Research Article

International Journal of Blockchain Applications and Financial Technology

Artificial Intelligence and Trusted Digital Credentials in Cross-Border Qualification Recognition

Edlira Adi Kahani Subashi[1]* & Enis Fita[2]

[1]Candidate University of Salento, Lecce, Italy
[2]Faculty of Economy, Law and Social Sciences, University College of Business, Tirana, Albania

***Corresponding author:** Edlira Adi Kahani Subashi, Candidate University of Salento, Lecce, Italy.

Submitted: 28 January 2026 **Accepted:** 03 February 2026 **Published:** 10 February 2026

Citation: *Subashi, E. A. K., & Fita, E. (2026). Artificial Intelligence and Trusted Digital Credentials in Cross-Border Qualification Recognition. Jou of Bloc App nd Fina Tech, 2(1), 01-07.*

Abstract

The continuous integration of Artificial Intelligence (AI) into higher education is redefining how qualifications are assessed and recognized across borders. This paper addresses the question of whether AI can strengthen the transparency, consistency, and efficiency of recognition procedures while remaining anchored to legal, ethical, and quality assurance principles. The analysis adopts a qualitative and comparative methodology, combining the review of international legal frameworks with selected institutional case studies. It examines instruments such as the Lisbon Recognition Convention, the Council of Europe Framework Convention on Artificial Intelligence, and the European AI Act, alongside initiatives such as CIMEA's ARDI and DiploMe platforms and the Europass Digital Credentials Infrastructure. The paper highlights both the opportunities introduced by AI, including reduced administrative burden and enhanced fraud detection, and the emerging risks, particularly those related to algorithmic opacity, bias, and due process. It also considers how trusted digital credential ecosystems and Distributed Ledger Technology (DLT) can strengthen document integrity and verifiability, drawing on DiploMe's blockchain-based publication and verification mechanisms, including digitally signed statements and QR-code or link-based "fast verification" features. Building on this foundation, the paper outlines operational requirements for competent authorities and higher education institutions, including risk-tiering of AI uses, minimum documentation and explainability expectations, clearly defined human oversight responsibilities, and accessible complaint and appeal pathways for applicants. It further discusses data quality and interoperability constraints when AI tools interact with digital credential infrastructures, emphasizing safeguards for cross-border data exchange, privacy-preserving design, and measures to prevent automation bias in decision-making. It concludes by proposing the development of a new subsidiary text to the Lisbon Recognition Convention to ensure the ethical, transparent, and accountable use of AI and trusted digital credentials in qualification recognition, and it offers a practical roadmap for piloting compliant AI-assisted recognition processes without eroding procedural fairness or institutional trust. In doing so, the paper positions AI-supported recognition not as a replacement for expert judgment, but as a regulated decision-support layer that must remain accountable to applicants' procedural rights and to the mutual-trust logic of cross-border recognition.

Keywords: Artificial Intelligence, Blockchain, Qualification Recognition, Lisbon Recognition Convention, Quality Assurance, Algorithmic Transparency.

Introduction

In recent decades higher education has undergone a profound transformation driven by digitalisation, globalisation, and the rapid diffusion of artificial intelligence (AI). Initially confined to administrative support functions, learning analytics, plagiarism detection and student advising, AI is now extending its influence into high-stakes decision-making domains, including the recognition of academic and professional qualifications. This shift is not merely technological; it reflects a deeper reconfiguration of how knowledge, skills and credentials are assessed, validated and trusted across borders. Recognition is therefore not a purely technical or bureaucratic process, but a legal, social and ethical mechanism that enables access to further study, professional mobility and full participation in the labour market [1, 2]. This raises a central governance dilemma: how to capture the administrative benefits of automation while preserving the legal guarantees that make recognition legitimate, contestable, and trusted.

In a context of intensified international mobility, diversified educational pathways and the proliferation of non-traditional credentials such as micro-credentials, joint degrees, digital badges and online programmes, recognition systems are under increasing pressure. Students and graduates expect faster decisions, greater consistency and clearer justifications, while institutions face growing volumes of applications and more complex qualification profiles. Delays, inconsistencies and opaque procedures risk undermining both individual opportunities and institutional credibility and may ultimately weaken trust in cross-border mobility frameworks. As recognition volumes grow and credential types diversify, the operational temptation to automate increases, making it essential to specify where automation is acceptable and where it must be constrained.

For more than two decades the Lisbon Recognition Convention (LRC) has provided the normative backbone for fair and transparent recognition, supported by its subsidiary texts and the professional work of the ENIC-NARIC networks [3, 4]. The Convention articulates a rights-based approach to recognition, centred on the presumption of recognition, the obligation to provide reasoned decisions and the right to appeal. These principles have contributed to building a culture of mutual trust across the European Higher Education Area and beyond. YYYYet, the practical enforceability of these principles depends on how decision processes are designed, recorded, explained, and reviewed when AI tools are introduced into the workflow.

However, these instruments were designed in a pre-digital era and are increasingly tested by technological change. AI offers powerful tools to streamline procedures, compare complex qualification frameworks, extract metadata from transcripts and detect fraudulent credentials [5, 6]. At the same time, it raises unresolved questions concerning transparency, bias, accountability and the right to appeal [7, 8]. The adoption of the Council of Europe Framework Convention on Artificial Intelligence in 2024 confirms that AI must operate within the boundaries of human rights, democratic values and the rule of law [9]. In recognition, this means that “better” outcomes cannot be assessed only by speed or throughput, but also by whether applicants can understand and challenge decisions, and whether authorities can demonstrate non-discrimination and proportionality.

Against this background, this paper examines how AI is reshaping recognition practices, focusing on both opportunities and vulnerabilities. Two research questions guide the analysis: (1) Can AI strengthen recognition while remaining faithful to international legal principles? and (2) Are existing legal and quality assurance frameworks sufficient, or is there a need for new instruments? The paper argues that a new subsidiary text to the Lisbon Recognition Convention is required to address the ethical and effective use of AI in recognition processes and to preserve trust, fairness and legal certainty in cross-border mobility. The paper’s original contribution lies in translating high-level human rights and QA principles into operational requirements for AI-assisted recognition, and in outlining the minimum clauses that a dedicated LRC subsidiary text would need to prevent fragmentation and safeguard procedural fairness.

Methodology

This study adopts a qualitative and comparative research design aimed at analysing the legal, ethical and governance implications of introducing artificial intelligence into the recognition of qualifications. The methodology is based primarily on systematic document analysis of international legal instruments, European policy documents and institutional reports that shape recognition practices and the regulation of AI. Core legal sources include the Lisbon Recognition Convention and its subsidiary texts the Council of Europe Framework Convention on Artificial Intelligence and European Union policy on automatic recognition [10, 11]. The analysis applies a structured lens focused on procedural rights (reason-giving and appeal), transparency and explainability, accountability and human oversight, non-discrimination and bias controls, and data governance in cross-border exchanges.

The analytical strategy combines doctrinal legal analysis with policy analysis. Legal provisions are examined in terms of their underlying principles, scope and mechanisms of implementation, with particular attention to procedural rights, transparency requirements and appeal mechanisms. Policy documents and quality assurance standards, in particular the Standards and Guidelines for Quality Assurance in the European Higher Education Area are analyzed to identify how fairness, accountability and consistency are operationalized in recognition procedures. This approach enables the identification of “governance gaps,” understood here as areas where existing norms do not specify how requirements should be met when recognition workflows rely on algorithmic tools.

In addition, selected institutional case studies are examined to illustrate emerging practices in digital and AI-supported recognition. These include CIMEA’s ARDI and DiploMe platforms and the Europass Digital Credentials Infrastructure. These cases are analyzed not as exhaustive empirical evidence, but as illustrative examples of how automation, digital credentialing and algorithmic tools are being introduced in practice. The case selection reflects initiatives that are institutionally anchored, operationally deployed in pilot or service form, and relevant to cross-border recognition workflows through verification, interoperability, or semi-automated decision support.

The study is exploratory in nature and aims to identify governance gaps, normative tensions and emerging patterns rather than to test causal hypotheses. The comparative dimension allows for the identification of convergences and divergences across legal and policy frameworks. The main limitation of the study lies in its reliance on documentary sources and pilot initiatives, which reflect early-stage developments rather than fully mature systems. Nevertheless, this approach provides a robust basis for mapping risks, opportunities and regulatory needs in the evolving field of AI-supported recognition. To mitigate this limitation, the paper focuses on minimum standards that remain valid across deployment maturity levels, rather than on performance claims tied to specific systems or models.

Analysis and Discussion

Legal and Institutional Foundations of Recognition

The Lisbon Recognition Convention (LRC), adopted in 1997 and ratified by a large majority of European states, constitutes the cornerstone of fair and transparent recognition practices in Europe and beyond. Its normative architecture is built on three fundamental principles: the presumption of recognition unless substantial differences are demonstrated, the obligation to provide written and reasoned decisions within a reasonable timeframe, and the right of applicants to appeal adverse decisions. Together, these principles establish recognition not as a discretionary favor, but as a rights-based administrative process grounded in legality and due process. Over time, these core principles have been operationalized through a set of subsidiary texts and professional instruments. The Recommendation on Criteria and Procedures for the Assessment of Foreign Qualifications clarified timelines, documentation requirements and procedural standards, while the Recommendation on the Use of Qualifications Frameworks promoted the systematic use of learning outcomes and level descriptors. The European Area of Recognition (EAR) Manual further consolidated best practices among ENIC-NARIC centres, contributing to greater procedural convergence across national systems. In practice, these standards function as a "trust infrastructure," ensuring that recognition authorities can justify decisions in comparable terms across jurisdictions.

However, these instruments were drafted in a pre-digital era and do not address the governance of automated or algorithmic decision-making. As recognition authorities begin to experiment with digital tools and AI-supported systems, this regulatory silence becomes increasingly problematic. In the absence of explicit standards, national practices risk diverging, thereby undermining the coherence and mutual trust that the LRC was designed to protect. This institutional gap provides the normative starting point for considering whether a new subsidiary text on AI is necessary to preserve the integrity of the recognition system in a digital age. Without a common reference point, "efficiency" may become the de facto criterion, while procedural safeguards are implemented unevenly or treated as optional.

Automatic Recognition and the Role of AI

Automatic recognition, as promoted by the 2018 Council Recommendation, represents a major policy shift aimed at reducing administrative burdens and facilitating academic mobility through mutual trust. Instead of relying on individual case-by-case assessments, automatic recognition presupposes that qualifications issued within aligned quality assurance frameworks should be accepted without substantial additional scrutiny. This model depends critically on transparency, interoperable qualifications frameworks and shared confidence in quality assurance mechanisms.

Within this context, AI has the potential to act as an enabling infrastructure. By analyzing large datasets, mapping learning outcomes to qualifications frameworks and detecting anomalies in documentation, AI can support faster and more consistent decision-making. Initiatives such as the Europass Digital Credentials Infrastructure and CIMEA's ARDI platform illustrate how semi-automated recognition can be implemented in practice. Yet, automatic recognition also reveals the limits of automation. Without robust safeguards, algorithmic matching may produce false equivalence or unjustified exclusion. AI systems must therefore remain embedded within a governance framework that preserves human oversight, transparency and the right to appeal. Automatic recognition can only function legitimately if efficiency gains are balanced by procedural fairness and accountability. A key distinction is therefore required between low-risk automation (e.g., intake, document completeness checks, verification prompts) and high-impact uses (e.g., recommending "substantial difference" outcomes), where stricter safeguards and mandatory human review should apply.

Human Rights and the Regulatory Instruments in Recognition

The Council of Europe Framework Convention on Artificial Intelligence marks a decisive normative shift by subjecting AI to binding human rights obligations . Unlike sectoral guidelines, this Convention treats AI as a socio-technical system capable of affecting fundamental rights, including the right to education, the right to a fair procedure and the principle of non-discrimination. In the context of recognition, these rights have direct operational consequences. Decisions informed by AI must be explainable, subject to meaningful human oversight and open to independent challenge [12]. Black-box systems that generate outcomes without intelligible reasoning risk undermining procedural guarantees under Article 6 ECHR (fair procedure), particularly where decisions determine access to further study or regulated professional pathways. Where applicants cannot meaningfully challenge an AI-informed decision, deficiencies may also engage Article 13 ECHR (effective remedy). Risks of disparate treatment or indirect discrimination linked to training data and model design must be assessed against Article 14 ECHR (non-discrimination), while the broader implications of recognition for access to education align with Article 2 of Protocol No. 1. In addition, the handling of applicant data and cross-border credential exchange raises privacy and data protection concerns that intersect with Article 8 ECHR. These guarantees should be operationalised through auditable procedures and QA criteria for AI supported recognition. This implies that recognition authorities must be able to demonstrate not only that a decision is correct, but that the pathway to the decision was reviewable, proportionate, and non-discriminatory, including where AI tools influenced the outcome.

These regulatory instruments thus reinforce the principle that innovation must strengthen, rather than weaken, procedural guarantees. Recognition authorities are not merely deploying technical tools, but exercising public power. The legitimacy of AI-supported recognition therefore depends on embedding these systems within a rights-based administrative framework that preserves accountability and legal certainty. In practical terms, this requires traceable decision logs, clear allocation of responsibility for override and review, and a minimum "explanation package" that applicants can use to activate remedies.

Ethical and Philosophical Dimensions

Beyond legal compliance, the introduction of AI into recognition raises deeper ethical and philosophical questions concerning agency, responsibility and justice. As Floridi argues, AI systems are not neutral instruments but value-laden artefacts shaped by the assumptions and priorities embedded in their design. In recognition, this insight is particularly salient, as algorithmic systems trained on past decisions may reproduce hidden biases and institutional hierarchies [13, 14]. Explainability and contestability therefore emerge as ethical imperatives rather than technical preferences. Applicants must be able to understand the reasoning behind decisions that affect their educational and professional trajectories. Without intelligibility, efficiency gains come at the cost of dignity and trust. Moreover, responsible innovation requires anticipatory governance capable of identifying risks before they crystallize into systemic injustices. Ethical reflection thus complements legal regulation by highlighting the moral limits of automation.

Recognition must remain a human-centred process, supported but never replaced by technology. AI may enhance efficiency, but its legitimacy ultimately depends on whether it reinforces fairness, inclusion and respect for persons. A further ethical risk lies in "automation bias," where human decision makers defer to algorithmic outputs even when they conflict with contextual knowledge or applicant-provided evidence; preventing such deference requires training, procedural checks, and explicit accountability mechanisms.

Table 1: Legal and Ethical Safeguards Relevant to AI Supported Qualification Recognition

Safeguard	Core requirement	Key legal and normative sources
Transparency and intelligibility	Applicants should receive clear information on whether and how AI is used, what data are processed, and what factors influence outcomes; reasons should be understandable enough to support contestability.	GDPR Arts. 12–15; GDPR Art. 22; ECHR Art. 6; CoE Framework Convention on AI (transparency and oversight); Lisbon Recognition Convention (fair recognition principles).
Nondiscrimination and bias prevention	AI supported processes should be designed, tested, and monitored to prevent discriminatory outcomes, including indirect discrimination; bias risks should be documented and mitigated.	ECHR Art. 14; CoE Framework Convention on AI (equality and non-discrimination).
Human oversight and accountability	Competent authorities must retain responsibility for decisions; meaningful human oversight should exist, including the ability to override automated outputs.	ECHR Art. 6; CoE Framework Convention on AI (oversight).
Data quality and proportionality	Data used for recognition should be accurate, relevant, and limited to what is necessary; processing should be proportionate to the purpose and risks involved.	GDPR Art. 5(1)(c)-(d).
Privacy and data protection	Cross-border exchange and processing of applicant data should ensure confidentiality, integrity, lawful basis, and secure handling, including privacy by design.	GDPR Arts. 5, 6, 25, 32; ECHR Art. 8.
Contestability and effective remedy	Applicants must be able to challenge outcomes, request review, and access clear, timely appeal procedures and remedies.	ECHR Art. 13; ECHR Art. 6; Lisbon Recognition Convention (procedural fairness and review mechanisms); CoE Framework Convention on AI (remedies and procedural safeguards).

Quality Assurance in AI-Supported Recognition

Quality assurance frameworks such as the ESG provide a normative foundation for transparency, accountability and continuous improvement in higher education (ENQA, 2015). These principles are equally relevant for AI-supported recognition, yet existing QA protocols were not designed for algorithmic systems. AI introduces new objects of quality assurance: training data, model updates, decision rules and audit trails. Without systematic oversight, algorithmic drift may undermine consistency and fairness over time. As shown in Table 2, governance requirements such as accountability, human oversight and data governance become central components of quality assurance in digital recognition. A new generation of QA criteria is therefore required, integrating technical audits with ethical and procedural standards. This evolution is essential to ensure that AI strengthens, rather than weakens, trust in recognition decisions. This also entails defining measurable QA indicators for AI-supported recognition, such as consistency across cases, error rates, disparate impact monitoring, turnaround times paired with appeal outcomes, and documented corrective actions when models or rules are updated.

Table 2: Operational Requirements for Trustworthy AI Assisted Recognition

Operational requirement	Practical implementation measures	Relevant frameworks and principles
Risk tiering of AI uses	Classify AI uses by impact on applicants and decision criticality; apply enhanced controls where outcomes affect access, admission, or professional pathways.	ECHR Art. 6; Protocol No. 1 Art. 2 (right to education).
Minimum documentation and traceability	Maintain documentation on model purpose, data sources, limitations, performance, and monitoring; ensure traceable decision logs and version control.	CoE Framework Convention on AI (transparency and oversight).
Explainability and reason giving	Provide intelligible explanations tailored to applicants; disclose key decision factors, limitations, and uncertainty; avoid black box justifications.	GDPR Arts. 12–15 and 22 (information and safeguards for automated decision-making); ECHR Art. 6; CoE Framework Convention on AI (transparency).
Meaningful human oversight	Assign a responsible decision maker; require human review for adverse outcomes; ensure override authority and clear accountability chains.	ECHR Art. 6; CoE Framework Convention on AI (oversight).
Bias testing and continuous monitoring	Conduct pre deployment bias assessment; monitor outcomes over time; implement corrective actions and periodic audits; document mitigation steps.	ECHR Art. 14; EU AI Act (risk management and monitoring for high-risk AI systems); CoE Framework Convention on AI (equality and non-discrimination).
Data governance and security	Apply data minimisation, purpose limitation, access control, retention policies, and security measures; ensure safe cross-border data exchange.	GDPR Arts. 5, 25, 32; ECHR Art. 8.
Appeal pathways and effective remedies	Provide clear complaint channels, deadlines, and review procedures; enable re-evaluation by a human; communicate outcomes and reasons.	ECHR Art. 13; ECHR Art. 6; Lisbon Recognition Convention; CoE Framework Convention on AI (remedies and procedural safeguards).
Interoperability with trusted digital credentials	Use interoperable credential formats; support verification of issuer identity and credential status; apply privacy preserving design and avoid storing personal data on-chain; ensure verifiable audit trails for integrity checks.	Europass Digital Credentials Infrastructure; CIMEA DiploMe (blockchain-based notarisation and verification mechanisms); GDPR Art. 25; CoE Framework Convention on AI (transparency and oversight).

Regulatory and Policy Gaps

Despite growing experimentation, there is no comprehensive European framework governing AI in recognition. The Lisbon Recognition Convention and its subsidiary texts remain silent on automated decision-making, while general AI regulation does not address sector-specific needs. This regulatory gap generates fragmentation and legal uncertainty. Without common standards, national authorities may adopt incompatible practices, undermining mutual trust. The absence of a subsidiary text dedicated to AI thus represents a structural weakness in the current framework. As summarized in Table 2, three measures appear essential: the adoption of a new subsidiary text, interoperable QA criteria and mandatory human oversight clauses. Together, these measures would anchor innovation within a coherent legal architecture. In addition, recognition-specific guidance is needed on procurement and vendor accountability, including access to system documentation, auditability requirements, and the ability of authorities to explain decisions even when tools are provided by external suppliers.

Case Studies and Emerging Practices

Existing pilot initiatives provide valuable insights into both opportunities and limits of AI supported recognition. CIMEA's ARDI and DiploMe platforms demonstrate how structured digitalisation can enhance efficiency, standardise workflows, and strengthen document integrity through traceable records and controlled validation processes (CIMEA, n.d.). DiploMe is described by CIMEA as a platform for comparability and verification services developed using blockchain technology, enabling applicants to submit credentials digitally, monitor the status of their request, and access the resulting Statement through a dedicated digital wallet in their DiploMe account (CIMEA, n.d.). CIMEA further indicates that issued Statements are generated in PDF format, digitally signed, and recorded on the CIMEA DiploMe Chain, enabling third party verification through a secure link or QR code that redirects to a "Fast Verification" page, where the Statement's metadata and blockchain transaction hash can be used to confirm integrity and authenticity (CIMEA, n.d.). These developments show how trust infrastructures can reduce verification friction, but they also highlight the need to distinguish between secure issuance and fair decision-making, which requires reasons, review, and remedy.

The Europass Digital Credentials Infrastructure offers a shared

European model for interoperable, machine verifiable credentials, supporting cross border portability and verification of qualifications (European Commission, 2022). At the same time, these cases reveal the fragmented nature of current governance. While technical interoperability is advancing through shared formats and trust infrastructures, standards for transparency, accountability, human oversight, and appeal remain underdeveloped. Moreover, blockchain based notarisation does not automatically resolve procedural fairness concerns. An immutable audit trail can record a decision without making the decision understandable or contestable. Estonia's digital diploma system illustrates the potential of secure, state backed infrastructures, yet large scale deployment across heterogeneous legal and institutional contexts remains limited. Taken together, these cases confirm that AI and trusted digital credentials can support more efficient and inclusive recognition only when embedded in strong public frameworks that clearly allocate responsibility, ensure explainability, and guarantee accessible remedies. Innovation without governance risks eroding, rather than strengthening, trust in recognition systems. To move beyond pilots, common evaluation criteria are required, including applicant-facing transparency metrics, appeal and reversal rates, and periodic bias and performance audits that are publicly reportable at least in aggregate form.

Policy and Operational Recommendations

Recognition authorities and HEIs should adopt a layered governance approach that translates human rights and quality assurance principles into operational controls. First, AI uses should be risk-tiered, distinguishing low-impact administrative automation from high-impact assessments that influence adverse outcomes, with mandatory human review for the latter. Second, competent authorities should define a minimum "explanatory package" for applicants, including disclosure of whether AI tools were used, the main factors considered, known limitations and clear instructions for requesting review. Third, authorities should implement traceability through decision logs, version control of models or rules and audit trails that enable independent scrutiny. Fourth, bias prevention should be treated as an ongoing duty through pre-deployment testing, continuous monitoring for disparate impact and documented mitigation actions. Fifth, interoperable digital credentials should be supported through common formats and issuer verification mechanisms, while applying privacy-preserving design and avoiding the storage of personal data on-chain. Finally, procurement and external tools use should be governed by contractual requirements for transparency, auditability and accountability, ensuring that public authorities remain able to explain and defend recognition decisions.

At the policy level, the LRC Committee and relevant European bodies should consider developing a dedicated subsidiary text that specifies minimum standards for AI-supported recognition, including transparency duties, human oversight requirements, non-discrimination safeguards, data governance expectations and effective remedies. A pilot roadmap could support implementation through controlled trials, defined evaluation indicators and iterative refinement, ensuring that innovation strengthens rather than weakens, trust in cross-border recognition.

Conclusion

Artificial intelligence is increasingly reshaping the governance of higher education and the recognition of qualifications, offering both significant opportunities and profound challenges. This paper has argued that AI can contribute to greater efficiency, consistency and integrity in recognition procedures, particularly in contexts characterized by growing mobility, diversified educational pathways and increasing administrative complexity. Tools such as digital credential infrastructures, semi-automated matching systems and fraud detection mechanisms demonstrate that technological innovation can support more timely and reliable recognition decisions. However, these gains should be assessed through a dual lens: operational performance and the preservation of procedural fairness, including the real-world accessibility of review and appeal for applicants.

At the same time, the analysis has shown that the introduction of AI into recognition cannot be treated as a purely technical upgrade. Recognition is a rights-based administrative process that directly affects access to education, employment and social mobility. Algorithmic systems that lack transparency, embed hidden biases or weaken avenues for appeal risk undermining the very principles of fairness, due process and non-discrimination that underpin the Lisbon Recognition Convention and the European Higher Education Area. Efficiency gains that come at the expense of accountability and human dignity are not compatible with the normative foundations of recognition. In this sense, explainability and contestability are not optional "ethical add-ons," but minimum conditions for lawful and legitimate recognition where algorithmic tools are involved.

The legal and institutional framework analysed in this paper reveals a structural tension between rapid technological change and slowly evolving governance instruments. While the Council of Europe Framework Convention on Artificial Intelligence establishes binding human rights obligations for AI, and quality assurance frameworks provide principles of transparency and accountability, the Lisbon Recognition Convention and its subsidiary texts remain silent on automated decision-making. This regulatory gap creates fragmentation and legal uncertainty, and risks eroding mutual trust among recognition authorities. The risk is not only inconsistent outcomes, but inconsistent standards of justification, documentation, and remedy, which can be equally damaging to mutual trust [15-22].

For this reason, the paper has argued for the adoption of a new subsidiary text to the Lisbon Recognition Convention dedicated specifically to the use of AI in recognition processes. Such an instrument should not prescribe particular technologies, but should articulate minimum standards for transparency, human oversight, explainability, data governance and appeal mechanisms. In parallel, quality assurance agencies should develop interoperable protocols for the audit and monitoring of algorithmic systems, integrating technical assessment with ethical and procedural safeguards. A possible structure for such a subsidiary text could include: scope and definitions of AI-supported recognition; mandatory disclosure and reason-giving duties; requirements for human oversight and accountability; risk-tiering of uses; bias assessment and monitoring; data governance for cross-border exchanges; recordkeeping and audit trails; and clear remedies and appeal rights.

Ultimately, the challenge is not whether AI will be used in recognition, but how it will be governed. If embedded within a coherent rights-based and quality-assured framework, AI can strengthen trust, fairness and access in cross-border mobility. If introduced without adequate safeguards, it risks transforming recognition from a human-centred process into an opaque administrative technology. The future of recognition in the digital age therefore depends on ensuring that innovation remains firmly anchored in law, ethics and respect for persons. This requires practical implementation, not only principles: defined responsibilities, auditable processes, applicant-facing transparency, and enforceable remedies that keep recognition accountable to the people it is meant to serve.

Conflict of Interest Disclosure

The authors declare no conflicts of interest.

Funding Acknowledgement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Ethical Approval Statement

Ethical approval was not required for this study because it is based on qualitative legal and policy analysis and selected institutional case studies using publicly available information and documentary sources; no human participants were recruited and no personal sensitive data were collected or processed for research purposes.

References

1. Council of Europe. (1997). Convention on the recognition of qualifications concerning higher education in the European region (Lisbon Recognition Convention). Council of Europe. https://www.coe.int
2. Knight, J. (2016). Transnational education remodeled: Toward a common TNE framework and definitions. Journal of Studies in International Education, 20(1), 34–47. https://doi.org/10.1177/1028315315602927
3. Council of Europe. (2001). Recommendation on criteria and procedures for the assessment of foreign qualifications. Council of Europe.
4. ENQA. (2015). Standards and guidelines for quality assurance in the European Higher Education Area (ESG). European Association for Quality Assurance in Higher Education.
5. European Commission. (2022). Europass digital credentials infrastructure: Overview. European Commission. https://europa.eu/europass
6. CIMEA. (2023). ARDI and DiploMe: Tools for digital recognition. Italian ENIC–NARIC Centre. https://www.cimea.it
7. Burrell, M. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 3(1), 1–12. https://doi.org/10.1177/2053951715622512
8. Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.
9. Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Council of Europe.
10. Council of Europe. (2013). Recommendation on the use of qualifications frameworks in the recognition of foreign qualifications. Council of Europe.
11. Council of the European Union. (2018). Council recommendation of 26 November 2018 on promoting automatic mutual recognition of higher education and upper secondary education and training qualifications and the outcomes of learning periods abroad (2018/C 444/01). Official Journal of the European Union, C 444, 1–6. https://eur-lex.europa.eu
12. Veale, M., & Binns, R. (2018). Fairer machine learning in the public sector: Lessons from the GDPR. Computer Law & Security Review, 34(2), 1–19. https://doi.org/10.1016/j.clsr.2018.02.002
13. Floridi, L. (2018). Soft ethics and the governance of the digital. Philosophy & Technology, 31(1), 1–8. https://doi.org/10.1007/s13347-018-0303-9
14. Floridi, L. (2021). The ethics of artificial intelligence: Key concepts and issues. Oxford University Press.
15. CIMEA. DiploMe: Comparability and verification services using blockchain. DiploMe by CIMEA. https://cimea-diplome.it/page-diplome
16. CIMEA. CIMEA DiploMe Chain: The renewed CIMEA's blockchain. DiploMe by CIMEA. https://cimea-diplome.it/page-CIMEA-diplome-chain
17. CIMEA. Comparability and verification service. DiploMe by CIMEA. https://cimea-diplome.it/page-comparability-verification-service
18. Council of Europe. (1950). Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights). Council of Europe.
19. Council of Europe. (1952). Protocol No. 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms. Council of Europe.
20. e-Estonia. (2023). AI and blockchain in education and public services. e-Estonia. https://e-estonia.com
21. European Parliament and Council of the European Union. (2016). 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
22. Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review, 1(1). https://doi.org/10.1162/99608f92.8cd550d1