



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

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.

A Comparative Look into India's Privacy Law in the WhatsApp Era and AI

-Chanchal Bhati

“Data is the new oil” is a popular and overused cliché that makes one wonder what oil has to do with data. Data is replicated and analyzed each nanosecond and it cannot escape: it is never wasted. The likes of Instagram, Facebook etc., all help in the creation of an economy whose primary output is our data. Thus, now the question to be asked is not, whether our data is being captured but how secure it is with the law.

Need for protection

Data Protection is comprised of Data Privacy and Data Security. Data privacy means a person's right of control over his own personal data. Personal data could be the location, age, gender, address, financial data, health information, and communications of the data subject. This information is utilized by companies to create targeted marketing campaigns and to make informed decisions. Hence, data privacy laws do not allow data to be shared with people that are not authorized to access the data, in order to prevent identity theft, phishing or other cybercrimes. Moreover, with the advent of an age of AI products and services, it has never been more critical to have individual data privacy laws that hold companies accountable and prevents them from being opaque with data.

India's response

India has recognized privacy as a fundamental right in its constitution as per Article 21. In furtherance of this, the Indian Parliament passed the Digital Personal Data Protection Act, 2023 on 11th August 2023. This was the first step towards formulating the privacy laws in India in the context of digital data. The Digital

Personal Data Protection Act, 2023 was brought into full effect by the notification of Digital Personal Data Protection Rules, 2025. This act gives the framework for data protection of personal data in India. It is able to identify and defend rights of the data principals. It makes companies that fail to comply with the law liable with punishments as high as 250 crores.

The Act requires that principles such as data minimization, consent, and transparency, accuracy and purpose limitation, storage limitation and security safeguards are also followed. Like every law, it too strikes a fine balance between an individual's right to privacy and the innovative needs of the companies to operate.

Key features of the Act

- 1.The off-territorial scope of the law applies to any data fiduciary outside India, that processes data of individuals in India for providing goods and services.
- 2.Take reasonable security precautions – data fiduciaries must implement security measures that are reasonably necessary to ensure the security of the personal data.
- 3.Data principals can have access to and rights over their data, which may be corrected or erased. They also are required to follow some obligations, such as not giving false information to the data fiduciaries.
- 4.The act lays out the establishment of a Data Protection Board of India (DPBI), which will be responsible for overseeing all aspects of personal data, and for receiving all complaints and breaches of the act.

A comparison of the other countries' laws

Digital Personal Data Protection Act is definitely steps ahead in the Indian data protection regime but it draws inspiration from the laws in other jurisdictions and also has some amendments to accommodate the local requirements. The GDPR (General Data Protection Regulation) of the EU is considered one of the toughest laws concerning data protection in the world and sets a high standard for other countries and companies that process the data of EU residents. The GDPR provides for very broad rights for data subjects, including a right to access, the right to be forgotten, the right to restrict processing, and the right to data portability. There are strict responsibilities on organisations such as the requirement for Data Protection Impact Assessments for activities that are likely to have a high impact on data protection and for Data Protection Officers to be appointed for some types of controllers and

processors. The GDPR also offers hefty fines for companies that do not comply, which range up to €20 million or 4% of the total worldwide revenue of the company for serious infringements.

The U.S. privacy laws, on the other hand, are less comprehensive and stricter; there is no single federal privacy law but instead an array of sector specific legislation that addresses specific types or categories of data, for instance, the HIPAA (Health Insurance Portability and Accountability Act) for health data. California also has its own set of laws, such as the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). The CPRA was written in 2020 and is scheduled to become effective in 2023; it is considered to be a reaction to the GDPR and gives California residents wide-ranging privacy rights.

Comparison laws from other countries

The new data protection law in India is somewhere in between the U.S. model and the GDPR. It sets out a detailed framework of privacy protection, as well as rights for businesses that deal with personal data. India's law has fewer restrictions for controllers and processors, which is expected to spur innovation and economic growth while maintaining data security, unlike the GDPR. Meanwhile, the data subjects' rights outlined in the law are less comprehensive than those of the GDPR, including the right to data portability and limiting the scope of automated decision-making. The lack of a clear definition on the scope of exemption in relation to the jurisdiction of the Data Protection Board in the Indian law is one of the most striking differences.

WhatsApp, AI, and next privacy challenge

It is clear that such a law is needed once one can take a look at the developments in technology and the degree to which social media platforms like WhatsApp have become an integral part of the day to day life. WhatsApp will now contain more personal information, thanks to the new features of AI. Even if end-to-end encrypted messages exist, WhatsApp would still be able to have access to the metadata, which could be used for commercial purposes or even transferred to third parties without the users' knowledge. Artificial Intelligence poses even more challenges to data privacy since AI requires a lot of personal data to operate and improve. In this context, it will be crucial for individuals to hold control over their personal information and their consent to how their information is processed by AI algorithms.

Conclusion

The Digital Personal Data Protection Act, 2023 is therefore only the first step in India's journey towards the protection and preservation of citizens' privacy. Enacted into full force, it will be interesting to see how it will be applied in practice and how it will balance individual privacy with the needs of businesses needing to process personal information for innovation and economic growth. Although the law is a significant milestone, it will be fascinating to observe the trajectory of the data protection regime in India over the years in the hands of the new Data Protection Board, and the judiciary's stance on the various provisions of the Act. Data privacy laws, including the data protection laws in India, are not just a technological problem, but a constitutional issue, and will be interesting to see how much India's courts will abide by the privacy of individuals over commercial and governmental interests.