court held that Member States cannot apply asylum responsibility rules in a way that exposes an applicant to a real risk of inhuman or degrading treatment. That reasoning applies by analogy to AI-assisted migration governance. An algorithmic risk indicator cannot sanitise an unlawful transfer, refusal, or credibility finding. The human officer must retain legal judgment. The reviewer must retain power to examine the real basis of the decision.[13]

C. Key obligations for high-risk AI systems: data governance, transparency, human oversight, accuracy, and risk management

High-risk AI regulation under the EU AI Act begins with risk management. Article 9 requires a documented and continuous system that follows the AI system throughout its lifecycle. This matters deeply in asylum, visa, and residence decisions. A flawed risk score may not merely create an administrative inconvenience. It may affect access to protection, lawful stay, family life, or removal. The Act therefore expects providers to identify known and reasonably foreseeable risks to health, safety, and fundamental rights. It also requires testing, mitigation, and review. In migration administration, this means that an AI tool must be examined not only for technical performance, but also for its effect on vulnerable applicants, language minorities, traumatised persons, and persons with incomplete records.[14]

Data governance sits at the centre of this framework. Article 10 requires training, validation, and testing datasets to remain relevant, representative, complete, and, as far as possible, free from error. It also requires attention to bias, data gaps, and the specific geographical, contextual, behavioural, and functional setting of use. This obligation is critical in asylum adjudication. Country-of-origin data may be uneven. Identity

[13] Joined Cases C-411/10 & C-493/10, N.S. v. Sec'y of State for the Home Dep't, ECLI:EU:C:2011:865.
[14] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 9, 2024 O.J. (L 2024/1689) 1.

documents may be missing. Narratives may contain delay, trauma, translation gaps, or cultural distance. An AI system trained on rigid or historically biased administrative data may reproduce suspicion as if it were evidence. Therefore, data governance must become a safeguard against digital stereotyping.[15]

Transparency under Articles 12 and 13 works through record-keeping, instructions for use, and interpretability for deployers. High-risk systems must allow automatic logs. They must also provide clear information about intended purpose, limits, accuracy, foreseeable misuse, performance across groups, input data, and output interpretation. This duty has special value in migration decisions because an official may treat a machine output as neutral. Yet output may hide assumptions about nationality, route, age, language, document quality, or perceived risk. In Case C-634/21, SCHUFA Holding (Scoring), ECLI:EU:C:2023:957, the Court of Justice treated a probability value as legally significant where another actor strongly relied on it. That logic fits AI-assisted migration files. A "mere" recommendation may become decisive if the officer follows it without real scrutiny.[16]

Human oversight under Article 14 must not become ceremonial. The Act requires oversight by natural people who can understand capacities and limits, detect automation bias, interpret outputs, disregard or reverse the system, and stop its operation where necessary. Article 26 further requires deployers to assign oversight to people with competence, training, authority, and support. For asylum and residence decisions, this imposes constitutional discipline on the case officer. The officer cannot simply sign what the system suggests. The officer must retain legal judgment. The officer must also record why algorithmic output was accepted or rejected. Without that discipline, human oversight becomes a rubber stamp, and the applicant loses the substance of due process.[17]

[15] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 10, 2024 O.J. (L 2024/1689) 1.
[16] Case C-634/21, SCHUFA Holding (Scoring), ECLI:EU:C:2023:957.
[17] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, arts. 14, 26, 2024 O.J. (L 2024/1689) 1.

 (ISSN: 2583-7753)

Accuracy, robustness, and cybersecurity under Article 15 form another essential layer. High-risk AI systems must perform consistently throughout their lifecycle. Their accuracy metrics must be declared. They must resist errors, faults, feedback loops, data poisoning, adversarial inputs, and model manipulation. In migration settings, cybersecurity also has a protection value. A manipulated identity-matching tool, document-analysis system, or risk assessment model may wrongly mark an applicant as deceptive or dangerous. The harm may then be tricked into interviews, credibility findings, detention decisions, and appeal records. Accuracy therefore cannot be measured in abstract laboratory conditions alone. It must be tested against the real conditions of asylum administration.[18]

D. The 2 August 2026 full applicability timeline and its significance

Article 113 fixes 2 August 2026 as the general date from which the AI Act applies, subject to specific exceptions. This date is legally significant because it converts the Act from a legislative promise into an operational duty. For migration, asylum, visa, and residence systems, the timeline should push authorities to complete procurement review, AI mapping, staff training, log retention protocols, applicant-notification templates, and appeal-facing explanation standards before deployment harden into practice. A migration authority cannot wait for litigation to discover where AI entered the file. It must know that before the first affected applicant receives a refusal.[19]

The timeline is, however, no longer a simple single-date story. Commission implementation materials now present the AI Act as progressively applicable. They still identify 2 August 2026 as the full application date with exceptions. Yet current standardisation materials state that the latest applicability date is 2 December 2027 for Annex III high-risk AI systems, and 2 August 2028 for high-risk systems embedded in regulated products, where support tools such as standards are not available earlier. This

[18] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 15, 2024 O.J. (L 2024/1689) 1.
[19] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 113, 2024 O.J. (L 2024/1689) 1.

nuance matters for the paper's argument. The protection question does not disappear because compliance is phased. In fact, the transition period may become the decisive window in which rights-based safeguards are either built into migration administration or lost to technical inertia.[20]

V. AI-ASSISTED DECISION-MAKING IN ASYLUM, VISA, AND RESIDENCE PROCEDURES

A. Eligibility screening and risk assessment tools

Eligibility screening in asylum, visa, and residence procedures now move through a dense digital environment. Authorities may use AI tools to organise applications, detect missing information, compare identity records, flag security concerns, or prioritise files. These tools appear administrative at first sight. Yet they may alter the applicant's legal position before a human officer gives reasons. The EU AI Act recognises this danger. Annex III treats AI systems used to assist the examination of asylum, visa, and residence permit applications as high-risk, including systems that assess eligibility and related complaints. This classification reflects a basic point. In migration law, screening is never neutral when it filters access to protection or lawful stay.[21]

Risk assessment tools raise sharper concerns. They may mark a person as a security risk, irregular migration risk, or health risk. ETIAS already shows the logic of automated screening. Its screening rules operate through an algorithm that enables profiling by comparing applicant data with specific risk indicators. The risk indicators relate to security, illegal immigration, or high epidemic risks. This structure may speed up travel authorisation and visa-related administration. Still, it also shifts part of legal assessment into a coded environment. The affected person may not know which indicator triggered

[20] European Comm'n, Standardisation of the AI Act, SHAPING EUROPE'S DIGITAL FUTURE, https://digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation (last visited June 21, 2026).
[21] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, annex III, pt. 7(c), 2024 O.J. (L 2024/1689) 1.

concern. Nor may the person know whether the indicator rests on reliable, updated, and non-discriminatory data.[22]

The danger grows when screening tools use group-based correlations. A person may be flagged because of route, nationality, prior movement pattern, family link, document history, or database match. Such indicators may help officials detect fraud or risk. But they may also convert migration patterns into suspicion. The Schengen and visa ecosystem already depends on large-scale databases. Interoperability increases the administrative appetite for cross-system comparison. Therefore, an AI risk flag may follow an applicant across borders, visa offices, asylum files, and residence decisions. Due process then requires traceability. The applicant must know the substance of the adverse material, subject only to narrow lawful limits.[23]

B. Evidence-reliability assessment, document analysis, and credibility indicators

Evidence-reliability assessment is one of the most sensitive uses of AI in asylum law. Refugee claims often rest on incomplete documents, oral testimony, fragmented digital evidence, and country-of-origin material. Flight itself may destroy records. Smugglers may keep papers. States of origin may not issue reliable documents to persecuted groups. Article 4 of the Qualification Regulation recognises this practical difficulty. It allows protection claims to proceed even when particular statements lack documentary proof, if the applicant has made a genuine effort, gives a satisfactory explanation, and presents coherent and plausible statements consistent with available information. AI must not erase that evidentiary generosity.[24]

---

[22] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 Establishing a European Travel Information and Authorisation System (ETIAS), art. 33, 2018 O.J. (L 236) 1.

[23] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 Establishing a Framework for Interoperability Between EU Information Systems in the Field of Borders and Visa, 2019 O.J. (L 135) 27.

[24] Regulation (EU) 2024/1347 of the European Parliament and of the Council of 14 May 2024 on Standards for the Qualification of Third-Country Nationals or Stateless Persons as Beneficiaries of International Protection, art. 4, 2024 O.J. (L 2024/1347) 1.

Document analysis tools may support authenticity checks, translation, classification, and anomaly detection. They may also compare formats, stamps, metadata, and image patterns. Yet their legal value depends on context. A document from a conflict zone may look irregular because the issuing system itself has collapsed. A low-quality scan may reflect displacement, not fraud. A translated certificate may contain spelling variation. Therefore, AI document analysis should never become a credibility verdict. It should remain one evidentiary aid among many. The determining authority must still assess personal circumstances, country conditions, and the applicant's explanation for gaps or inconsistencies.[25]

Credibility indicators are even more dangerous when reduced to behavioural or biometric signals. Demeanour, eye contact, emotion, hesitation, linguistic style, or narrative order may reflect trauma, culture, fear, interpretation error, or shame. The Court of Justice has already warned against degrading and intrusive methods in asylum credibility assessment. In Joined Cases C-148/13 to C-150/13, A, B & C v. Staatssecretaris van Veiligheid en Justitie, ECLI:EU:C:2014:2406, the Court rejected assessment methods that violated human dignity and private life in sexual orientation claims. That reasoning applies with force to AI tools that infer credibility from intimate, behavioural, or stereotype-laden signals.[26]

The same principle appears in Case C-473/16, F v. Bevándorlási és Állampolgársági Hivatal, ECLI:EU:C:2018:36. The Court held that a psychological test to determine sexual orientation amounted to a disproportionate interference with private life. This judgment matters beyond sexuality-based claims. It tells decision-makers that scientific language cannot legitimise intrusive proof. An AI system may appear more objective than a psychologist's test. Yet it may still create pseudo-scientific certainty. If it measures facial

[25] European Union Agency for Asylum, Practical Guide on Evidence and Risk Assessment 11–13 (2024), https://www.euaa.europa.eu/sites/default/files/publications/2024-02/Practical-Guide-Evidence-Risk-Assessment.pdf (last visited June 21, 2026).
[26] Joined Cases C-148/13 to C-150/13, A, B & C v. Staatssecretaris van Veiligheid en Justitie, ECLI:EU:C:2014:2406.

movement, voice stress, memory sequence, or emotional congruence, it risks turning human vulnerability into adverse evidence.[27]

C. Country-of-origin information, profiling, and predictive analytics

Country-of-origin information is indispensable to asylum adjudication. The new Asylum Procedure Regulation requires determining authorities to examine applications objectively, impartially, and individually. It also requires relevant, precise, and up-to-date information on the situation in the country of origin, including laws and their practical application. AI can assist this work. It can summarise reports, detect conflict trends, classify sources, translate material, and map risk factors. Used carefully, it may improve consistency. Used poorly, it may flatten human experience into country-wide generalisation.[28]

The legal danger lies in predictive analytics. A system may infer that a claim is unlikely because applicants from a particular region usually receive rejection. It may predict risk of absconding because people with similar routes previously disappeared. It may rank claims by historic recognition rates. These predictions may be statistically useful. But asylum law does not decide a person by cohort probability. It decides whether this individual faces persecution or serious harm. Therefore, country-of-origin AI must not replace the personal narrative. It must only strengthen the officer's ability to ask better questions and test facts fairly.[29]

[27] Case C-473/16, F v. Bevándorlási és Állampolgársági Hivatal, ECLI:EU:C:2018:36.
[28] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 Establishing a Common Procedure for International Protection in the Union, art. 34, 2024 O.J. (L 2024/1348) 1.
[29] U.N. High Comm'r for Refugees, Handbook on Procedures and Criteria for Determining Refugee Status and Guidelines on International Protection ¶¶ 196–205 (2019), https://www.unhcr.org/sites/default/files/legacy-pdf/4d93528a9.pdf (last visited June 21, 2026).

 (ISSN: 2583-7753)

VI. THE RIGHT TO ASYLUM AND NON-REFOULEMENT UNDER EU LAW

A. The right to asylum under the EU Charter and the Common European Asylum System

Article 18 of the Charter gives asylum a constitutional place within EU law. It does not treat asylum as administrative charity. It frames it as a right exercised with due respect for the Geneva Convention, the 1967 Protocol, and the Treaties. This matters for AI-assisted migration governance. An algorithm may help organise files. It may assist with document review. Yet it cannot reduce asylum to an efficiency exercise. The right to asylum requires a legal pathway through which fear, risk, identity, vulnerability, and proof are examined with care. It also requires the State to hear the person before it classifies the person.[30]

The Common European Asylum System gives operational form to that right. Article 78 TFEU directs the Union to develop a common policy on asylum, subsidiary protection, and temporary protection, in accordance with non-refoulement. The new Pact instruments deepen that architecture through common rules on qualification, procedure, responsibility, reception, and crisis management. For this paper, the Qualification Regulation and the Asylum Procedure Regulation are especially important. They convert the Charter's protection promise into standards on who qualifies, how claims are examined, and how negative decisions must be reasoned.[31]

The right to asylum also has a personal and evidentiary character. The Qualification Regulation requires assessment of facts and circumstances through cooperation between the applicant and Member State. It recognises the applicant's statements, documents, individual position, personal circumstances, background, age, gender, gender identity, sexual orientation, and country conditions. These standard resists mechanical

[30] Charter of Fundamental Rights of the European Union art. 18, 2012 O.J. (C 326) 391.
[31] Consolidated Version of the Treaty on the Functioning of the European Union art. 78, 2012 O.J. (C 326) 47.

classification. Therefore, AI cannot decide asylum by probability alone. A system trained in past recognition rates or rejection patterns may show administrative history. It cannot answer the legal question whether this applicant faces persecution or serious harm.[32]

B. Non-refoulement as a substantive limit on algorithmic governance

Non-refoulement is the hard boundary of migration control. Article 33 of the Refugee Convention prohibits a State from returning a refugee "in any manner whatsoever" to territories where life or freedom would be threatened. EU law carries that rule through Article 19 of the Charter. The European Convention system reinforces it through Article 3 ECHR, which forbids removal to a real risk of torture or inhuman or degrading treatment. In algorithmic governance, non-refoulement means that a technical system cannot justify return where legal risk remains unresolved. No risk score can dilute that command.[33]

The EU AI Act recognises this in its own language. Recital 60 treat migration, asylum, and border-control AI as high-risk because affected persons often depend on public authorities and may stand in a vulnerable position. It further warns that Member States and Union bodies must not use AI to circumvent obligations under the 1951 Convention and the 1967 Protocol. Nor may they use AI to infringe non-refoulement or deny safe and effective legal avenues into the Union. This recital gives the AI Act a refugee-law spine. It tells deployers that technical legality does not cure protection illegality.[34]

The Court of Justice adopted the same rights-first logic in Joined Cases C-411/10 and C-493/10, N.S. v. Secretary of State for the Home Department, ECLI:EU:C:2011:865. The Court held that Member States may not transfer an asylum seeker under Dublin rules where systemic deficiencies create substantial grounds for believing that the applicant

[32] Regulation (EU) 2024/1347 of the European Parliament and of the Council of 14 May 2024 on Standards for the Qualification of Third-Country Nationals or Stateless Persons as Beneficiaries of International Protection, art. 4, 2024 O.J. (L 2024/1347) 1.
[33] Convention Relating to the Status of Refugees art. 33, July 28, 1951, 189 U.N.T.S. 137.
[34] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, recital 60, 2024 O.J. (L 2024/1689) 1.

faces a real risk of inhuman or degrading treatment. This reasoning applies with force to automated screening. A database match, route indicator, or transfer recommendation cannot override the duty to examine real risk. The Charter controls the system, not the other way around.[35]

The European Court of Human Rights also refuses mechanical migration action where protection risk is ignored. In Hirsi Jamaa and Others v. Italy, App. No. 27765/09, the Grand Chamber condemned push-back operations which lacked individual screening and exposed applicants to onward refoulement. The case is relevant to AI because collective return can now occur through digital sorting as much as through physical interception. If algorithm groups people with low merit or safe to remove without real individual inquiry, it creates a modern form of collective risk disposal.[36]

C. Procedural fairness, individualised assessment, and reason-based decision-making

Procedural fairness gives practical life to asylum and non-refoulement. The Asylum Procedure Regulation requires determining authorities to examine applications objectively, impartially, and on an individual basis. It also requires relevant, precise, and up-to-date country-of-origin information. Further, it requires attention to the applicant's individual position and personal circumstances. These requirements impose a direct limit on AI-assisted adjudication. The officer must not outsource the legal imagination of the case. He must assess the person, the story, the evidence, and the risk in their proper setting.[37]

The same Regulation requires negative decisions to be given in writing. Where an application is rejected as inadmissible, unfounded, or manifestly unfounded, the decision must state reasons in fact and in law. It must also inform the applicant how to challenge

[35] Joined Cases C-411/10 & C-493/10, N.S. v. Sec'y of State for the Home Dep't, ECLI:EU:C:2011:865.
[36] Hirsi Jamaa & Others v. Italy, App. No. 27765/09 (Eur. Ct. H.R. Feb. 23, 2012).
[37] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 Establishing a Common Procedure for International Protection in the Union, art. 34, 2024 O.J. (L 2024/1348) 1.

the decision. This requirement becomes sharper where AI enters the file. If an AI output materially affects credibility, evidence reliability, security risk, or eligibility, the reasons must not hide that influence. A reasoned decision that conceals the real basis of refusal becomes a decorative document. It fails the applicant and it weakens judicial review.[38]

The right to be heard strengthens this procedural discipline. In Case C-277/11, M.M. v. Minister for Justice, Equality and Law Reform, ECLI:EU:C:2012:744, the Court treated the right to be heard as part of the rights of defence in international protection procedures. The applicant must have an effective opportunity to present views before an adverse decision. AI-assisted systems may threaten that opportunity where they generate unseen credibility doubts before the interview. They may also shape questions, tone, and suspicion. Fairness therefore requires prior disclosure, or at least meaningful post-decision access, to the substance of machine-influenced concerns.[39]

VII. EFFECTIVE REMEDY, DUE PROCESS, AND EXPLAINABILITY IN AI-ASSISTED MIGRATION DECISIONS

A. The right to an effective remedy under EU law

Article 47 of the Charter gives every person an enforceable right to an effective remedy before a tribunal when rights guaranteed by Union law are violated. It also protects fair hearing, legal advice, representation, and legal aid where access to justice would otherwise fail. In asylum, visa, and residence decisions, this right cannot operate as a symbolic appeal. It must give the affected person a real chance to test the factual and legal basis of the decision. When AI assists the file, the remedy must also reach the machine-influenced part of the reasoning. Otherwise, the court reviews only the visible surface of the administrative act.[40]

[38] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 Establishing a Common Procedure for International Protection in the Union, art. 36, 2024 O.J. (L 2024/1348) 1.
[39] Case C-277/11, M.M. v. Minister for Justice, Equality and Law Reform, ECLI:EU:C:2012:744.
[40] Charter of Fundamental Rights of the European Union art. 47, 2012 O.J. (C 326) 391.

The Asylum Procedure Regulation gives specific force to this guarantee. Article 67 requires an effective remedy before a court or tribunal against decisions rejecting international protection, withdrawing protection, or issuing related return decisions. It also requires a full and ex-nunc examination of both facts and points of law at least before a court or tribunal of first instance. This standard has direct relevance for AI. A court cannot conduct full and current review if an algorithmic risk score, credibility flag, or document-reliability output remains outside the file. The appeal must reach the real decision chain.[41]

The Court of Justice reinforced this position in Case C-585/16, Serin Alheto v. Zamestnik-predsedatel na Darzhavna agentsia za bezhantsite, ECLI:EU:C:2018:584. The Court treated effective remedy in asylum as a review that may require examination of international protection needs in light of current facts and law. This approach resists narrow appellate formalism. It means that AI-assisted migration decisions must remain judicially intelligible. If the authority used a model to rank risk or assess evidence, the reviewing body must know enough to test whether the system distorted the applicant's legal protection claim.[42]

B. Access to reasons, evidence, and contestability of AI-influenced outcomes

Reasons are the bridge between administrative power and legal accountability. Article 36 of the Asylum Procedure Regulation requires written decisions and reasons in fact and in law where an application is rejected as inadmissible, unfounded, manifestly unfounded, explicitly withdrawn, or implicitly withdrawn. This duty cannot be satisfied by generic language. If an AI tool materially influenced by refusal, the reasons must reveal that influence in usable terms. The applicant must understand what was doubted,

[41] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 Establishing a Common Procedure for International Protection in the Union, art. 67, 2024 O.J. (L 2024/1348) 1.
[42] Case C-585/16, Serin Alheto v. Zamestnik-predsedatel na Darzhavna agentsia za bezhantsite, ECLI:EU:C:2018:584.

what evidence was discounted, and why the officer accepted or rejected the system's output.[43]

The AI Act adds a specific right to explanation. Article 86 gives an affected person the right to obtain clear and meaningful explanations of the role of an Annex III high-risk AI system in the decision-making procedure, and of the main elements of the decision, where that decision produces legal effects or similarly significant effects. Migration, asylum, border-control, visa, and residence systems fall within Annex III point 7. Therefore, a person refused protection, a visa, or residence on the basis of AI-assisted assessment should not receive a bare administrative conclusion. The person should receive an explanation that makes contestation possible.[44]

Article 26 of the AI Act strengthens this route. It requires deployers of Annex III high-risk AI systems that make or assist decisions related to natural people to inform those people that they are subject to the use of such a system. This notice is not a small procedural formality. In migration law, it is the entry point for challenge. Without notice, an applicant may attack the wrong issue. He may defend a document, statement, or route history, while the hidden harm lies in a model's inference. Contestability begins when the person knows that AI plays a role.[45]

EU case law on restricted reasons also helps in this field. In Case C-300/11, ZZ v. Secretary of State for the Home Department, ECLI:EU:C:2013:363, the Court held that national security limits may restrict disclosure, yet the person must still know the essence of the grounds in a manner that allows effective defence. This logic applies to algorithmic secrecy. Trade secrets, cybersecurity, and database integrity may justify some limits. They

[43] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 Establishing a Common Procedure for International Protection in the Union, art. 36, 2024 O.J. (L 2024/1348) 1.
[44] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 86, 2024 O.J. (L 2024/1689) 1.
[45] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 26(11), 2024 O.J. (L 2024/1689) 1.

cannot justify total opacity. The essence of the AI-based concern must reach the applicant, counsel, or court through a lawful procedure.[46]

Case C-159/21, GM v. Országos Idegenrendészeti Főigazgatóság, Alkotmányvédelmi Hivatal, Terrorelhárítási Központ, ECLI:EU:C:2022:708, sharpens the same principle in international protection. The Court rejected a structure in which the asylum authority could not depart from national security opinions, and the applicant had no usable access to the substance of the material. The relevance to AI is immediate. If a migration officer must follow a system's risk output in practice, and the applicant cannot test it, the AI becomes an unchallengeable authority. That result is inconsistent with effective remedy and due process.[47]

C. The problem of opacity in automated evidence and credibility assessments

Opacity enters AI-assisted migration decisions at several levels. The model may be technically complex. The dataset may be inaccessible. The output may be expressed as a score or flag. The officer may not know how the system reached its result. The applicant will know even less. This is dangerous in evidence and credibility assessment because small doubts can carry heavy legal effects. A date inconsistency, document anomaly, route pattern, or language feature may quietly harden into adverse credibility. The system may then appear objective, while actually reproducing historical suspicion.[48]

The GDPR shows why automated legal effects require caution. Article 22 gives the data subject a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significant effects. This does not solve every migration case, because many decisions are formally human made. Yet it supplies an important benchmark. Where automation materially affects legal status,

[46] Case C-300/11, ZZ v. Sec'y of State for the Home Dep't, ECLI:EU:C:2013:363.
[47] Case C-159/21, GM v. Országos Idegenrendészeti Főigazgatóság, Alkotmányvédelmi Hivatal, Terrorelhárítási Központ, ECLI:EU:C:2022:708.
[48] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 10, 2024 O.J. (L 2024/1689) 1.

liberty, removal risk, family unity, or residence, the legal system must demand safeguards. A human name on the decision cannot hide machine control.[49]

The Court's judgment in Case C-634/21, OQ v. Land Hessen, ECLI:EU:C:2023:957, is especially useful. The Court held that the automated establishment of a probability value may amount to automated decision-making where a third party draws strongly on that value. Although the case concerned credit scoring, its logic fits asylum and residence procedures. If an officer relies strongly on an AI credibility flag or risk score, the system may become decisive in substance. The law must then examine function, not label. A recommendation may operate as a decision.[50]

Opacity also undermines law because it weakens contradiction. Article 29 Working Party's guidelines on automated decision-making explain that meaningful information should not be reduced to complex mathematical formulae. The person should receive information that enables understanding of the reasons for the decision and the logic involved in a practical way. In migration files, this means that applicants must know the categories of data used, the kind of inference made, and the adverse conclusion drawn. They do not need source code in every case. They do need a fair opportunity to answer the machine-shaped allegation.[51]

VIII. ARE THE EU AI ACT'S "HIGH-RISK" SAFEGUARDS SUFFICIENT?

The EU AI Act gives migration governance a long-needed regulatory discipline. It classifies AI systems used in migration, asylum, and border-control management as high-risk where they assess risk, assist asylum, visa, or residence applications, evaluate evidence reliability, or identify persons in this field. This is a major legal gain. It rejects the fiction that migration AI is only technical administration. It recognises that digital

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data, art. 22, 2016 O.J. (L 119) 1.
[50] Case C-634/21, OQ v. Land Hessen, ECLI:EU:C:2023:957.
[51] Article 29 Data Prot. Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, WP251 rev.01, at 25 (Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/items/612053 (last visited June 21, 2026).

tools may affect liberty, protection, residence, family unity, and removal. Yet classification is not protection in itself. A high-risk label permits use, subject to compliance. It does not ask whether some tools should be excluded from asylum adjudication altogether.[52]

The Act's core safeguards are meaningful. Risk management, data governance, transparency, record-keeping, human oversight, accuracy, robustness, and cybersecurity create a serious compliance burden. These duties can reduce arbitrary automation. They can also help courts and regulators detect bias, errors, and unsafe deployment. Still, these safeguards mainly control system design and deployment. They do not fully answer the refugee-law question. The question is not only whether the AI system functions properly. The question is whether its use preserves individualised protection assessment, non-refoulement, and an effective remedy in the concrete file.[53]

The strongest gap lies in opacity. Migration applicants may not know when AI has shaped a risk flag, credibility concern, or document-reliability finding. Article 26 requires deployers to inform people where Annex III high-risk systems make or assist decisions. Article 86 adds a right to explanation where high-risk AI produces legal or similarly significant effects. These provisions help. Yet they remain vulnerable to narrow administrative interpretation. An authority may say the system merely supported internal workflow. The applicant may never learn that the officer's suspicion began with machine output.[54]

Data quality creates a second gap. Asylum files rarely contain perfect evidence. Many applicants flee without documents. Some documents come from fragile or hostile States. Some narratives contain trauma-based inconsistencies. Article 10 requires data sets to be

[52] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, annex III, pt. 7, 2024 O.J. (L 2024/1689) 1.
[53] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, arts. 9–15, 2024 O.J. (L 2024/1689) 1.
[54] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, arts. 26, 86, 2024 O.J. (L 2024/1689) 1.

relevant, representative, and as far as possible free from errors. But asylum data can carry old institutional bias. Past refusal patterns may reflect poor access to lawyers, stereotypes, or weak country information. A model trained on such material may convert historical injustice into statistical confidence. This makes compliance necessary, but not enough.[55]

Recital 60 gives the Act its clearest protection warning. It states that AI in migration, asylum, and border control must not be used to circumvent obligations under the Refugee Convention and the 1967 Protocol. Nor may it infringe non-refoulement or deny safe and effective legal avenues into the Union. This language is powerful. But it sits in a recital, not as a detailed procedural code. Therefore, courts and authorities must translate it into hard duties. These include disclosure, reasons, audit trails, legal assistance, and power to challenge the substance of AI-influenced findings.[56]

IX. TOWARDS A RIGHTS-CENTRED MODEL FOR AI IN EU ASYLUM AND MIGRATION LAW

A rights-centred model should treat AI use as a procedural fact that must enter the case record. Every applicant should know whether AI assisted eligibility screening, risk assessment, document analysis, country-of-origin research, or credibility evaluation. The notice should not be vague. It should identify the type of tool, its function, the stage of use, and whether the output influenced the decision. The Asylum Procedure Regulation already requires written decisions with reasons in fact and law. AI-related reasons should fit inside that duty. A refusal should not hide the digital route by which doubt was formed.[57]

Contestability must become the practical test of legality. The applicant need not receive source code in every case. But the applicant must receive the essence of the AI-influenced

[55] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 10, 2024 O.J. (L 2024/1689) 1.
[56] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, recital 60, 2024 O.J. (L 2024/1689) 1.
[57] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 Establishing a Common Procedure for International Protection in the Union, art. 36, 2024 O.J. (L 2024/1348) 1.

concern, the data categories used, and the role of the output in the file. Where secrecy is claimed for security or technical reasons, a court or independent body should still examine the material. The CJEU in ZZ accepted that disclosure may face limits, but the person must know the essence of the grounds to defend himself. That principle should govern algorithmic migration decisions with equal force.[58]

Public authorities should treat the fundamental rights impact assessment as more than a compliance form. Article 27 requires assessment of affected groups, risks, oversight measures, and complaint mechanisms before certain high-risk systems are used. In asylum and residence procedures, this assessment should examine non-refoulement, discrimination, privacy, effective remedy, legal aid, vulnerability, and access to interpretation. Independent audit should also test outcomes across nationality, ethnicity, language, gender, age, disability, route, and document status. Without such testing, bias may remain invisible while still deciding lives.[59]

Some AI uses deserve prohibition or a near-prohibition standard in asylum law. Tools that infer credibility from emotion, demeanour, voice stress, facial movement, or behavioural signals should not decide protection claims. Such tools risk pseudo-science and stereotypes. The Court of Justice's rulings in A, B & C and F show that intrusive methods of credibility assessment cannot be justified merely because an authority seeks truth. Human dignity and private life set boundaries on proof. A rights-centred model should therefore ban or severely restrict AI systems that make intimate, behavioural, or identity-based credibility inferences.[60]

High-risk safeguards should operate as the minimum floor. They should not become the ceiling of protection. Migration decisions require a higher standard because error may lead to persecution, torture, family separation, detention, or unlawful removal. The correct model is not anti-technology. It is anti-secret law. AI may assist translation,

[58] Case C-300/11, ZZ v. Sec'y of State for the Home Dep't, ECLI:EU:C:2013:363.
[59] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 27, 2024 O.J. (L 2024/1689) 1.
[60] Case C-473/16, F v. Bevándorlási és Állampolgársági Hivatal, ECLI:EU:C:2018:36.

organisation, country research, and consistency review. It must not become an invisible adjudicator. A rights-centred EU model should require notice, meaningful explanation, independent review, auditable records, and a decisive human officer who can reject the machine in law and in practice.[61]

X. CONCLUSION

The EU AI Act marks a decisive regulatory moment for migration governance. It accepts that artificial intelligence can no longer remain a hidden administrative tool in asylum, visa, residence, and border-control decisions. By classifying several migration-related AI systems as "high-risk," the Act recognises that digital screening, evidence analysis, risk assessment, and identity tools may affect fundamental rights in serious ways. Yet this classification does not resolve the central legal concern. It regulates use. It does not fully answer whether some AI tools should be used at all in protection-sensitive adjudication.[62]

The right to asylum under Article 18 of the Charter and the prohibition of refoulement under Article 19 impose a higher standard than ordinary administrative legality. These rights demand individualised assessment, serious attention to evidence, and protection against persecution, torture, or inhuman treatment. Therefore, an AI system that is technically compliant may still produce an unlawful process if it weakens access to reasons, evidence, hearing, or appeal. The legality of AI in asylum law must be tested by its effect on the applicant's protection claim, not only by its conformity certificate.[63]

The Act's safeguards are valuable. Risk management, data governance, transparency, record-keeping, human oversight, accuracy, and cybersecurity may reduce arbitrary automation. Article 86's right to explanation and Article 26's notice requirement also creates openings for contestability. Still, these safeguards remain incomplete unless authorities translate them into case-file rights. The applicant must know when AI shaped

[61] Charter of Fundamental Rights of the European Union arts. 18, 19, 47, 2012 O.J. (C 326) 391.
[62] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, annex III, pt. 7, 2024 O.J. (L 2024/1689) 1.
[63] Charter of Fundamental Rights of the European Union arts. 18–19, 2012 O.J. (C 326) 391.

the decision. The applicant must understand the substance of the adverse inference. The reviewing court must see the logs, the output, and the human reasons for accepting or rejecting it.[64]

Non-refoulement sets the strongest substantive limit. Recital 60 of the AI Act rightly warns that AI must not circumvent the Refugee Convention, the 1967 Protocol, or safe and effective access to international protection. This warning should guide courts, regulators, and migration authorities. The CJEU's reasoning in N.S. confirms that administrative systems cannot operate automatically where they expose applicants to a real risk of inhuman or degrading treatment. Algorithmic migration control must therefore remain subordinate to Charter rights and refugee protection.[65]

A rights-centred model should treat AI as an accountable evidentiary influence, not as an invisible adjudicator. It should require prior fundamental rights impact assessment, meaningful disclosure, independent audit, trained human review, and effective judicial scrutiny. Tools that infer credibility from emotion, demeanour, voice, facial movement, or behavioural signals should face prohibition or near-prohibition in asylum adjudication. Such tools risk turning trauma and culture into suspicion.[66]

The answer to the paper's central question is therefore qualified. The EU AI Act's high-risk safeguards are necessary, but not sufficient. They form a regulatory floor. They should not become the ceiling of protection. In asylum, visa, and residence decisions, the decisive test must remain human dignity, non-refoulement, individualised assessment, and effective remedy. AI may assist administration. It must never displace protection.[67]

[64] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, arts. 9–15, 26, 86, 2024 O.J. (L 2024/1689) 1.
[65] Joined Cases C-411/10 & C-493/10, N.S. v. Sec'y of State for the Home Dep't, ECLI:EU:C:2011:865.
[66] Case C-473/16, F v. Bevándorlási és Állampolgársági Hivatal, ECLI:EU:C:2018:36.
[67] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 Establishing a Common Procedure for International Protection in the Union, arts. 34, 36, 67, 2024 O.J. (L 2024/1348) 1.

XI. BIBLIOGRAPHY

A. Primary Legal Instruments

1. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.
2. Consolidated Version of the Treaty on the Functioning of the European Union, 2012 O.J. (C 326) 47.
3. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.
4. Convention Relating to the Status of Refugees, July 28, 1951, 189 U.N.T.S. 137.
5. Protocol Relating to the Status of Refugees, Jan. 31, 1967, 606 U.N.T.S. 267.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data, 2016 O.J. (L 119) 1.
7. Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 Establishing a European Travel Information and Authorisation System (ETIAS), 2018 O.J. (L 236) 1.
8. Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 Establishing a Framework for Interoperability Between EU Information Systems in the Field of Borders and Visa, 2019 O.J. (L 135) 27.
9. Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard, 2019 O.J. (L 295) 1.
10. Regulation (EU) 2024/1347 of the European Parliament and of the Council of 14 May 2024 on Standards for the Qualification of Third-Country Nationals or Stateless Persons as Beneficiaries of International Protection, 2024 O.J. (L 2024/1347) 1.

11. Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 Establishing a Common Procedure for International Protection in the Union, 2024 O.J. (L 2024/1348) 1.

12. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 2024/1689) 1.

B. Cases

1. Case C-69/10, Brahim Samba Diouf v. Ministre du Travail, de l'Emploi et de l'Immigration, ECLI:EU:C:2011:524.

2. Case C-277/11, M.M. v. Minister for Justice, Equality and Law Reform, Ireland and Attorney General, ECLI:EU:C:2012:744.

3. Case C-300/11, ZZ v. Secretary of State for the Home Department, ECLI:EU:C:2013:363.

4. Case C-473/16, F v. Bevándorlási és Állampolgársági Hivatal, ECLI:EU:C:2018:36.

5. Case C-585/16, Serin Alheto v. Zamestnik-predsedatel na Darzhavna agentsia za bezhantsite, ECLI:EU:C:2018:584.

6. Case C-159/21, GM v. Országos Idegenrendészeti Főigazgatóság, Alkotmányvédelmi Hivatal and Terrorelhárítási Központ, ECLI:EU:C:2022:708.

7. Case C-634/21, OQ v. Land Hessen, ECLI:EU:C:2023:957.

8. Joined Cases C-411/10 & C-493/10, N.S. v. Secretary of State for the Home Department, ECLI:EU:C:2011:865.

9. Joined Cases C-148/13 to C-150/13, A, B & C v. Staatssecretaris van Veiligheid en Justitie, ECLI:EU:C:2014:2406.

10. Chahal v. United Kingdom, App. No. 22414/93 (Eur. Ct. H.R. Nov. 15, 1996).

11. Hirsi Jamaa & Others v. Italy, App. No. 27765/09 (Eur. Ct. H.R. Feb. 23, 2012).

12. M.S.S. v. Belgium & Greece, App. No. 30696/09 (Eur. Ct. H.R. Jan. 21, 2011).

13. Soering v. United Kingdom, App. No. 14038/88 (Eur. Ct. H.R. July 7, 1989).

14. Tarakhel v. Switzerland, App. No. 29217/12 (Eur. Ct. H.R. Nov. 4, 2014).

C. Books

1. PAUL CRAIG & GRÁINNE DE BÚRCA, EU LAW: TEXT, CASES, AND MATERIALS (7th ed. 2020).

2. GUY S. GOODWIN-GILL & JANE MCADAM, THE REFUGEE IN INTERNATIONAL LAW (4th ed. 2021).

3. JAMES C. HATHAWAY & MICHELLE FOSTER, THE LAW OF REFUGEE STATUS (2d ed. 2014).

4. ELSPETH GUILD, STEVE PEERS & JONATHAN TOMKIN, THE EU CITIZENSHIP DIRECTIVE: A COMMENTARY (2d ed. 2019).

5. HELEN O'NIONS, ASYLUM: A RIGHT DENIED: A CRITICAL ANALYSIS OF EUROPEAN ASYLUM POLICY (2014).

6. STEVE PEERS, EU JUSTICE AND HOME AFFAIRS LAW: VOLUME I: EU IMMIGRATION AND ASYLUM LAW (4th ed. 2016).

D. Reports, Guidelines, and Institutional Materials

1. Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, WP251 rev.01 (Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/items/612053 (last visited June 21, 2026).

2. European Comm'n, AI Act, SHAPING EUROPE'S DIGITAL FUTURE, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (last visited June 21, 2026).

3. European Comm'n, Standardisation of the AI Act, SHAPING EUROPE'S DIGITAL FUTURE, https://digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation (last visited June 21, 2026).

4. European Parliamentary Research Service, Artificial Intelligence at EU Borders: Overview of Applications and Key Issues (2021), https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf (last visited June 21, 2026).

5. European Union Agency for Asylum, Practical Guide on Evidence and Risk Assessment (2024), https://www.euaa.europa.eu/sites/default/files/publications/2024-01/Practical-Guide-Evidence-Risk-Assessment.pdf (last visited June 21, 2026).

6. U.N. High Comm'r for Refugees, Handbook on Procedures and Criteria for Determining Refugee Status and Guidelines on International Protection (2019), https://www.unhcr.org/sites/default/files/legacy-pdf/5ddfcdc47.pdf (last visited June 21, 2026).

E. Journal Articles and Research Papers

1. Lilian Edwards & Michael Veale, Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For, 16 DUKE L. & TECH. REV. 18 (2017).

2. Gianclaudio Malgieri & Giovanni Comandé, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, 7 INT'L DATA PRIVACY L. 243 (2017).

3. Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 INT'L DATA PRIVACY L. 76 (2017).

4. Yiran Yang, Frederik Zuiderveen Borgesius, Pascal Beckers & Evelien Brouwer, Automated Decision-Making and Artificial Intelligence at European Borders and Their Risks for Human Rights (2024), https://arxiv.org/abs/2410.17278 (last visited June 21, 2026).

F. Online Legal and Policy Sources

1. European Data Protection Board, Automated Decision-Making and Profiling, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en (last visited June 21, 2026).

2. European Union Agency for Asylum, Country of Origin Information, https://euaa.europa.eu/country-origin-information (last visited June 21, 2026).

3. EUR-Lex, Regulation (EU) 2024/1689 of the European Parliament and of the Council, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (last visited June 21, 2026).

4. EUR-Lex, Regulation (EU) 2024/1348 of the European Parliament and of the Council, https://eur-lex.europa.eu/eli/reg/2024/1348/oj/eng (last visited June 21, 2026).

5. UNHCR, Asylum and Migration, https://www.unhcr.org/asylum-and-migration (last visited June 21, 2026).