



ISSN: 3107-4324 (Online)
Vol. 2, Issue No.1
November 2025

Inspired Impressions

A Multidisciplinary Journal of Adani International School



adani
international
school
Growing Together

Title: Digital Rights and Digital Privacy as Emerging Human Rights in India

Student's Name: Aahan Ritesh Prajapati

School: Adani International School, Ahmedabad

Grade: XI

Category: Senior

Title: Digital Rights and Digital Privacy as Emerging Human Rights In India

Abstract

The Internet has now become an integral part of our lives, profession and communication. Hence, digital rights are essential human rights to protect. Privacy, equitable internet access, and facial recognition ethics create significant legal and regulatory gaps in digital rights in India. Justice K.S. Puttaswamy v. Union of India (2017) established digital privacy as a fundamental right of the Indian Constitution under Article 21, protecting online privacy. Without a data protection law, citizens have experienced mass surveillance and breaches like the Aadhaar data revelation. The 2023 Digital Personal Data Protection Bill addresses these issues; however, it is criticized for giving government agencies significant exemptions and lacking clarity on user permission and data security. Education, freedom of expression, and information depend on internet connectivity, which is becoming a global right. India's National Digital Literacy Mission has not eliminated digital inequities, especially in rural and undeveloped areas with poor infrastructure, affordability, and digital skills. This research proposes making digital rights essential human rights in India. Strengthening the legislation framework, adopting the Internet as a digital right, and ethically regulating all technology will ensure that the digital revolution protects dignity, equality, and freedom.

Keywords

Surveillance, exemptions, affordability.

Introduction

Digital rights become fundamental human rights in today's digital world. They include Digital rights of access to the Internet, digital literacy, freedom to express on Digital platforms, data privacy, personal data protection, protection from online fraud and harassment, and ethical challenges due to AI and facial recognition technology: digital technology, especially the use of the Internet, has spread widely (“Digital Rights: Understanding Its Importance and Challenges in India - Testbook Blog”).

According to a report, by 2025, more than 300 million people will be using the Internet. On one side, digital technology proved a boon in healthcare banking agriculture, but it may also bring some challenges, such as data breaches, cybercrime, surveillance, and others. So, it becomes crucial to address these challenges, strengthen the legal framework, and make robust policies to protect digital rights (Sharma et al.).

Discussion

Digital rights:

Digital rights mean basic to advanced rights that people should have in this digital world. These include easy access to the Internet, freedom of expression online, data privacy, and ethical issues related to AI and facial recognition technology. In this article, we emphasize the challenges observed in implementing Digital rights and the need to fill the gaps in the legal framework for digital rights and privacy in India (“Digital Rights: Understanding Its Importance and Challenges in India - Testbook Blog”).



Challenges in Digital rights:

There are four main challenges to be addressed.

1. Digital privacy as a fundamental right

The Indian government has various laws, such as the right to freedom of speech and expression (Article 19), the Right to life and personal liberty (Article 21), the Right to education (Article 21A), the Digital personal data protection bill (2023), and the Information technology act (2000) (“Ministry of Electronics and Information Technology, Government of India | Home Page”). Justice KS Puttaswamy versus Union of India (2017) gave a benchmark judgement that included the right to privacy in Article 21 of the Constitution. Mass surveillance, data collection and data breaches faced by the people in India, do not fulfil Digital privacy (Khosla).

Mass surveillance and data collection:

The government of India and some private companies monitor the digital communication of people to identify terrorism for national security and to protect against crime. Information such as email, data, phone calls, data, social media interactions, and other online services are also gathered to identify crime (Shehu and Shehu). Mass surveillance also safeguards our privacy rights, which are fundamental rights of people by the Supreme Court of India under Article 21 of the Indian Constitution in Justice KS Puttaswamy vs Union of India (2017) (Khosla). It was also reported that technology giants like Facebook and Google exploit people's data for advertisement and personal benefits (Tungekar). The personal data protection bill, framed to protect personal and non-personal data of people and propose stringent penalties for breaches, is still pending in the Indian Parliament since 2019. India has strengthened digital personal data privacy by constituting the Digital Personal Data

Protection Bill 2023. However, it has been criticized for providing data to government agencies. (Tunggal)

Data breaches:

India has the second-highest number of data breach incidents. It includes other data leaks, credit card data and medical data breaches. State-owned utility organization leaked biometrics of Aadhaar card in 2018 (“Aadhaar Data Leak | Personal Data of 81.5 Crore Indians on Sale on Dark Web: Report”). The Indian Council of Medical Research (ICMR) lost 81.5 million COVID-19 testing records in 2023. The government of India passed the Digital Personal Data Protection Act in 2023, which has set rules and regulations for collecting, processing, storing and transferring Digital data. However, there is still a crucial need for robust data protection measures (“Data Breaches in India”).

2. Data literacy and equality in access to the Internet:

The United Nations has declared internet access a fundamental human right, interconnected with rights to education and freedom of expression (“Global Internet User Survey 2012”). The Indian government has taken initiatives, such as the national digital literacy mission, to increase the spread of the Internet to rural and underprivileged areas. However, still, 30% of people lack Internet access due to a lack of infrastructure, affordability, and lack of skilled people, especially in rural areas, resulting in inequalities in education, job, opportunities, and healthcare. Bharat Net policy (“BharatNet: Bridging the Digital Divide”), which was aimed at improving internet connectivity, has not been successfully implemented (Bajoria).

3. Frequent internet shut down:

The Internet has now become an integral part of our lives and businesses. A shutdown of the Internet would hinder healthcare, services, education, weather forecast services, and online jobs related to foreign investments (Shehu and Shehu). From 2014 to 2023, India experienced more than 780 Internet shutdowns, mainly for national security reasons and to prevent rumours and fake news. A shutdown of the Internet would also violate the right to access information and freedom of speech and expression (Article 19) (Johannes Thumfart).

4. Ethical challenges due to AI and facial recognition:

AI applications have transformed the world and brought a revolution in the healthcare and finance sectors, but it also raises ethical challenges. Its algorithmic bias, lack of transparency and mass surveillance capabilities exploit the digital rights of people. It utilizes automated facial recognition techniques, which may violate individuals, privacy and reveal identities (Huang et al.). Facial recognition technologies are known to miss and misidentify people, leading to wrong arrests and other discriminatory aspects and online harassment (The Upwork Team). AI systems should be inclusive, transparent, accountable, and free from buyers. The government must have definite protocols and regulations for AI use. The Information Technology Act 2000 has provisions for cyber security regulation but no clear guidelines for AI. Hence, implementing ethical regulations for AI technologies is important to protect digital rights (“Ministry of Electronics and Information Technology, Government of India | Home Page”).

Global policies and interventions in digital rights in India:

Digital rights are not as well defined in India as in other countries. However, the government of India is working hard to introduce regulations and protect rights, such as the Personal Data Protection Bill 2023. India’s participation in the G20 reflects its

commitment to regulate cyber security norms (Bajoria). European Union's act for digital rights, the General Data Protection Regulation (GDPR), sets a benchmark framework to protect digital rights by implementing user consent while processing data, also enabling them freedom of choice, inclusion, and promoting the equitable and sustainable Digital future. GDPR also includes strict penalties for non-compliance, ensuring robust personal data protection. Brazil's General Data Protection Law (LGPD) also gives priority to user rights (Valdívia). South Africa's Protection of Personal Information Act (POPIA) framed clear guidelines for data handling and data privacy. The United Nations Guidelines address internet access as a fundamental human right (Secure Privacy). By adopting these global best practices, India can reconsider the existing laws to reduce the gaps in its digital rights framework (GDPR).

Interventions recommended:

India should focus on key areas, such as strengthening the legal framework, making provisions for easy internet access, developing ethical guidelines for new technologies like artificial intelligence and face recognition technology, and adopting well-established global practices for addressing the challenges in digital rights.

1. Strengthening the legal frameworks

To protect digital rights and address the challenges posed by rapid technological advancements, a robust legal framework is essential, and so the Digital Personal Data Protection Bill (2023) should include provisions for user consent for data processing, data minimization, and accountability in alignment with GDPR (GDPR). Incorporation of strict penalties can minimize data breaches and online harassment. Specific regulations AI and facial recognition must be developed to handle the challenges like algorithmic bias, transparency and mass surveillance. The government can establish

an independent regulatory authority to check compliance with digital rights and digital data protection laws to work with transparency (Tunggal).

2. Providing easy access to the Internet

Providing internet services that are both dependable and economical should be the government's responsibility through programs such as Bharat Net ("BharatNet: Bridging the Digital Divide"). Internet services must be able to reach all members of the population, including those living in urban and rural areas of India. People can be educated and trained to work digitally through initiatives like the National Digital Literacy Mission (Johannes Thumfart).

3. Ensuring the Internet is a fundamental right

Internet access is a fundamental right as it is crucial for enabling education, healthcare, and job opportunities in the digital age ("Ashlesh Biradar v. State of West Bengal - Global Freedom of Expression"). Unless for exceptional emergencies, policy framing is necessary to restrict frequent internet shutdowns (Bhardwaj).

4. Promoting ethical technology use

We cannot imagine a situation where AI and facial recognition are not among the most advanced technologies. Because they are now a crucial component of the development of any nation, they must be used ethically (Huang et al.). Transparent artificial intelligence rules, the development of algorithms that are not biased, and auditing mechanisms that are fair are all equally necessary in order to prevent prejudice among groups. It is necessary to establish ethical rules for both the public and private sectors to facilitate progress while including human rights (Jauhar).

5. Adopting global practices:

India can strengthen digital human rights by taking guidance from global frameworks such as GDPR and forming ethical policies for AI and digital governance. By providing easy internet access, strengthening digital laws, and enhancing accountability in technology usage, India can create a digital ecosystem that is equal, accountable and safe for all citizens of India (Sarkar).

Conclusion

Digitalization has produced vast benefits in various sectors, like healthcare, national security, businesses and many more, but it has also introduced challenges that compromise individual freedoms and rights. In India, gaps in proper legal frameworks, frequent internet shutdowns, and the use of AI and facial recognition without proper regulations require urgent action. Digital privacy, freedom of expression, and the internet are the fundamental rights that are essential to ensure that all citizens can participate equitably in the digital revolution.

India can strengthen digital human rights by taking guidance from global frameworks such as GDPR and forming ethical policies for AI and digital governance. By providing easy internet access, strengthening digital laws, and enhancing accountability in technology usage, India can create a digital ecosystem that is equal, accountable and safe for all citizens of India.

Works Cited

- “Aadhaar Data Leak | Personal Data of 81.5 Crore Indians on Sale on Dark Web: Report.” *The Economic Times*, 31 Oct. 2023, economictimes.indiatimes.com/tech/technology/aadhaar-data-leak-personal-data-of-81-5-crore-indians-on-sale-on-dark-web-report/articleshow/104856898.cms?from=mdr.
- “Ashlesh Biradar v. State of West Bengal - Global Freedom of Expression.” *Global Freedom of Expression*, Nov. 2023, globalfreedomofexpression.columbia.edu/cases/ashlesh-biradar-v-state-of-west-bengal/.
- Bajoria, Jayshree. “India’s Digital Governance ‘Model’ Fails on Rights | Human Rights Watch.” *Human Rights Watch*, 6 Sept. 2023, www.hrw.org/news/2023/09/06/indias-digital-governance-model-fails-rights.
- “BharatNet: Bridging the Digital Divide.” *Pib.gov.in*, 2024, www.pib.gov.in/PressReleasePage.aspx?PRID=2086701.
- Bhardwaj, Shrutanjaya. “Rising Internet Shutdowns in India: A Legal Analysis.” *The Indian Journal of Law and Technology*, vol. 6, no. 1, 2020, pp. 122–57.
- “Data Breaches in India.” *Wikipedia*, 20 Sept. 2022, en.wikipedia.org/wiki/Data_breaches_in_India.
- “Digital Rights: Understanding Its Importance and Challenges in India - Testbook Blog.” *Testbook*, 2023, testbook.com/articles/digital-rights. Accessed 8 Jan. 2025.
- GDPR. “Personal Data | General Data Protection Regulation (GDPR).” *General Data Protection Regulation (GDPR)*, 2018, gdpr-info.eu/issues/personal-data/.
- “Global Internet User Survey 2012.” *Internet Survey*, 20 Nov. 2012.
- Government of India. “Ministry of Electronics and Information Technology, Government of India | Home Page.” *Www.meity.gov.in*, 11 Aug. 2023, www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
- Huang, Changwu, et al. “An Overview of Artificial Intelligence Ethics.” *IEEE Transactions on Artificial Intelligence*, vol. 4, no. 4, 2022, pp. 1–21, <https://doi.org/10.1109/tai.2022.3194503>.

- Jauhar, Ameen. "Facing up to the Risks of Automat Facial-Recognition Technologie in Indian Law Enforcement." *The Indian Journal of Law and Technology*, vol. 6, no. 1, 2020, pp. 1–15.
- Johannes Thumfart. "Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory." *Journal of Global Security Studies*, vol. 9, no. 1, Oxford University Press, Jan. 2024, <https://doi.org/10.1093/jogss/ogad024>.
- Khosla, Sunil. "The Right to Privacy: Constitutional Perspective in India." *INNOVATIVE RESEARCH THOUGHTS*, vol. 3, no. 2, Apr. 2017, pp. 121–27.
- Lucchi, Nicola, Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression (February 6, 2011). *Cardozo Journal of International and Comparative Law (JICL)*, Vol. 19, No. 3, 2011, Available at SSRN: <https://ssrn.com/abstract=1756243>
- "Ministry of Electronics and Information Technology, Government of India | Home Page." *Www.meity.gov.in*, 11 Aug. 2023, www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf
- Sarkar, Manoj Roy. "The Evolving Landscape of Digital Privacy in India: Balancing Innovation and Data Protection by the Government." *The E-Journal of ICISA*, vol. 9, pp. 4–10.
- Secure Privacy. "Understanding South Africa's POPIA | Data Protection Law, Compliance, and More." [Https://Secureprivacy.ai/](https://Secureprivacy.ai/), 19 Oct. 2023, secureprivacy.ai/blog/south-africa-popia-compliance.
- Sharma, Saurabh, et al. "Digital Transformation in India: Perspectives, Challenges, and Future." *Research Journal of Agricultural Sciences*, vol. 15, no. 01, Feb. 2024, pp. 31–37, www.researchgate.net/publication/383409687_Digital_Transformation_in_India_Perspectives_Challenges_and_Future.
- Shehu, Vlonia Pollozhani, and Visar Shehu. "Human Rights in the Technology Era – Protection of Data Rights." *European Journal of Economics, Law and Social Sciences*, vol. 7, no. 2, June 2023, pp. 1–10, <https://doi.org/10.2478/ejels-2023-0001>. Accessed 30 June 2023.

The Upwork Team. "6 Ethical Considerations of Artificial Intelligence | Upwork."
Www.upwork.com, 4 Oct. 2023, www.upwork.com/resources/ai-ethical-considerations.

Tungekar, Bushra. "How Google and Facebook Exploit the Users' Personal Data for Advertisement." *IPladers*, 14 Aug. 2021, blog.ipleaders.in/how-google-and-facebook-exploit-the-users-personal-data-for-advertisement/.

Tunggal, Abi Tyas. "What Is the Personal Data Protection Bill 2019? | UpGuard."
Www.upguard.com, 18 Nov. 2024, www.upguard.com/blog/personal-data-protection-bill.

Valdívia, Heloisa. "Brazil's General Data Protection Law (LGPD) Explained." *Termly*,
14 Feb. 2024, termly.io/resources/articles/brazils-general-data-protection-law/.



adani
international
school

Growing Together