Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Digital Identity and Legal Recognition in International Law

Article History:

Name of Author:
Cody Robinson[1], Michael Hill[2], April Rodriguez[3] and Shirley Diaz[4]

Affiliation: [1]Head of Department, Department of Marketing, Central Eurasia University, Kazakhstan
[2]Associate Professor, Department of Commerce, Alexandria School of Governance, Egypt
[3]Senior Research Fellow, Department of Marketing, Cape Innovation Institute, South Africa
[4]Dean of Commerce, Department of Corporate Governance, Nairobi Metropolitan University, Kenya
Corresponding Author: Cody Robinson

How to cite this article: Cody Robinson, *et, al*. Digital Identity and Legal Recognition in International Law. *J Community Med* 2023;4(1);7-10.

Abstract: Digital identity is rapidly becoming the cornerstone of global citizenship, commerce, and governance in the digital era. Defined by the interplay of personal, biometric, behavioral, and legal data, digital identities now determine individuals' access to essential services and participation in the digital economy. This article explores the evolving legal foundations and human rights dimensions of digital identity, examining international treaties, domestic frameworks (such as the GDPR, eIDAS, Aadhaar, and CCPA), and the absence of harmonized global norms. While digital identities offer significant benefits for inclusion, accessibility, and privacy control, they also pose risks including exclusion, surveillance, cross-border misuse, and legal uncertainty for stateless populations. Through a comparative analysis of regulatory approaches and emerging technologies such as Self-Sovereign Identity (SSI) and biometric authentication, this article underscores the urgent need for global legal standards. It concludes that ensuring digital identity rights as an extension of legal personality and privacy is essential for equitable and secure digital transformation worldwide.

Keywords: Digital identity, legal identity, international law, human rights, GDPR, eIDAS, Aadhaar, cross-border data,

INTRODUCTION

As societies, economies, and governments transition into the digital era, **digital identity** is becoming foundational to citizenship, commerce, and rights. The advent of digital identities is reshaping traditional concepts of legal personality, privacy, and cross-border recognition. However, the international legal system faces significant challenges in keeping pace with this rapid transformation. This article explores the definition, legal frameworks, human rights implications, practical challenges, and the future trajectory of digital identity in the context of international law.

WHAT IS DIGITAL IDENTITY?

Digital identity refers to a collection of *digitally stored data and attributes* that uniquely identify an individual, organization, or even device within online and virtual environments. At its core, digital identity bridges personal data (such as biometrics, legal names, and behavioral traits) with legal recognition, enabling entities to access digital services, transact, and prove status across borders.

Key elements comprise:

- Personal identifiers (name, date of birth, biometrics)
- Credentials (passwords, digital certificates)
- Behavioral information (login patterns, device usage)
- Legal links (citizenship, official status)[1][2]

THE LEGAL FOUNDATIONS OF DIGITAL IDENTITY

International Human Rights Instruments

The right to legal identity is longstanding in international law, but explicit *digital identity* recognition is still evolving:

- **Universal Declaration of Human Rights (UDHR, 1948)**: Article 6 establishes the right to recognition as a person before the law[2][3].
- **International Covenant on Civil and Political Rights (ICCPR, 1966)**: Articles 16 and 24 underline legal personality and the right of children to identity.
- **UN Sustainable Development Goal 16.9**: Calls for legal identity for all, including birth registration, by 2030.

While these refer to *legal identity* broadly, there is growing academic and policy consensus that digital identity is an extension and necessary adaptation of these established rights for the digital age[2][3].

Domestic and Regional Frameworks

- **European Union (GDPR, eIDAS Regulation)**: Offers robust legal protection for personal data, including data forming digital identities, and facilitates mutual recognition of electronic identification across member states[3].
- **National Identities**: India's Aadhaar system, Estonia's digital ID, and similar frameworks provide models, though often raise privacy and exclusion issues.

Legal Recognition: Gaps and Progress

Digital Identity as a Legal Right

A digital identity is often not recognized as a *standalone legal right* in international law, but protected as part of the broader right to identity and privacy[4][2]. Some legal systems and charters (e.g., Spain's Charter of Digital Rights) explicitly reference digital identity, while most extend rights from physical to digital spheres.

Interplay with Privacy, Data Protection, and Anonymity

- **GDPR and global data protection laws**: Protect digital identity attributes as personal data.
- **Right to be Forgotten**: Landmark European Court of Justice rulings (e.g., *Google Spain SL v. AEPD*) have established that digital identity can be curated and controlled by the subject[3].

Digital identity creation has unique legal boundaries around anonymity and pseudonymity, fundamental to privacy and freedom of expression. International law increasingly sees digital anonymity as requiring protection, though the legal status of anonymous identities varies[3].

Human Rights and Digital Identity: Opportunities and Risks

Benefits

- **Global Accessibility & Inclusion**: Digital identity can facilitate legal recognition, social services, and participation for those without traditional ID, addressing gaps for refugees or marginalized groups[5][6].
- **Cross-Border Transactions**: Streamlines access to banking, education, healthcare, and voting.
- **Personal Data Control**: Enables stronger assertion of individual data rights and informed consent[7].

Risks

- **Exclusion & Discrimination**: Poorly implemented systems may exclude stateless, displaced, or marginalized persons, worsening inequality and statelessness[6].
- **Mass Surveillance & Security**: Weak safeguards can enable surveillance, data breaches, and misuse.
- **Lack of Remedial Mechanisms**: Legal recourse in case of digital ID revocation or misuse is often unclear, especially across borders.
- **Weaponization in Conflict Zones**: Digital ID can be misused to target or disenfranchise minorities in fragile states[6].
- **Consent and Transparency**: Users may not fully understand or control the extent of identity usage or sharing[2][8].

Comparative Legal Frameworks

Region	Primary Legal Instruments	Key Provisions on Digital Identity

European Union	GDPR, eIDAS Regulation	Data protection for personal data; mutual recognition of electronic IDs; standardized cross-border recognition[3]
United States	CCPA, state-based privacy laws	Varying treatment of "personally identifiable information"; lacks comprehensive digital identity legal framework[3][9]
India	Digital Personal Data Protection Act, Aadhaar Act	Mandatory digital ID for many services; ongoing privacy and constitutional challenges[9][6]
Global	UN Sustainable Development Goals, various conventions	Aspirational right to legal (and by extension, digital) identity for all; diverse implementation at state level

Graph: Growth of Digital Identity Legal Frameworks (2015-2025)
[image:1]
A line graph illustrating the rapid adoption of digital identity laws and frameworks globally, with notable spikes post-GDPR (2018) and the surge in national digital ID programs (2020-2025).

Key Challenges for International Law

- **Lack of Harmonization**: National laws diverge widely on privacy standards, mutual recognition, and the definition of digital identity[10][3].
- **Cross-Border Enforcement**: No global enforcement mechanism for digital identity misuse or unauthorized data transfer[3].
- **Evolving Technologies**: Blockchain-based systems, the Metaverse, and AI introduce complexities around autonomy, verification, and legal subjectivity[11][8].
- **Gaps for the Stateless and Displaced**: Refugees and undocumented migrants are especially vulnerable if digital ID is tied to citizenship or official status.

FUTURE DIRECTIONS

Toward a Globally Recognized Digital Identity
Efforts from entities like the UN and World Bank emphasize developing universal standards, inclusive frameworks, and cross-border interoperability[2][10]. Principles include:

- Privacy by design
- Consent and user control
- Access and inclusion guarantees
- Robust security standards

Social and Technological Trends

- **Mobile and Biometric IDs**: Rise of mobile-based credentials and biometrics for authentication, raising both convenience and ethical concerns[7][12].
- **Self-Sovereign Identity (SSI)**: Emergence of decentralized, user-controlled digital identities.
- **AI and Deepfakes**: New threats to identity integrity and authenticity.

Illustration: Components of a Digital Identity System
[image:2]
Infographic displaying the layers of digital identity: core identity data, biometric markers, authentication methods, and legal/consent controls.

CONCLUSION

Digital identity stands at the intersection of technological innovation and fundamental human rights. International law, though foundational, still lags behind the realities of our digital society. To protect individuals and strengthen transnational trust, policy and legal frameworks must focus on harmonization, inclusion, robust privacy protections, and recourse mechanisms. As digital identities deepen their presence in every walk of global life, their legal recognition, integrity, and ethical management are essential to ensuring *digital citizenship* for all.

"The right to identity, as an international fundamental human right, should now be recognized and protected in relation to digital identity." – Clare Sullivan[3]

For further reading, consult the cited academic legal sources and review standards by the UN, World Bank, EU, and national authorities on digital identity.

[image:1]
[image:2]

REFERENCES

1. https://en.wikipedia.org/wiki/Digital_identity
2. https://academic.oup.com/ijlit/article/doi/10.1093/ijlit/eaae019/7760180
3. https://policyreview.info/articles/analysis/legal-boundaries-digital-identity-creation
4. https://www.signaturit.com/blog/what-defines-your-digital-identity-and-what-legal-rights-are-associated-with-it/
5. https://www.futureagenda.org/focus-on/future-of-digital-identity/
6. https://www.salzburgglobal.org/news/topics/article/between-progress-and-exclusion-the-human-rights-challenges-of-digital-id
7. https://www.identity.com/2025-predictions-for-the-future-of-digital-identity/
8. https://journals.sagepub.com/doi/10.1177/2053951719855091
9. https://emudhra.com/en/blog/the-intersection-of-digital-identity-and-legal-compliance
10. https://emudhra.com/en/blog/cross-border-digital-identity-challenges-and-opportunities
11. https://sands.edpsciences.org/articles/sands/full_html/2023/01/sands20220011/sands20220011.html
12. https://egovstandards.gov.in/sites/default/files/2021-07/Guidelines on Mobile as Digital identity.pdf

