



Algorithmic Borders and Global Law: A Qualitative Study of Digital Identity, Migration, and Legal Recognition

1. Tara. Sadeghi*: Department of International Law, Tarbiat Modares University, Tehran, Iran. Email: tara.sadeghi.ip@gmail.com (Corresponding Author)
2. Babak. Bagheri: Department of International Law, Tarbiat Modares University, Tehran, Iran
3. Pegah. Yeganeh: Department of Private Law, Tarbiat Modares University, Tehran, Iran

ABSTRACT

This study aimed to explore how digital identity systems, biometric infrastructures, and algorithmic border practices reshape migrants' experiences of legal recognition, rights access, and belonging in contemporary global law. This qualitative study was conducted in Tehran using semi-structured interviews with 24 participants selected through purposive and snowball sampling. Participants included migrants with cross-border legal experiences, legal practitioners, civil society workers, and digital governance specialists familiar with migration, identification, and administrative recognition. Data collection continued until theoretical saturation was achieved. Interviews were audio-recorded with informed consent, transcribed verbatim, and analyzed through thematic analysis. NVivo software was used for coding, retrieval, category development, and comparison across participant groups. Trustworthiness was enhanced through member checking, peer debriefing, reflexive memo-writing, and preservation of an audit trail. Five main categories were identified: digital identity as a gateway to legal personhood; algorithmic opacity and procedural vulnerability; biometric bordering and embodied exposure; fragmented recognition across legal systems; and human mediation as a corrective to technological exclusion. Participants described digital identity as both enabling and exclusionary: it could accelerate access to services, but it could also intensify dependency on databases, biometric verification, and opaque administrative judgments. Migrants emphasized that legal recognition increasingly depended not only on documents, but also on whether digital systems could "read" and validate them. The findings suggest that algorithmic border systems are transforming legal recognition from a documentary and institutional process into a data-mediated condition. While digital identity may improve administrative efficiency and service delivery, it also raises concerns regarding privacy, accountability, discrimination, and access to remedy. Rights-based governance, human oversight, transparency, and inclusive design are essential to ensure that digital borders do not reproduce or deepen existing inequalities in migration law.

Keywords: Algorithmic borders; digital identity; migration law; legal recognition; biometric governance; qualitative research; global law.

How to cite this article:

Sadeghi, T., Bagheri, B., & Yeganeh, P. (2025). Algorithmic Borders and Global Law: A Qualitative Study of Digital Identity, Migration, and Legal Recognition. *Contemporary Issues in Law, Culture, and Globalization*, 1(5), 51-60. <https://doi.org/10.61838/cileg.1.5.6>

© 2025 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Introduction

Legal identity has long been central to the relationship between individuals and the state. Birth certificates, passports, residence permits, refugee cards, work permits, and civil registration documents do not merely record personal facts; they

determine whether individuals can cross borders, claim protection, access services, work legally, open bank accounts, enroll in education, and participate in civic life. In the context of migration, legal identity is especially consequential because migrants often encounter multiple legal systems, fragmented documentation regimes, and competing institutional demands. A person may be recognized as a citizen in one jurisdiction, an irregular migrant in another, a refugee by an international organization, and an undocumented person by a host-state bureaucracy. This instability reveals that legal recognition is not a single event but an ongoing process of verification, classification, and institutional acceptance.

In recent years, this process has been increasingly transformed by digital technologies. States, humanitarian organizations, border agencies, and private contractors have adopted biometric registration, digital identity platforms, automated risk assessment, database interoperability, electronic visa systems, algorithmic triage, and mobile-based identity verification. These technologies are often justified in terms of efficiency, security, fraud prevention, humanitarian coordination, and administrative modernization. International development institutions have also emphasized the importance of legal identity as part of sustainable development, particularly through the global commitment to provide legal identity for all, including birth registration, by 2030 (United Nations Statistics Division, 2025). At the same time, scholars and human rights organizations have warned that digital identity systems can produce exclusion when they are implemented without sufficient attention to rights, accessibility, due process, and the lived conditions of mobile and marginalized populations (Manby, 2021; McGregor & Molnar, 2023).

The concept of the “algorithmic border” captures this transformation. Borders are no longer limited to territorial checkpoints or visible legal barriers. They are increasingly dispersed across databases, consular platforms, biometric archives, airline data systems, humanitarian registration tools, mobile applications, and automated decision-support systems. Amoore (2020) argues that algorithms increasingly govern social and political life by drawing inferences from partial, uncertain, and relational data. In migration governance, such inference-based systems may affect who is considered risky, credible, eligible, removable, or deserving of protection. Oliveira Martins and Jumbert (2022) similarly describe the digitalization of sovereignty as a process through which border power is exercised through data infrastructures rather than only through territorial enforcement. Thus, the contemporary border is not only a physical line but also a computational environment.

Digital identity occupies a central position in this environment. For migrants, refugees, asylum seekers, and stateless persons, the ability to prove identity may be essential for legal recognition and protection. UNHCR has emphasized that government-recognized identity documentation can support legal, socio-economic, and digital inclusion for persons of concern (UNHCR, 2023). Similarly, the World Bank’s Identification for Development initiative frames identification systems as foundational infrastructures for service delivery and development, while also stressing privacy, inclusion, and user protection (World Bank, 2017). However, the promise of digital identity must be examined critically. Digital identity can facilitate recognition, but it can also make recognition conditional on technological legibility. Individuals whose names are inconsistently transliterated, whose documents are expired or lost, whose biometric data cannot be captured reliably, or whose records are mismatched across databases may experience new forms of administrative invisibility.

This problem is particularly significant in migration contexts because migrants often move through legal and bureaucratic discontinuity. Their identities may be recorded differently across countries, agencies, languages, alphabets, and databases. A minor inconsistency in spelling, date format, place of birth, family relationship, or biometric record can produce major consequences. Torpey (2000) showed that modern states monopolized the legitimate means of movement by developing documentary systems such as passports. The digital era extends this logic: states increasingly seek to monopolize not only movement, but also machine-readable identity. The migrant subject is therefore governed through a combination of documentary evidence, biometric verification, database matching, and algorithmic risk analysis.

The use of artificial intelligence and automated decision-making in migration control has intensified these concerns. Recent scholarship identifies multiple uses of automated decision-making at borders, including biometric identification, risk assessment, border monitoring, and experimental technologies such as emotion detection or credibility assessment (Yang, Zuiderveen Borgesius, Beckers, & Brouwer, 2024). These systems raise human rights concerns related to privacy, non-discrimination, fair procedures, and effective remedies. Molnar (2019) argues that artificial intelligence in migration management frequently operates at the margins of accountability, affecting populations who already face structural vulnerability. Bither and Ziebarth (2021) likewise note that automated decision-making may assist public administrations, but migration policy actors often lack adequate governance frameworks to evaluate accuracy, bias, transparency, and proportionality.

The legal issue is not simply whether such systems are technically accurate. Rather, the deeper question is how they reshape legal recognition. Recognition before the law is a foundational principle of human rights. Yet algorithmic borders can make recognition dependent on data quality, system interoperability, institutional trust, and technological design. When a migrant cannot access a digital portal, fails biometric verification, lacks a recognized credential, or cannot understand the basis of an automated decision, legal personhood becomes practically unstable. The individual may remain formally entitled to rights while being practically blocked from exercising them. This distinction between formal rights and operational access is central to the present study.

Existing literature has examined digital borders, biometric governance, legal identity, and AI in migration management, but there remains a need for qualitative research that investigates how these systems are experienced and interpreted by actors situated within specific socio-legal contexts. Much of the discussion on algorithmic border governance is based on legal analysis, policy review, technical critique, or European border case studies. Less attention has been given to how migrants, legal practitioners, civil society actors, and technology specialists understand digital identity and legal recognition in urban settings where migration, legal pluralism, and administrative digitization intersect. Tehran provides a relevant context for such inquiry because it is a major urban center shaped by internal mobility, international migration, refugee presence, transnational family networks, and expanding digital administrative systems.

This study therefore investigates how digital identity and algorithmic border practices are understood by participants in Tehran who have direct or professional experience with migration and legal recognition. The study does not treat technology as neutral infrastructure. Instead, it approaches digital identity as a socio-legal arrangement that distributes recognition, vulnerability, and institutional power. The central research question is: How do migrants and migration-related professionals in Tehran perceive the role of digital identity and algorithmic border systems in shaping legal recognition, rights access, and belonging? By answering this question, the study contributes to global law, migration studies, and critical digital governance by showing how legal recognition is increasingly mediated by algorithmic infrastructures that operate across national, humanitarian, and administrative domains.

Methods and Materials

This study used a qualitative research design based on semi-structured interviews. A qualitative approach was selected because the research objective required in-depth exploration of participants' meanings, perceptions, and lived experiences rather than measurement of predetermined variables. The study focused on how participants interpreted the relationship between digital identity, migration, algorithmic border governance, and legal recognition. Semi-structured interviews were appropriate because they allowed the researcher to follow a consistent interview guide while also giving participants space to describe personal narratives, professional observations, and context-specific concerns in detail (Kvale & Brinkmann, 2015).

The study was designed as an exploratory qualitative inquiry. It did not aim to test a hypothesis or produce statistical generalization. Instead, it sought to identify recurring themes and conceptual patterns across participants' accounts. Thematic analysis was used because it provides a flexible yet systematic method for identifying, organizing, and interpreting patterned meanings within qualitative data (Braun & Clarke, 2006).

The participants consisted of 24 individuals from Tehran who were selected because of their direct or professional knowledge of migration, digital identity, and legal recognition. The sample included 10 migrants or persons with recent cross-border legal experiences, 6 legal practitioners working with migration, documentation, or administrative law issues, 4 civil society or humanitarian workers, and 4 digital governance or information technology specialists familiar with identity verification systems. Participants were recruited through purposive sampling, followed by snowball sampling to reach individuals with specialized experience.

Inclusion criteria were: being 18 years or older; residing, working, or receiving services in Tehran at the time of the study; having direct personal or professional experience related to migration, legal documentation, digital identity, border procedures, refugee registration, administrative recognition, or digital service access; and willingness to participate in an interview. Exclusion criteria included inability to provide informed consent or lack of relevant experience with the study topic.

The final sample size was determined through theoretical saturation. Saturation was considered achieved when additional interviews no longer generated substantially new categories or conceptual insights, and the main themes had become sufficiently developed and internally coherent (Saunders et al., 2018).

Data were collected through semi-structured interviews. The interview guide included open-ended questions about participants' experiences with identity documents, digital verification, biometric registration, migration-related legal procedures, online administrative platforms, access to services, cross-border recognition, and perceptions of fairness or exclusion in digital systems. Example questions included: "How do digital identity systems affect migrants' access to legal recognition?"; "Can you describe a situation in which a digital system helped or prevented someone from proving identity?"; "What concerns do you have about biometric or algorithmic systems in migration control?"; and "How should legal systems respond when digital records and human narratives conflict?"

Interviews lasted between 45 and 75 minutes. They were conducted in Persian, with some participants using legal, technical, or migration-related terms in English where relevant. All interviews were audio-recorded with participant consent and transcribed verbatim. Field notes were written after each interview to record contextual impressions, emerging ideas, and reflexive observations.

Data were analyzed using thematic analysis. The analysis followed six broad stages: familiarization with the data, initial coding, searching for themes, reviewing themes, defining and naming themes, and producing the final report (Braun & Clarke, 2006). NVivo software was used to organize transcripts, assign codes, retrieve coded segments, compare participant groups, and develop category structures.

The analysis began with repeated reading of transcripts. Initial codes were generated inductively from participants' accounts. These codes included terms such as "database mismatch," "biometric dependency," "lack of explanation," "service access," "fear of data sharing," "document translation," "human discretion," "digital exclusion," and "legal invisibility." Related codes were then grouped into subcategories and main categories. Throughout the process, the researcher wrote analytic memos to document interpretive decisions and connections between empirical findings and the theoretical literature.

To enhance trustworthiness, several strategies were used. Credibility was strengthened through member checking with selected participants and peer review of the coding framework. Dependability was supported by maintaining an audit trail of coding decisions, theme revisions, and analytic memos. Confirmability was addressed through reflexive note-taking to reduce

unexamined assumptions. Transferability was supported by providing detailed descriptions of the research setting, participant characteristics, and category development (Lincoln & Guba, 1985).

The study followed standard ethical principles for qualitative research. Participation was voluntary, and all participants received information about the purpose of the study, interview procedures, confidentiality, and their right to withdraw. Written or verbal informed consent was obtained before each interview. Pseudonyms or participant codes were used in transcripts and reporting. Identifying details were removed or modified to protect confidentiality, especially because migration status and documentation experiences may be sensitive. Audio files and transcripts were stored securely and accessed only for research purposes.

Findings

The study included 24 participants from Tehran. Of these, 13 participants were male and 11 were female. In terms of age, 5 participants were between 20 and 29 years old, 9 were between 30 and 39 years old, 7 were between 40 and 49 years old, and 3 were 50 years old or older. Regarding educational level, 4 participants had completed secondary education, 7 held bachelor's degrees, 9 held master's degrees, and 4 held doctoral or professional degrees. In terms of participant role, 10 participants were migrants or individuals with direct cross-border legal experiences, 6 were legal practitioners, 4 were civil society or humanitarian workers, and 4 were digital governance or information technology specialists. The diversity of participants enabled the study to compare personal experiences of legal recognition with professional interpretations of digital identity and algorithmic border systems.

The first main category concerned the role of digital identity as a gateway to legal personhood. Participants repeatedly described legal recognition as increasingly dependent on digital registration, online verification, biometric records, and database visibility. For migrants, having a document was no longer sufficient if the document could not be confirmed by a digital system. Several participants explained that access to banking, employment, education, health care, mobile services, and administrative procedures depended on whether their identity could be validated through official or semi-official platforms. A migrant participant stated, "Before, I thought identity meant having a paper. Now I feel identity means being accepted by the system. If the system does not show my name, the paper in my hand becomes weak" (P04). Legal practitioners similarly observed that digital identity had become an operational condition for exercising rights. One lawyer noted, "The law may say a person has rights, but the office asks for a code, a digital record, or biometric confirmation. Without that, the right remains theoretical" (P13). This category shows that digital identity was perceived as both enabling and restrictive: it could accelerate administrative recognition, but it could also convert legal personhood into a form of technological legibility.

The second category was algorithmic opacity and procedural vulnerability. Participants reported that digital and automated systems often produced decisions, delays, flags, or rejections without clear explanation. Migrants described uncertainty when online applications were rejected or suspended without knowing whether the problem was related to documentation, spelling, biometric records, risk classification, or data mismatch. A participant with migration experience explained, "When an officer says no, at least you can ask why. When the portal says rejected, you do not know who decided, what was wrong, or how to defend yourself" (P07). Legal professionals emphasized that opacity weakened procedural justice because individuals could not effectively challenge decisions whose logic was unknown. One lawyer stated, "The main problem is not only that a digital system makes mistakes. The problem is that the mistake becomes invisible, and the person must prove that the machine is wrong" (P15). Participants also described a shift in the burden of proof: instead of institutions explaining decisions, migrants had to resolve unexplained inconsistencies. This category suggests that algorithmic systems may intensify procedural vulnerability when transparency, appeal mechanisms, and human review are inadequate.

The third category concerned biometric bordering and embodied exposure. Participants described biometric data—fingerprints, facial images, iris scans, and digital photographs—as powerful forms of identification that could help prevent fraud and support continuity across systems. However, they also expressed concern that biometric registration made the body itself a border document. Migrants reported feelings of discomfort, fear, and loss of control when required to provide biometric data without understanding how long it would be stored, who could access it, or whether it could be shared across agencies or countries. One participant said, “When they take your fingerprint, it feels final. You cannot change your finger like you can replace a lost paper. It follows you everywhere” (P02). Civil society workers emphasized that biometric systems may be particularly sensitive for refugees, undocumented migrants, and people with previous experiences of state violence. A humanitarian worker noted, “For some migrants, biometrics are not neutral. They remember surveillance, deportation, police control, and fear. The technology may be presented as service delivery, but it is also experienced as exposure” (P18). This category reveals that biometric identity systems are not merely technical tools; they are embodied encounters with state and institutional power.

The fourth category was fragmented recognition across legal systems. Participants emphasized that digital identity does not automatically solve the problem of legal recognition because recognition remains divided across states, organizations, databases, and legal categories. A person may be recognized by one authority but not another, registered in one system but invisible in another, or documented under different spellings and classifications. Migrants described difficulties when documents issued in one country or by one institution were not accepted elsewhere. One participant explained, “I had proof from one office, but another office said it was not in their system. I was the same person, but legally I became different in each place” (P09). Technology specialists also noted that interoperability can be both a solution and a risk. While linked databases may reduce duplication, they can also spread errors and increase surveillance. One IT specialist stated, “If systems are connected without accountability, one wrong record can travel faster than the person can correct it” (P22). This category demonstrates that digital identity may reproduce legal fragmentation when institutional recognition is not harmonized, rights-based, and accountable.

The fifth category concerned the importance of human mediation as a corrective to technological exclusion. Across participant groups, there was strong agreement that digital systems should not replace human judgment in migration-related legal recognition. Participants valued digital tools when they improved speed, reduced corruption, or made procedures more predictable, but they objected to systems that eliminated explanation, discretion, and empathy. A legal practitioner stated, “Technology can organize the file, but it should not become the judge of the person’s existence” (P14). Migrants emphasized the need for trained officers, interpreters, legal advisors, and civil society intermediaries who could help resolve inconsistencies and explain procedures. One migrant participant said, “The only time my problem moved forward was when a person listened and compared the documents carefully. The system had blocked me, but a person understood the story” (P06). This category indicates that participants did not reject digital identity in principle; rather, they called for hybrid systems in which digital verification is combined with human review, legal safeguards, accessible appeals, and contextual understanding.

Discussion

This study explored how participants in Tehran perceived the relationship between algorithmic borders, digital identity, migration, and legal recognition. The findings show that digital identity is increasingly experienced as a condition of practical legal personhood. Participants did not define recognition only as possession of official documents; rather, they associated recognition with being visible, searchable, verifiable, and accepted within digital administrative infrastructures. This finding aligns with scholarship showing that legal identity has become a central development and governance objective while also raising concerns about exclusion and harm when implemented without sufficient safeguards (Manby, 2021; World Bank, 2017).

It also extends Torpey's (2000) argument regarding the state's documentary control over movement by showing how contemporary recognition depends not only on documents but also on database legibility. In this sense, algorithmic borders transform identity from a legal status into an infrastructural condition. The migrant becomes recognizable when paper documents, biometric records, administrative categories, and digital systems align.

The first finding, digital identity as a gateway to legal personhood, reflects a broader transformation in global law and governance. International organizations increasingly frame identity as essential for inclusion, development, and rights access. UNHCR (2023) emphasizes that recognized identity documentation can support legal, socio-economic, and digital inclusion for refugees and other persons of concern. However, participants' accounts reveal that digital identity may also create a new threshold of exclusion. Individuals who cannot satisfy digital verification requirements may be prevented from exercising rights that formally belong to them. This supports Manby's (2021) warning that legal identity initiatives should follow a "first, do no harm" approach. Digital identity systems can improve access, but they may also intensify dependency on institutional categories, data quality, and technological infrastructure. The study therefore suggests that legal recognition should not be reduced to digital registration. Recognition must include accessible procedures for correction, alternative proof, contextual assessment, and protection against exclusion.

The second finding, algorithmic opacity and procedural vulnerability, is consistent with literature on automated decision-making in migration governance. Yang et al. (2024) identify privacy, non-discrimination, fair trial, and effective remedy as key human rights risks associated with automated decision-making at borders. Participants in the present study described these risks in practical terms: unexplained rejections, unclear responsibility, inability to challenge decisions, and a reversed burden of proof. This finding also corresponds with Molnar's (2019) argument that AI and automated systems in migration management often affect people who are already structurally vulnerable and may lack the resources to challenge opaque systems. In legal terms, opacity undermines procedural justice because affected individuals cannot understand the basis of decisions or meaningfully contest them. The findings indicate that a human-in-the-loop model is insufficient if human review is superficial or if officials simply rely on system outputs. Effective remedy requires intelligible explanations, accessible appeal procedures, independent oversight, and the ability to correct data errors.

The third finding, biometric bordering and embodied exposure, supports critical scholarship on biometric governance and digital borders. Biometric technologies are often presented as reliable solutions to identity fraud and administrative uncertainty, but participants described them as emotionally and politically charged. Their accounts align with Ajana's (2013) analysis of biometrics as a mode of governing identity and with recent studies showing how biometric technologies reshape citizenship, border control, and migrant subjectivity (Segate, 2024; Tsagarousianou, 2024). The body becomes a durable identity credential that can travel across systems, institutions, and jurisdictions. For migrants, this durability can be protective when it preserves identity continuity, but it can also be threatening when it increases surveillance, deportability, or data-sharing risks. The finding is also consistent with McGregor and Molnar's (2023) human rights-based approach to digital border governance, which emphasizes legality, necessity, proportionality, non-discrimination, and remedy. Biometric systems in migration contexts must therefore be evaluated not only for technical accuracy but also for their impact on dignity, autonomy, privacy, and power.

The fourth finding, fragmented recognition across legal systems, highlights a central paradox of digital identity. Digital systems are often promoted as tools for integration and interoperability, yet participants reported that recognition remained fragmented across institutions. A person could be visible in one database and invisible in another. This finding aligns with Cheesman's (2022) critique of self-sovereign identity for refugees, which shows that technological portability does not automatically resolve the political problem of recognition. Even when credentials are technically verifiable, legal acceptance depends on institutional authority, trust, and jurisdictional willingness. Similarly, Oliveira Martins and Jumbert (2022) argue

that digital border infrastructures are tied to sovereignty and political control. Interoperability may reduce administrative friction, but it may also allow errors, suspicion, and surveillance to circulate across systems. The present study therefore suggests that legal recognition requires more than technical connection between databases. It requires accountable governance of data-sharing, clear responsibility for errors, and legal standards for cross-institutional acceptance.

The fifth finding, human mediation as a corrective to technological exclusion, shows that participants did not reject digital identity or algorithmic tools categorically. Rather, they wanted digital systems to remain subordinate to legal judgment, human rights, and contextual understanding. This finding is important because it avoids a simplistic opposition between technology and law. Participants recognized that digital systems can reduce delays, improve record management, and support access to services. However, they insisted that migration-related decisions require human interpretation because identity, vulnerability, family history, displacement, and documentation loss cannot always be captured by standardized data fields. This finding aligns with Bither and Ziebarth's (2021) argument that automated decision-making in migration policy requires governance capacity, transparency, and accountability. It also resonates with Amoore's (2020) argument that algorithms produce partial accounts of persons through attributes and correlations. Human mediation is therefore not merely an administrative supplement; it is a legal safeguard against reducing persons to data profiles.

Overall, the study contributes to global law by showing that algorithmic borders are reshaping the meaning of legal recognition. Recognition is no longer located solely in courts, civil registries, immigration offices, or physical border posts. It is increasingly distributed across digital platforms, biometric systems, databases, and automated classifications. This diffusion complicates accountability because responsibility may be divided among states, international organizations, private contractors, software providers, and frontline officers. It also challenges traditional legal remedies because affected individuals may not know whether harm resulted from law, policy, code, data error, institutional discretion, or system design. The findings suggest that global law must respond by developing stronger rights-based standards for digital identity and border technologies. Such standards should include transparency, explainability, independent auditing, data minimization, privacy by design, non-discrimination testing, accessible correction mechanisms, and meaningful human review.

This study has several limitations. First, the research was conducted in Tehran with 24 participants, and the findings cannot be statistically generalized to all migrants, legal professionals, or digital identity systems. Second, the study relied on semi-structured interviews, meaning that findings are based on participants' perceptions, memories, and interpretations rather than direct observation of digital border systems or administrative decision-making processes. Third, because migration status and legal documentation are sensitive topics, some participants may have avoided discussing certain experiences in detail. Fourth, the sample included diverse participant groups, but the number of participants in each subgroup was limited. Future studies with larger and more varied samples could provide deeper comparison between migrants, lawyers, policymakers, humanitarian organizations, and technology developers.

Future research should examine algorithmic borders through comparative, multi-sited, and interdisciplinary designs. Comparative studies across different countries could show how digital identity systems vary according to legal tradition, migration policy, data protection law, and administrative capacity. Ethnographic research inside border agencies, humanitarian registration centers, legal clinics, and digital service offices could provide deeper insight into how digital identity decisions are made in practice. Future studies should also investigate specific technologies such as biometric verification, automated risk assessment, digital wallets, refugee registration platforms, and database interoperability. Mixed-methods research could combine interviews with policy analysis, technical audits, and case-file review. Finally, future research should include the perspectives of women, children, stateless persons, undocumented migrants, and people with disabilities, as these groups may face distinctive barriers in digital recognition systems.

Policymakers and institutions should ensure that digital identity and algorithmic border systems are designed around human rights rather than administrative convenience alone. Migration-related digital systems should provide clear explanations for decisions, accessible appeal procedures, alternative non-digital routes, and mechanisms for correcting data errors. Biometric data should be collected only when necessary and proportionate, with strict limits on storage, sharing, and secondary use. Legal aid providers and civil society organizations should receive training on digital identity procedures so they can help migrants navigate system errors and documentation mismatches. Technology developers should involve migrants and affected communities in system design and evaluation. Above all, digital systems should support legal recognition, not replace it; the final measure of legitimacy should be whether technology strengthens dignity, fairness, and access to rights.

Conclusion

This qualitative study examined how digital identity, algorithmic border systems, and migration governance reshape legal recognition in contemporary global law. Based on interviews with 24 participants in Tehran, the study identified five main categories: digital identity as a gateway to legal personhood; algorithmic opacity and procedural vulnerability; biometric bordering and embodied exposure; fragmented recognition across legal systems; and human mediation as a corrective to technological exclusion. The findings show that digital identity can support inclusion by facilitating documentation, service access, and administrative efficiency. However, it can also create new forms of exclusion when recognition becomes dependent on database visibility, biometric verification, algorithmic classification, or institutional interoperability.

The study argues that algorithmic borders are not merely technological innovations; they are socio-legal infrastructures that determine how migrants are seen, classified, and recognized. As legal identity becomes increasingly digitized, global law must protect individuals from being reduced to data profiles or excluded by opaque systems. Rights-based governance, transparency, accountability, privacy protection, non-discrimination, and meaningful human review are essential. Digital identity should enhance legal recognition, not make rights conditional on technological legibility. In migration contexts, where identity is often contested, fragmented, or vulnerable, the law must ensure that every person remains recognizable not only to databases, but also before institutions, communities, and the law itself.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

- Ajana, B. (2013). *Governing through biometrics: The biopolitics of identity*. Palgrave Macmillan.
- Amoore, L. (2020). *Cloud ethics: Algorithms and the attributes of ourselves and others*. Duke University Press.
- Bither, J., & Ziebarth, A. (2021). *Automating decision-making in migration policy: A navigation guide*. Robert Bosch Stiftung.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. doi: 10.1191/1478088706qp063oa
- Cheesman, M. (2022). Self-sovereignty for refugees? The contested horizons of digital identity. *Geopolitics*, 27(1), 134–159. doi: 10.1080/14650045.2020.1823836
- International Organization for Migration. (2023). *Access to digital identity for people on the move in Europe*. IOM.
- Kvale, S., & Brinkmann, S. (2015). *InterViews: Learning the craft of qualitative research interviewing* (3rd ed.). Sage.
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.
- Manby, B. (2021). The Sustainable Development Goals and “legal identity for all”: “First, do no harm.” *World Development*, 139, 105343. doi: 10.1016/j.worlddev.2020.105343
- McGregor, L., & Molnar, P. (2023). *Digital border governance: A human rights based approach*. Office of the United Nations High Commissioner for Human Rights and University of Essex.
- Molnar, P. (2019). Technology on the margins: AI and global migration management from a human rights perspective. *Cambridge International Law Journal*, 8(2), 305–330.
- Oliveira Martins, B., & Jumbert, M. G. (2022). Border security and the digitalisation of sovereignty: Insights from EU borderwork. *European Security*, 31(3), 475–494. doi: 10.1080/09662839.2022.2101884
- Rinaldi, A. (2025). The use of artificial intelligence technologies in border and migration control and the subtle erosion of human rights. *International and Comparative Law Quarterly*, 74(1), 1–29.
- Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, 52, 1893–1907. doi: 10.1007/s11135-017-0574-8
- Segate, R. V. (2024). Biometric technology at the borders of citizenship. *Frontiers in Human Dynamics*, 6, 1–14.
- Torpey, J. (2000). *The invention of the passport: Surveillance, citizenship and the state*. Cambridge University Press.
- Tsagarousianou, R. (2024). Biometric data, power and resistance at the borders of Europe. *Media, Culture & Society*, 46(2), 290–307.
- United Nations High Commissioner for Refugees. (2023). *Registration and identity management*. UNHCR.
- United Nations Statistics Division. (2025). *SDG indicator metadata: Indicator 16.9.1*. United Nations.
- World Bank. (2017). *Principles on identification for sustainable development: Toward the digital age*. World Bank.
- Yang, Y., Zuiderveen Borgesius, F., Beckers, P., & Brouwer, E. (2024). Automated decision-making and artificial intelligence at European borders and their risks for human rights. *Computer Law & Security Review*, 55, 106066.