

## Legal And Ethical Considerations of Managing Identities, Ranging from Aadhaar to Global Digital Ids

<sup>1</sup>Dr. Petikam Sailaja, <sup>2</sup>Prof. Dr. N. Rajeswari, <sup>3</sup>Dr kandula Veera Brahman,

<sup>1</sup>Associate Professor, KLEF College of Law, KLEF Deemed To Be University, Guntur, AP

<sup>2</sup>Faculty of Law, Dr MGR Educational and Research Institute (Deemed to be University), Chennai-95

<sup>3</sup>Associate Professor, DNR college of Law Bhimavaram west Godavari District, A.P PIN-534203

**Abstract:** Digital identity systems have quickly grown in number and are now being used to prove an individual's identity and provide services by governments, institutions and private organisations. Digital IDs are now part and parcel of the governance architecture in India with Aadhaar, and are now increasingly playing a key role in promoting financial inclusion, healthcare services, and social welfare distribution, as well as in enabling digital transactions across borders globally. The potential for efficiency, transparency and access for public services is juxtaposed with important legal and ethical issues regarding privacy, surveillance, data security, exclusion, algorithmic discrimination and misuse of personal information. The more these technologies are becoming involved in biometric, artificial intelligence and centralised databases, the more debates have been raised about informational self-determination and constitutional protection. The understanding of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India has changed the legal landscape in India on digital identity governance. There are also differences in regulatory approaches to the trade-off between innovation and civil liberties at the international level, for instance with the European Union's data protection regime. This article reflects on the history of the development of digital identity systems, the legal framework around digital IDs as well as some ethical questions regarding access to personal information by states and corporations. It also examines the development of new international standards, cyber security issues and the importance of establishing strong accountability frameworks to help make digital identity governance transparent, inclusive, rights-centric and constitutionally sound in the digital era.

**Keywords:** Digital Identity, Aadhaar, Privacy Rights, Data Protection, Identity Governance

### 1. Introduction

Historically, the concept of identity has been associated with physical documents issued by a sovereign authority to provide recognition, access to public services and verification of citizenship. States imposed administrative control and provided legal recognition to persons through traditional identity mechanisms – birth certificates, passports, ration cards and voter ID cards. Due to globalization, digital governance, quick technological progress and the growing reliance on online transactions, however, the concept of identity has turned into a technologically enabled system dubbed digital identity. Digital identity is electronic data which is stored to verify and identify people in digital platforms and governance systems. It has become a crucial tool for the delivery of welfare services, financial inclusion, health care benefits, access to education, taxation systems, and online authentication methods that are more efficient by governments and private institutions.

The adoption of digital identity systems for identification from traditional systems has picked up pace with the increase in e-governance programs around the world. Governments realised digital technologies could help to ease administrative burdens, to stop duplication and increase the effectiveness of welfare delivery systems. The capacity of states to develop centralized identity databases further increased with the use of biometric technologies, including fingerprints, iris scans, facial recognition and artificial intelligence. Estonia was one of the first countries to adopt sophisticated digital governance systems, incorporating digital identity systems into

nearly all facets of public life—such as the processing of taxes, voter registration and voting, and plans for accessing healthcare. Likewise, the European Union has created the idea of interoperable digital identity frameworks to enable the secure processing of digital transactions between the EU member states.

Aadhaar was a revolutionary change in the identity governance system in India. Aadhaar was launched in 2009 by the Unique Identification Authority of India (UIDAI) to issue a unique 12-digit identifier to all residents that would be based on biometric and demographic information. The main objective of the system is to prevent ID fraud, cut leakages in welfare programs, and enable direct cash transfers. Aadhaar quickly grew the world's largest biometric identity system with millions of people in its database. The linking of Aadhaar to banking, telecom, welfare schemes, tax and digital payments profoundly changed the digital governance landscape in the country. The system helped in financial inclusion by providing banking facilities and government subsidy to the disadvantaged population based on biometric authentication.

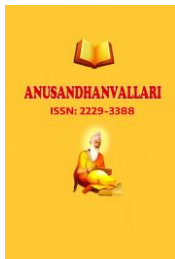
Although the digital identity initiatives had many administrative benefits, they also raised complex legal and ethical issues. The centralisation of both collection and storage of biometric data posed privacy-related risks of violation of privacy, unauthorised surveillance and data breaches. As the use of digital authentication grew, concerns were raised about vulnerable populations that were not able to access technology or about whose biometric authentication failed. However, in some cases, people were not able to access welfare services because of authentication issues or technical issues, highlighting the fragility of over depending on digital identity systems for providing welfare services.

On a global scale, the concept of digital identity governance has shifted towards more transnational systems and frameworks, as well as interoperability. Digital identity initiatives are advocated as a means of policy achieving financial inclusion and sustainable development objectives, by international organizations including the World Bank and the United Nations. There is now a level of interest in cross-border digital identity frameworks, to support international trade, international migration control, digital banking and online trading. Private digital identity authentication systems embedded in social media, financial applications and digital wallets are also developed by technological corporations to join the digital identity ecosystem. The merging of state and corporate identity systems has undermined the public governance-commercial surveillance divide. This mingling of state and corporate identity systems has created a 'blurring' of the public governance-commercial surveillance divide.

## 2. Constitutional provisions related to digital identity in India

With the rollout of Aadhaar and digital governance it has undergone tremendous change in the legal and constitutional context in India. While the Indian Constitution does not explicitly mention digital identity or informational privacy, it offers a foundational basis for regulating the state's actions with regard to personal data, identity management, and technological governance through constitutional guarantees under Part III. The concept of individual dignity, equality, liberty and privacy in the digital age is provided by the combined effect of three constitutional articles – 14, 19 and 21. The judiciary has been pivotal in shaping the meaning of these constitutional provisions in response to the new challenges that have arisen with digital identity systems.

Statutory status to Aadhaar based identity governance in India was given with the enforcement of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. The act was meant to simplify the welfare delivery process by connecting pay-outs and benefits to the biometric authentication process. The Act mandated the Unique Identification Authority of India to gather the biometric and demographic data of the citizens of India and also to issue unique identification number for their authentication. The government explained the law based on the reasons of administrative efficiency and less corruption and more inclusive governance.



But linking Aadhaar to the banking services, mobile, tax and welfare schemes has raised constitutional doubts on privacy, surveillance and overreach of the state. The historic ruling in Justice K.S. Puttaswamy vs the Union of India had a profound impact on the legal debate on digital identity governance in India. In 2017, the Supreme Court in a unanimous verdict, held that the right to privacy is a fundamental right under the Constitution and is inherent in the other fundamental rights. The Court recognized informational autonomy, bodily integrity and the right of individuals to limit dissemination of information as aspects of privacy. This was an important ruling in the digital rights jurisprudence in India.

In turn, in 2018, the Supreme Court heard the constitutionality of the Aadhaar Act in the Aadhaar judgment. The Court confirmed that Aadhaar was constitutionally valid for welfare purposes and set guidelines on how Aadhaar could not be compulsorily linked. It also held that there should be statutory provisions to make Aadhaar compulsory for private sector entities like banks and telecom companies. The Court stressed the need for collection and use of the biometric information to meet the requirements of legality, necessity and proportionality. The judgment tried to strike a balance between the interests of the state in running welfare effectively and the rights of individuals with privacy rights.

With the introduction of data protection laws, India's legal framework for digital identity systems was further bolstered. Concerns about data breaches, the unauthorized use of personal data for profiling or surveillance required a thorough legal approach to the processing of personal data. India later passed personal data protection laws to govern the collection, storage, processing and transfer of personal data. These legal developments are a response to the growing awareness of the need for strong protections of digital identity systems to steer clear of misuse and hold accountable those who use them.

Another important question is on the matter of digital exclusion. While Aadhaar was meant to be a means to inclusive governance, its implementation has resulted in technology issues and authentication errors that have denied welfare benefits to the vulnerable at times. Some people, especially elderly, manual workers and people living in remote areas usually fail to get biometric authentication because of a worn fingerprint, lack of connectivity or technical issues. This exclusion is a matter of concern as far as the right to life and the right to dignity, guaranteed under Article 21 of the Constitution is concerned.

The constitutional and legal framework of digital identity in India is thus a process of negotiation between technology and democratic accountability and human rights safeguards. The judiciary, legislature and executive remain influential in establishing the boundaries of digital governance that are developing in the face of emerging tech realities. The legal protection frameworks, independent monitoring, and rights-centred regulatory regimes are becoming increasingly important in the context of strengthening legal protections, increasing the scope of DPPII, and implementing AI-based governance in India.

### **3. Privacy, Surveillance and Data Protection Issues in Digital Identity Governance**

Digital identity systems have completely changed the nature of the relationship between people and the state by allowing for the utilization of a massive amount of personal data to be gathered, stored and processed. Being able to manage welfare distribution more efficiently and easily with digital identities is important to administrative effectiveness, but also raises significant privacy, surveillance and data protection concerns. Having this information in centralized databases raises the risk of misuse, unauthorised access, profiling and intrusive monitoring by state and private actors. Governmental and corporate use of digital identity infrastructures in governance and commerce has made the protection of informational privacy a major challenge in the digital era.

Private is an integral aspect of human dignity and autonomy. The expectation of privacy in democratic societies is that personal information in relation to a person's identity, finances, health, communications and movements will not be arbitrarily accessed or misused. Digital identity systems, on the other hand, require a lot of critical data

like fingerprints, iris scans, facial data, location data, etc., as well as behavioral patterns. These data can be integrated across platforms, allowing to generate complete digital profiles that show very personal details about a person's life. These practices of profiling cause concerns about information self-determination and personal autonomy.

This constitutional protection of privacy as a fundamental right in India had a great impact on the discussion of digital identity governance. Informational privacy was recognized as a part of personal liberty in the context of Article 21 of the Constitution by the Supreme Court in the case of Justice K.S. Puttaswamy vs Union of India. The judgment highlighted that any interference with personal information by the State has to meet with the constitutional standards of legality, necessity, proportionality and procedure. Still, the use of digital identity systems has sparked controversies over privacy issues.

Mass surveillance is one of the main issues of concern regarding digital identity governance. Governments can track people's movements and transactions across various industries, such as banking, telecom, healthcare, travel, education and taxation, thanks to the centralized digital identity databases. By combining identity systems with other technologies like facial recognition cameras, AI and predictive analytics, states become equipped with unprecedented powers to monitor their citizens' activities and movements. Such powers can be used to create a culture of governance based on surveillance. Ontop over-surveillance can create an environment that can impede the ability to express oneself freely, participate in politics, and dissent, which in turn can help to weaken constitutional freedoms.

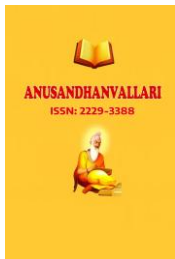
The greater role played by private companies in digital identities' ecosystems further complicates privacy protection. The processing of identity related data for purposes of business is a common occurrence in technology companies, financial institutions and online platforms. Profiling of the users is a crucial part of data-driven business models for targeting ads, shaping consumer actions and forecasting their preferences. People are often unaware of how much data they are giving away, how it is being used, or how it is being monetized. Digital platforms generally lack meaningful consent mechanisms due to the absence of meaningful choice or understanding of what is being processed by the data.

Another big hurdle in the digital identity governance landscape is data breaches. Biometric and demographic data in large quantities is an appealing source for cyber criminals. Access to any identity database may lead to identity theft, financial fraud, blackmail and other cyber crime. Biometric info is not easily changed after it is compromised and unlike passwords or identification cards. With biometric identifiers being permanent, this often adds to the ramifications of data breaches. The leakages of Aadhaar-related information came from various sources, raising concerns about the security of Indian's digital identity system.

International data transfers are more complicated. Digital identity systems are more and more found in an international digital life that includes cloud computing, worldwide service providers and multinational tech corporations. Personal data can be collected and processed in various geographical regions and have varying laws and enforcement policies. Lack of harmonised international laws and standards results in uncertainty about accountability, jurisdiction and remedies for those affected. Issues of data localization and sovereignty and international co-operation have thus come to the fore in today's digital governance discussions.

#### **4. Ethical issues in biometric identification and AI-based identity systems**

In the era of increasing dependency on biometric identification and artificial intelligence (AI) based identity systems, there are complex moral issues to consider regarding the notion of autonomy, dignity, equality and technological accountability. Biometric technologies are based on a unique physiological or behavioral characteristic of a person, like their fingerprint, iris scan, face, voice or gait. AI adds to these systems by facilitating automated analysis, predictive profiling and identification, in both digital and physical environments. While these



technologies offer the promise of efficiency and security, their general usage brings up critical questions of ethics that confront the norms of democratic governance and the securing of human rights.

The most prominent ethical issue is that of consent and autonomy of the body. Biometric data is unique in that it is associated with a person's physical identity and is fundamentally different from other personal information. Biometric characteristics can't be easily altered or changed as in the case of a password or identity card. The requirement to collect biometric data is, therefore, subject to scrutiny of how much real choice do people have to opt out of digital identity systems? In many instances, biometric authentication is a condition for access to welfare benefits, financial services, employment opportunities or to public services, de facto forcing people to hand over a sensitive piece of personal information. These practices could be counter to the ethical standard of informed and voluntary consent.

Ethics also play a prominent role in the discussions about biometric governance. With the aid of AI, facial recognition technology can monitor a wide variety of public environments, including transportation systems, educational facilities, offices, and businesses. Governments and private entities are capable of monitoring people's movements, interactions and behavior without them knowing. This can have psychological impacts that can hinder freedom of expression, assembly, and political participation. People who are monitored all the time can change their behaviour as they are scared of being monitored, which will impact on their personal liberty and democratic engagement.

Another significant ethical issue with AI systems is bias and discrimination. Bias and discrimination in AI systems is also a big ethical problem. AI-based identity systems are based on algorithms trained on massive amounts of data that can include past inequalities, or bias, in society. For instance, facial recognition systems have been found to misidentify racial minorities, women and minorities. These inaccuracies can lead to misidentification, denial of services, welfare program benefits, and discriminatory practices. When automated systems affect the decision-making process in areas such as law enforcement, immigration, employment, and access to basic services, ethical issues come to the fore.

There are additional moral issues about proportionality and misuse of power with regard to the use of biometric identification in law enforcement. The use of predictive policing and artificial intelligence-based surveillance systems can lead to inequities regarding who is targeted and who is not. Predictive policing and AI-based surveillance systems, which can be based on patterns from historical data, may unfairly target vulnerable communities. The use of automated identification technologies to the extent that it removes the presumption of innocence and raises the risk of arbitrary state action is problematic. The opacity of algorithmic decision-making also makes it difficult to hold algorithms accountable as people affected by the algorithm often don't have the capacity to understand or challenge the decision made by the algorithm.

The digital exclusion and inequality is another major ethical problem. Digital identity systems often are touted as tools for inclusion, but they can effectively exclude populations unable to access the internet, unable to master the technological systems, or not have biometric authentication systems. Many elderly people, people with disabilities, people doing manual work, rural people, and economically depressed people have problems accessing digital platforms and/or biometric verification processes. Not being recognized by digital identity systems can therefore lead to exclusion from welfare or healthcare services, from banking services or from education. Ethical governance must involve making sure that technological systems do not widen the gap in social inequalities.

Ethical concerns of commercial exploitation of the biometric data also arise. The private sector is gathering biometric data via social media, smartphone apps, wearables and online services more and more. This information can be often used for targeted advertising, consumer profiling, behavior prediction and business analytics. People might not be fully aware of what happens with their biometric data – how it is processed, stored or shared with

third parties. Personal attributes related to identity are turned into economic resources, which poses issues about who owns the data, who benefits from its exploitation and who exercises control over it.

### **5. Comparative International Approaches to Digital Identity Regulation and Governance**

Countries have adopted various strategies to manage digital identity systems because of their constitutional histories, technological capabilities, governance systems and human rights undertakings. Comparative analysis of the different approaches adopted to the digital identity in different countries has led to the conclusions that, although many Governments want to take advantage of digital technologies in their efficient administration and for the economic development of their countries, they differ considerably in balancing innovation with privacy, security and civil liberties. A comparison of these international perspectives offers insights for the legal and ethical aspects of identity governance in the digital world.

One of the most rights-oriented ways to regulate digital identity is that of the European Union. Principles of privacy, data protection and the right to self-determination in information are strongly featured in the regulatory framework of the EU. The General Data Protection Regulation (GDPR) is a detailed regulation that outlines the safeguards to be implemented for the collection, processing and transfer of personal data. Personal data protection is a fundamental right under GDPR, and GDPR has specific requirements on consent, purpose limitation, data minimization, transparency and accountability. They have enforceable rights over their own information, to access, correct, delete and pass on their own personal information. Strict fines for breach of privacy help to ensure organizations implement strong privacy measures.

EU has also adopted the eIDAS framework, which aims to enable electronic identification and trust services to be used with security across the borders of the member states. The eIDAS system supports interoperability of the national identity systems, and meets the standards of privacy and cybersecurity. The EU's decision-making process focuses on decentralisation, user consent and robust regulatory safeguards, which align with the EU's emphasis on the protection of human rights and digital innovation.

Estonia is considered one of the world's leaders in digital identity governance. It's a highly developed digital ecosystem in which citizens are able to use their secure digital identities to access healthcare, taxation, banking, voting, education, and business services. Estonia's model is based on decentralized architecture, security mechanisms based on blockchain and transparent governance. Citizens have significant control over their personal information and can track who accesses their personal information. The Estonian system illustrates the importance of building trust in the public and efficient governance with the use of digital identities while using strong legal protection and cybersecurity system.

By contrast, the Chinese system of digital identity governance is more centralized and based on surveillance. Digital identities are broadly used by the Chinese state in conjunction with facial recognition systems, AI and social credit platforms, as well as mass surveillance. Digital identity infrastructures can not only be used for administrative purposes, but also for surveillance of public behaviour and to assure state control. The Chinese model has been technologically integrated and managed efficiently, but has received international condemnation for infringing privacy rights, the absence of transparency, and the restriction of civil liberties. The Chinese case is an example of the potential use of digital identity systems as tools of surveillance and political control if there is insufficient legal protection.

Digital identity governance in the USA is multifaceted and piecemeal. The United States does not have a single federal data protection law that applies to the entire economy. The United States does not have a single national comprehensive data protection law which applies to the economy equally. Rather, privacy laws are scattered throughout different statutes that are relevant to protecting privacy in healthcare, financial, consumer protection, and internet communication. Private companies and market-based processes are the drivers of digital identity



verification to a large extent. Technology firms have a big part to play in identity authentication, data analytics and platform governance. While innovation is a hallmark of the U.S. digital economy, data commercialization, privacy concerns and corporate power are the areas of contention.

India's model lies somewhere in between the welfare-oriented governance and the centralized digital governance. Aadhaar has facilitated financial inclusion and direct benefit transfers to a large scale, but has also sparked concerns on the issues of surveillance, privacy and exclusion. Judicial rulings have played a major role in shaping constitutional rights in India's digital identity system by affirming the rights of privacy as a fundamental right. But issues of enforcement of data protection, institutional oversight and technologized exclusion persist and remain a threat to the legitimacy of the system.

## **6. Cybersecurity, Accountability and the future of rights-based digital identity systems**

Nowadays, a cybersecurity and accountability aspect is an essential part of digital identity governance. Governments and private organizations are increasingly turning to digital identity infrastructures to validate identities, to deliver services, and to govern people, giving digital data about identity a huge legal, economic and social importance for its security. Highly sensitive details such as biometric information, demographic data, financial information and behavioural data are included within digital identity systems. Unauthorized disclosure of these information can lead to identity theft, financial frauds, cybercrime, surveillance and large-scale invasion of privacy. The success of digital identity governance in the future will therefore largely rely on how well the states and institutions are able to implement strong cybersecurity and accountability mechanisms.

As technology has advanced and digitization has become more prevalent, there have been rapid developments of cybersecurity threats ubiquitous in digital identity systems. Centralised databases with biometric data are high-profile targets of hackers, cybercriminal groups and malicious actors. Millions of users could be impacted by a data breach in which digital identity systems are involved. Biometric identifiers like fingers and Iris scans can't be easily changed once they are exposed unlike passwords or physical identification documents. Hence, there are long term risks to those whose data is compromised in a breach. Cybersecurity failures can also lead to loss of trust in digital governance systems, and lower interest in digital economies participation.

The major challenge is related to the lack of technology protections in the digital ID infrastructures. Inadequate data encryption, limited access rights, outdated software systems and data sharing practices make systems more vulnerable to cyber attacks. As the number of countries rolling out digital identity programs grows, there are many that do not have enough cybersecurity experience, infrastructure, and institutional capacity to build effective cybersecurity for large-scale databases. All developed countries are at risk of high-tech attacks against their public institutions and critical digital infrastructure.

New technologies, notably AI and cloud computing, have added to the cybersecurity governance complexity. New and evolving threats to digital authentication include AI-powered cyber attacks, deepfakes, automated phishing scams, and identity spoofing. At the same time, there are concerns about jurisdiction, cross-border transfers of identity-related information and responsibility of the multinationals in charge of the technology. Governance for cybersecurity needs to be constantly evolving to meet new challenges related to technology and the emergence of new threats and vulnerabilities.

Another crucial aspect of digital identity governance is accountability. Accountability mechanisms need to be explicit about institutional accountability, have independent oversight bodies, be transparent and have grievance redressal procedures that are transparent. Those who have been wrongly denied services, had their personal data breached or misused should have effective legal remedies. If there is no accountability in digital identity systems they can be subject to excessive power and limited democratic control.

Independent regulatory bodies are an important component in holding to account and maintaining public confidence. Authorities such as data protection authorities and cyber security agencies should have the necessary powers to investigate breaches of these systems, impose penalties on these violations, monitor compliance and audit the systems of digital identity. It is also vital to be transparent about the data, how it's processed, and how decisions are made using algorithms. Governments and private organisations should explain its use, sharing and storage of personal information. Algorithmic systems which impact on public rights should be explainable and independently subject to review.

Other key accountability features relate to corporate responsibility on digital identity ecosystems. Private companies are becoming more and more involved in authentication processes, cloud storage and services, biometric analytics, and development of artificial intelligence. Such corporations can have a significant influence on the processes of digital governance. Thus, the regulatory frameworks should include requirements on privacy protection, cybersecurity requirements, ethical requirements in the use of AI, and the responsible handling of data. The accountability of corporations is crucial as they might be tempted to gather too much data, to profile users.

Newly emerged approaches to digital identity governance increasingly focus on rights-based and human-centric approaches. Rights-based governance aims to ensure that digital identity systems are based on constitutional values, democratic principles and are consistent with the international human rights standards. Such systems focus on individual freedom and autonomy, informed consent, transparency, accessibility and non-discrimination. The focus is more on making the operation of technological systems in line with human dignity and social justice rather than improving administrative efficiency.

Decentralized identity models or self-sovereign identity systems are starting paths of development in the rights-based governance. The goal of these systems is to give more control over their identity credentials to individuals and their personal information. By leveraging blockchain technologies and decentralized architectures, reliance on centralized databases can be mitigated and there is a possibility of greatly decreasing surveillance risks. But these systems must also be legally recognized, interoperable and accountability frameworks must be put in place to ensure the effective implementation of these systems.

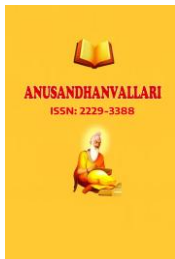
## 7. Conclusion

Digital identity systems are one of the most radical changes in current governance, changing the dynamics between states, private institutions and individual citizens. The governance and management of identity is now widely embedded in welfare administration, financial inclusion, healthcare access, digital commerce and cybersecurity mechanisms, ranging from Aadhaar to the development of international digital identity frameworks. Expansion of biometric technologies, artificial intelligence and centralized databases have yielded benefits in terms of increasing efficiency and improving public services. Comes also huge questions about accountability, data security, exclusion, discrimination, surveillance, and privacy in the context of these technological advances.

The recognition of privacy as a fundamental right in the constitution has been a key element in the digital identity jurisprudence, especially in India. There is a strong focus on the necessity of technological governance within the confines of the constitutional framework, and with respect to individual autonomy, dignity and informational self-determination. The experience gained in other countries also illustrates the importance of robust legal protections, clear regulatory structures, cybersecurity measures, and autonomous regulators for effective digital identity governance.

Risks of unchecked surveillance, algorithmic bias, and power centralization are raised by the ethical dilemmas of biometric identification and AI-driven systems. The ethical issues of biometric identification and AI-driven systems raise concerns about unchecked surveillance, algorithmic bias, and excessive concentration of power. Likewise, the threats of cyber security and data breaches highlight the importance of strong technological security





measures and sanctions. The new trend of digital identities that go beyond the national border will require international cooperation and standardisation to safeguard human rights in the digital world.

The future of digital identity governance should be shaped by a democratic and rights-based approach to innovation while keeping constitutional principles and values in mind, with a strong focus on democratic accountability. Technological progress should not lead to restriction of civil liberties, but technological systems for digital identity should be developed in a way that ensures inclusion, transparency, security and respect for basic rights.

### References

- [1] Dixon, P. (2017). A failure to “do no harm” – India’s Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. *Health and Technology*, 7(4), 539–567. <https://doi.org/10.1007/s12553-017-0202-6>
- [2] Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. *Government Information Quarterly*, 37(2), 101442. <https://doi.org/10.1016/j.giq.2019.101442>
- [3] Ramanathan, U. (2014). *Biometrics use for social protection programmes in India: Risking exclusion?* Oxford University Press.
- [4] Jayal, N. G. (2013). *Citizenship and its discontents: An Indian history*. Harvard University Press.
- [5] Khera, R. (Ed.). (2019). *Dissent on Aadhaar: Big data meets big brother*. Orient BlackSwan.
- [6] World Bank. (2019). *ID4D practitioner’s guide: Version 1.0*. World Bank ID4D
- [7] Access Now. (2019). *National digital identity programmes: What’s next?* Access Now
- [8] Ngullie, O. G. (2025). *The social and ethical implications of Aadhaar in India’s digital governance*. Institute for Social and Economic Change Working Paper No. 610.
- [9] Karmwar, M., & Kunwar, D. (2025). *The dilemma between digital identity and privacy in modern governance: Comparing South Africa and India*. *Indian Journal of Public Administration*, 61(3). <https://doi.org/10.1177/00219096251352368>
- [10] Felt, C. (2025). *Exploring the global digital ID landscape*. Atlantic Council.
- [11] Sullivan, C. (2011). *Digital identity: An emergent legal concept*. University of Adelaide Press.
- [12] United Nations Development Programme (UNDP). (2021). *Legal identity for inclusive development: Principles and practice*. UNDP Digital Identity Report