Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

E-Governance and Digital Exclusion: Legal Barriers in Ensuring Equal Access

Rakshita Adchitre[a] Aanya Agrawal[b]

[a]Symbiosis Law School, Pune, India [b]National Law University Bhopal, India

Received 28 February 2025; *Accepted* 28 March 2025; *Published* 31 March 2025

E-governance in the 21st century has become a boon for the government. With its revolutionary ability, it has made governance, administration, social work, and jurisdiction easier, but there are some cons of e-governance as well. People who are unaware of this digital world and those who don't know how to fully use this technology somehow fail to keep up with the current world. Even though e-governance has helped people to access public services effortlessly, there are still some people who don't even know what the internet is and what the benefits of the same are. Data of this stratum of the public never gets registered, thus resulting in systematic exclusion and a digital divide in society. Lack of education, gender inequality, and socio-economic disparities are the major reasons for this issue. Thus, this article tries to explore the cons of e-governance and examines loopholes in the existing legal frameworks. It has tried to explore various factors that are responsible for this digital divide and tried to provide insights into the same.

Keywords: *e-governance, digital divide, digital exclusion, cybersecurity, government, data, aadhar.*

INTRODUCTION

With the advent of technology, governance has also become easier. E-governance refers to the digitalisation of various government activities such as Aadhar verification, E-courts, procurements, etc.[1] With the launch of the Digital India Flagship Programme in 2015, the motive of the Government is to make India digitalised so that every person would be able to make the best use of the technology[2]. Even though the Government is trying to include every citizen under the ambit of E-governance, there are still some communities left behind that are deprived of such benefits for many reasons. The aforementioned inability of people refers to Digital Exclusion[3].

In the context of e-governance, exclusion occurs when people are unable to:

1. Register for digital identity systems (e.g., Aadhaar in India).

2. Accessing online legal and administrative services.

3. Receive government benefits due to technical errors or authentication failures.

The ascent of e-governance has metamorphosed public service delivery by digitising key governmental functions such as identity verification, social welfare distribution, and legal documentation. Though digital transformation proclaims capability, it threatens the reality of excluding the marginalised section of society, deprived of access to the digital infrastructure and unaware of making use of the same. These problems raise questions related to superior socio-legal issues that include access to justice, rights on the internet, and the role of the state towards egalitarian governance.

Through this research article, we will dive into the issue of Digital Exclusion through the lens of judicial architecture and plausible solutions for the same, as it eventually poses an inquiry into the plethora of existing socio-legal rights of the citizens.

---

[1] 'Digital Exclusion' *(Cedefop)* <https://www.cedefop.europa.eu/en/tools/vet-glossary/glossary/digitale-uitsluiting> accessed 11 February 2025
[2] *Ibid*
[3] *Ibid*

UNDERSTANDING DIGITAL EXCLUSION IN E-GOVERNANCE

Digital Exclusion can be understood through the concept of the Digital Divide. Digital Divide occurs when there exists a gap between the marginalised sections of society and digital technologies due to a lack of knowledge about them. People who lack education or digital knowledge somehow get left behind in making full use of E-Governance[4]. Due to this Digital Divide or exclusion, most of the time the Government fails to reach the needy section of the society, who are the targeted beneficiaries for the same. There are many reasons responsible for this Digital Exclusion, such as poverty, disability, geography, etc.

The Third Annual Report by the Centre for Equity Studies in New Delhi, India, Exclusion Report (IXR) 2016,[5] provides data regarding the exclusion of people from accessing various public goods and services. According to this report, marginalised people such as Dalits, slum dwellers, and women have lower access to healthcare or digital facilities due to the lack of education, which is leading to exacerbating social inequalities and social exclusion. Many workers and students are unable to make full use of digital technology at this time. An average daily wage earner has to spend his entire daily wage just to get his Aadhar or ID card printed digitally because accessing the internet through cybercafes is a highly cost-demanding effort.[6]

According to the IAMAI Survey done by the Internet and Mobile Association of India[7] in 2015, rural internet users only account for up to 28% of the total internet users, whereas their population accounts for up to 70% of the country's total population. This explains the extreme side of Digital Exclusion, which has existed in our country. The survey highlighted issues such as the lack of availability of digital devices, the lack of digital literacy, and gender inequality are key issues for Digital Exclusion.

Literacy is another such barrier for this Digital Divide. According to the census done in 2011[8], the literacy rate of India is 74.04% which is comparatively less, which means in total 25.96% of

[4] Rahul Awati and Katie Terrell Hanna, 'What is the digital divide?' (*Tech Target*) <https://www.techtarget.com/whatis/definition/digital-divide> accessed 11 February 2025
[5] Centre for Equity Studies, *India Exclusion Report 2016* (2016)
[6] Digital Empowerment Foundation, *India Exclusion Report: Digital Exclusion Chapter* (2017)
[7] Internet and Mobile Association of India, *Mobile Internet Report* (2015)
[8] *Ibid*

the total population is illiterate. People are not aware of the latest technological advancements. Due to this illiteracy, they are lagging in Digital Inclusion.

The latest research done in this area was the NITI Aayog's Report for a Digitally Inclusive Bharat,[9] done in 2021. This report highlights the stark difference existing between urban and rural areas in terms of Digital inclusion, where in rural areas only 22% of the population own smartphones as compared to 68% in urban households[10].

LEGAL CHALLENGES AND BARRIERS

Several legal issues emerge in the implementation of e-governance systems:

Right to Equality and Non-Discrimination: Digital exclusion violates the principle of the Right to equality because it leads to a huge digital divide in society, where every person stands unequal in accessing Digital benefits. The right to equality is enshrined in Article 14 of the Indian Constitution[11] and violation of this right has serious consequences for the same. This inability of people to access equal opportunities, only because they lack the necessary resources, results in the violation of their Right to Equality. Whereas in the case *Justice K.S. Puttaswamy (Retd.) v Union of India*[12], it was held that the Right to Privacy is a fundamental right, but this judgment has become a menace to the idea of the Right to Privacy because those people who have access to digital devices, but due to lack of digital awareness and lack of education, do not know how to use them efficiently, have had to face a barrier to safeguard their rights. It has created a situation of social stratification where marginalised sections of society are eventually left behind. Through this judgment, the court has raised concerns regarding the rule of mandatory Aadhaar for accessing various digital schemes, such as Pradhan Mantri Jan Arogya Yojana, MGNREGA, etc. Cases such as this Aadhaar judgment raised concerns about mandatory digital identity violating privacy and exclusionary effects.

---

[9] 'NITI Aayog's Report for a Digitally Inclusive Bharat' (*Drishti IAS*, 11 May 2001) <https://www.drishtiias.com/daily-updates/daily-news-analysis/niti-aayog-s-report-for-a-digitally-inclusive-bharat/> accessed 11 February 2025

[10] *Ibid*

[11] Constitution of India 1950, art 14

[12] *Justice K.S. Puttaswamy (Retd.) and Anr v Union of India and Ors* (2017) 10 SCC 1

A similar concern was raised in the case of *Ravi Sharma v Union of India (2020),* in which many underprivileged students were not able to make full use of online education because of a lack of technological means. Poor internet infrastructure is also a major setback, resulting in an increasing barrier to the digital divide.

According to the IAMAI-Kantar report (2022)[13], active internet users in rural areas account for only 31% of the total population, whereas the Government has failed to provide any alternate non-digital ways for people to avail of digital facilities.

According to the World Development Report 2016: Digital Dividends,[14] people belonging to the lower strata of the economy are not able to use healthcare services efficiently because of the compulsory digital verification. Such digital identity programs disproportionately affect rural populations, elderly citizens, and economically weaker sections, leading to potential violations of fundamental rights. India needs to convert its offline audience into online to push growth, profit, and generate jobs.[15] Even though India ranks among the top five countries in terms of the total number of internet users, it remains behind at 18% as compared to the US.[16]

Due to poor Digital Laws in India, cyberattacks have also become a common threat. Many large-scale digital identifications hold sensitive data of citizens, making them an easy target of digital attacks. For example, there were cases of Aadhaar leaks in India, in which the personal data of citizens was leaked. This poses a greater threat to the privacy rights of vulnerable sections of society.

Due Process and Denial of Services: To enhance the delivery of services through e-governance systems, the government depends mainly on digital identity verification, particularly biometric authentication. Problems in these systems have resulted in the denial of services. At times, individuals are deprived of food rations, pensions, and medical attention because of identification problems, such as fingerprint non-matching, and technical errors. Another issue

[13] IAMAI-Kantar, *Internet in India Report* (2022)
[14] World Bank, *World Development Report* (2016)
[15] Digital Empowerment Foundation, *India Exclusion Report: Digital Exclusion* (2017)
[16] *Ibid*

is generated as a result of the lack of well-defined legal measures and redressal of grievances, thereby excluding weaker sections from availing of fundamental rights.

The Indian experience with Aadhaar-linked benefit packages has exposed the pitfalls of obligatory biometric authentication. According to reports, individuals, notably the elderly and manual labourers, were unable to get food handouts owing to problems in fingerprint authentication. In Justice K.S. Puttaswamy v Union of India (2017),[17] the Supreme Court declared that Aadhaar could not be made mandatory for welfare benefits, finding that denial of service due to technological problems infringed fundamental rights. However, Aadhaar verification remains a barrier for many people, demonstrating a disconnect between legal orders and implementation.[18]

Cybersecurity and Data Protection: The growing use of identification systems by e-governance heightens cybersecurity and privacy issues. Biometric details, financial data, and health information, which are sensitive, are retained in government databases in gigantic amounts, making them the main targets for hackers. Illegal entry to these databases is extremely problematic, insofar as identity theft, money laundering and bulk surveillance, if practised, will inevitably lead to human rights violations.

The weakness of large digital identification systems has been brought to the fore by recent cyberattacks. Aadhaar data of over one billion Indians was discovered on the dark web in 2018, which put the security of national systems in question. The same has occurred with other digital governance initiatives around the world, which brings into focus the need for proper cybersecurity policies and enforcement mechanisms.

Many developing nations have significant difficulty in the absence of effective data privacy regulations to oversee the government's handling of personal data. While the European Union's General Data Protection Regulation (GDPR)[19] requires rigorous security requirements for public

[17] *Justice K.S. Puttaswamy (Retd.) and Anr. v Union of India and Ors* (2017) 10 SCC 1
[18] Jean Drèze et al., 'Aadhaar and Food Security in Jharkhand: Pain Without Gain?' (2017) 52(50) Economic & Political Weekly <https://www.epw.in/journal/2017/50/special-articles/aadhaar-and-food-security-jharkhand.html> accessed 11 February 2025
[19] General Data Protection Regulation 2016

sector data collecting, many countries do not have such safeguards. India implemented the Digital Personal Data Protection Act, 2023 (DPDPA)[20].

To regulate data processing and collection based on individual consent, purpose limitation, and the responsibility of data fiduciaries. Enactment of the legislation also generated fears over the obscurity of delegated legislation. There have also been concerns about individuals' lack of capability to assert their rights since the Act focuses more on data protection than privacy, and might leave loopholes in the surveillance methods of the government.

One of the root issues of cybersecurity in e-governance is the lack of compliance standards compared to actual data protection practices.[21] Many corporations and government organisations participate in data hoarding, which is the practice of gathering more information than is necessary. Businesses harvest enormous amounts of personal information in the name of KYC (Know Your Customer) policies, often neglecting to implement adequate security procedures to protect it. The absence of stringent access controls exacerbates threats by allowing sensitive information to be abused internally within firms.[22]

There are also fears about the monetisation of individual data, where platforms and companies make profits from user information without clear approval. If you are not paying for the product, you are the product, a term that has come into use in the digital economy to describe how companies harvest user data to generate profits. This requires more robust regulatory systems and independent oversight agencies to keep illicit data sharing at bay. As information is becoming the most valuable digital commodity, the consequences of poor data protection laws will only increase.

WAY FORWARD: A LEGAL FRAMEWORK FOR INCLUSIVE E-GOVERNANCE

Digital Inclusion Policies: One of the biggest obstacles to inclusive e-governance is the digital divide, which happens when some sections of society do not have access to the means of

[20] Digital Personal Data Protection Act 2023
[21] Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32(2) Computer Law & Security Review <https://doi.org/10.1016/j.clsr.2016.02.006> accessed 11 February 2025
[22] *Ibid*

accessing the internet and the relevant technical expertise to use services offered online. The governments need to implement policies that guarantee mass connectivity, particularly in rural and economically backwards regions. Legal mandates should prioritise inexpensive internet access, subsidised digital devices, and public access points like community internet centres.

Beyond infrastructure, digital literacy initiatives must be legally required and integrated into the classroom curriculum and adult training programs. Many people, particularly the elderly and those from lower socioeconomic backgrounds, are unable to take advantage of e-governance because they lack appropriate knowledge of digital platforms. Laws should promote collaboration among the government, commercial sector, and civil society to develop organised digital literacy efforts that enable individuals to successfully interact with digital governance systems.

Biometric authentication, common in electronic identification systems, has proved to be a two-edged sword. Though biometric authentication is more convenient and secure, errors have led to the denial of vital services to individuals unjustly. A step must be taken through the law to ensure individuals are not deprived of government assistance by a technological malfunction or authentication malfunction. The concept of human oversight has to be incorporated into digital regulation guidelines, requiring alternative means of verification in the event of failures by biometric technology. Laws must also hold technology firms and government agencies accountable for digital authentication failures, providing affected parties with a chance to go to the courts of law.

Independent Regulatory Agencies: There should be an effective system of accountability so that digital rules do not violate core rights. Independent regulatory agencies need to be established to oversee the implementation of digital identity programs and deal with concerns of exclusion, data privacy, and denial of services.

These agencies need to be given the power to carry out audits, investigate complaints, and suggest remedial action. The legislation should clearly articulate the role of the regulatory bodies so that transparency in buying, holding, and using digital identities is ensured. Legal redress must be extended to citizens to challenge unfair exclusions, data loss, and misuse of

personal information. Public campaigns must also be initiated so that people are made aware of their digital governance rights as well as redressal mechanisms.

CONCLUSION

E-governance, though revolutionary, has to be inclusive, legally valid, and ethically executed. Making digital accessibility a legal right can bridge the digital divide and ensure equal access to justice and government services. A balanced strategy with technological progress and legal protection is essential to avoid digital exclusion in governance. There is a significant number of people who eventually get left behind due to this digital exclusion. If the government tries to incorporate this section of society under the ambit of digital inclusion, then our country can reach new heights where every person would be able to make full and efficient use of the technology.