COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS IN INDIA AND USA

Neha Yadav, AIALS, Amity University, Noida

ABSTRACT

This paper performs comparative research on India and the United States regarding data protection regimes presented in the dynamic digital ecosystem environment. The personal data is one of the assets with the blistering development of digital technologies, and it is also a matter of concern because of the issues of privacy, security, and misuse. This paper considers the legal contexts of the two countries in terms of data protection, i.e., the Digital Personal Data Protection Act of 2023 in India and the sectoral and fragmented strategy in the United States. It examines the most important features including territorial coverage, nature of data, applicability to the government and other foreign parties, data protection principles, rights of the data subjects, enforcement of the same, and the consent models. The paper indicates that although India is on the path of adopting a comprehensive, centralized framework based on the constitutional principles of privacy, the United States still refers to the model that is decentralized and sector-specific and provides flexibility, but not uniformity. The study also finds several important distinctions in the enforcement principles, personal rights, and the philosophy of the regulation and the existence of common issues, including the need to strike a balance between innovation and safeguarding privacy. It has been concluded in the paper that as a developing country with a formative stage, India can adopt the experience of the United States, one of the developed countries, and elaborate a more robust, transparent, and rightsbased data protection regime relevant to the Indian constitutional and social-economic conditions.

Keywords: Data Protection, Digital Privacy, Personal Data, Information Privacy, Data Security, Consent Models

INTRODUCTION

The fast evolution of digital technologies and data-oriented economies has altered the manner in which the personal information is gathered, processed, and used worldwide. With this changing digital environment, the issue of protection of personal data has become a pressing legal and policy issue leading to the development of a number of varied approaches to data protection across the jurisdictions. India and the United States are two extreme ways of regulating data privacy. Whereas India has just recently taken a more organized and holistic approach in the Digital Personal Data Protection Act, 2023, the United States still operates with a more fragmented and sector-specific approach that is regulated by a combination of federal and state laws. These variations are not only the differences in the legal traditions but also the differences in the priorities in the balancing between privacy, innovation, and regulation control.

This comparative study is aimed to discuss the main peculiarities of data protection legislation in India and the United States, their legal base, area of the jurisdiction, the nature of information they concern, the right of the government and foreign organizations, their general principles, the rights of the individuals, the system of punishment and the model of consent. By trapping the conclusions between the two systems, the paper will measure their efficiency in protecting personal information and will deal with the issues of regulatory loopholes, enforcement constraints, and contradiction with other primary rights. Finally, the given analysis highlights the necessity of the balanced and reasonable approach to data protection that does not obstruct the technological advancement and economic growth but enables personal privacy and dignity.

LEGAL FRAMEWORKS

India's Digital Personal Data Protection Act, 2023 (DPDPA) is its first comprehensive privacy statute, enacted after the Landmark Puttaswamy judgement recognized privacy as a fundamental right. however, the Act is limited to digital personal data, excluding manual records, and grants wide exemptions to state authorities. Scholars caution that while the DPDPA is step forward, it lacks the breadth of GDPR like framework. The DPDP Act, which was enacted in 2012, was India's first comprehensive data protection legislation[1]. When processing personal data, there are stricter requirements for clear, informed, and

[1] Vaibhav Shanker, An Analysis of Data Protection Laws and Right to Privacy A Comparative Study of India United States of America and United Kingdom, Manupatra, 178 (2025) [2] Id. at 177

purposespecific permission for children and those with disabilities. Additionally, the Act stipulates responsibilities like the appointment of Data Protection Officers, the completion of data protection impact assessments, and the upkeep of audit compliance. Violations may attract penalties of up to ₹250 crore, even though the law does not impose strict limitations on crossborder data transfers by the government.

While the United States adopts a fragmented approach. Key laws include the Health Insurance Portability and Accountability Act for health data, the Gramm-Leach-Bliley Act for financial data, and the California Consumer Privacy Act for consumer rights. This patchwork created inconsistency, leaving significant gaps in coverage. Critics contend that the lack of a comprehensive federal privacy law undermines the United States' credibility in global data protection and privacy governance. In the United States, there is not a single federal data protection law. Instead, sectoral laws like HIPAA (health information) and state laws like the California Consumer Privacy Act (CCPA) are cited. While some policies require opt-in consent, others provide opt-out choices for sensitive data. The Federal Trade Commission (FTC) and attorneys general of state are the primary decentralized agents in enforcement[2].

TERRITORIAL SCOPE

In India, the Data Protection and Privacy Act of 2023 (DPDP Act) is applicable globally. Because they handle personal data about Indians in connection with 180 products and services offered, domestic and international organizations are subject to this regulation. This implies that while dealing with the personal information of Indian individuals, businesses headquartered outside of India (such an American ecommerce platform) are required to adhere to Indian data privacy rules.

While in USA, a thorough federal data protection statute is non-existent in the US. It has rules at the federal and state levels (like HIPAA for health data and GLBA for financial data) as well as at the sector level (like California's CCPA/CPRA). Its legal framework is disjointed. There is a certain area to which each statute applies. Take HIPAA as an example:

- The law applies specifically to businesses operating within the United States, such as healthcare providers.

2

- Businesses that gather personal information from California citizens are subject to the CCPA if they meet certain requirements, such as having annual sales of more than $25 million or collecting data from more than 100,000 customers.

- Due to its lack of uniformity and limited scope, the United States model is not well-suited for effective extraterritorial application.

NATURE OF DATA

In India whether the personal data is gathered online or converted to the digital form after the offline collection, the DPDP Act, 2023 only pertains to the latter. A significant limitation is that the regulation does not address data that is not digital or accessible online. In addition, unlike the GDPR, the legislation does not provide precise definitions of "sensitive" or "critical" categories of personal data; however, such classifications may be included in regulations that are put into effect.[3]

While in USA the concept of "Personal data" is defined differently in each state's legal code. On the other hand, definitions vary by industry: In the financial industry, GLBA defines "nonpublic personal information," HIPAA defines "protected health information" (PHI), and CCPA extensively defines "personal information," which includes identifiers, geolocation, biometric data, and inferences. This means that there is more room for misunderstandings, gaps, and overlaps for groups that work in multiple industries.[4]

APPLICABILITY TO GOVERNMENT ENTITIES

In India the DPDP Act is applicable to both public and private organizations; however, there are some circumstances in which the Central government is excluded, such as when it is necessary to protect the nation's security, maintain law and order, or serve the public interest. Some have voiced concerns that this may pave the way for more monitoring or compromise user privacy in governmental settings.

While in USA Data protection laws in the United States typically apply to both the public and private sectors, with a few notable exceptions for matters related to national security, law

[3] Vaibhav Shanker, An Analysis of Data Protection Laws and Right to Privacy A Comparative Study of India United States of America and United Kingdom, Manupatra, 181 (2025)
[4] Id.

enforcement, and defense. The National Security Agency and the Federal Bureau of Investigation are two government agencies that may not be subject to privacy laws.

Furthermore, neither federal agencies nor state agencies are subject to the transparency laws.

APPLICABILITY TO FOREIGN ENTITIES

In India the DPDP Act applies to data processors and data fiduciaries outside of India who handle Indian citizens' personal information for the purpose of providing goods or services or profiling. In keeping with worldwide standards, this extraterritorial provision seeks to shield Indian nationals against the exploitation of foreign businesses.

While in USA only a small portion of U.S. legislation is legally binding for international businesses. Foreign companies that collect data from California citizens are subject to the CCPA if they meet certain criteria, such as:

- Making $25 million or more in yearly revenue,183 Processing data from 100,000 or more Californians, or
- Making 50% or more of their income from selling personal data.
- However, extraterritorial enforcement is either non-existent or poorly defined for the majority of federal legislation (such as HIPAA). Because of this, its global significance is severely limited.

KEY PRINCIPLES OF DATA PROTECTION

Rules for handling data are the backbone of any privacy protection system. Organizations are required to treat personal information in a responsible, ethical, and lawful manner according to these standards.

In India the DPDP Act includes a number of concepts that are similar to international standards. For the data to be processed legally, there must be a legitimate reason, it must be limited in scope, it must be accurate, it must be protected, and it must only be kept for the time necessary. The actions of a controller ought to be transparent and sincere, and they ought to accept responsibility for the data they handle.

While in the United States does not adhere to any kind of global code of conduct. The concepts are different for legislation that are particular to different industries. For example,

- HIPAA protects patient information.
- The financial industry is required to implement safeguards under GLBA.
- While the CCPA does provide some consumer control and transparency, it does not impose any data minimization or accountability requirements that are required.
- There is currently no industry-wide set of privacy standards because of this disjointed system.

RIGHTS OF DATA SUBJECTS

Data protection laws play a crucial role in granting individuals control over the use and processing of their personal data; however, the scope and nature of these rights vary significantly across jurisdictions. In India, the legal framework does not explicitly provide comprehensive rights such as the right to object, data portability, or broad-based erasure. Instead, individuals are primarily granted rights to access their personal data, seek correction of inaccuracies, and avail grievance redressal mechanisms. The right to erasure exists in a limited and indirect form, mainly through the withdrawal of consent, and does not extend uniformly to all situations.[5] Additionally, certain rights may be restricted in cases involving public interest, state functions, or government processing of data.

In contrast, the United States follows a fragmented and sector-specific approach to data protection, resulting in a lack of uniformity in data subject rights. For instance, under statelevel legislation such as the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), individuals are granted relatively strong rights, including the right to access, delete personal data, and opt out of the sale of their information. Similarly, sector-specific laws like the Health Insurance Portability and Accountability Act (HIPAA) allow individuals to access and correct their health-related information[6]. However, the absence of a

[5] Amala Maria George, Rights of Data Principals under the DPDP Act and Rules, legality.com, (2025)
[6] Vaibhav Shanker, An Analysis of Data Protection Laws and Right to Privacy A Comparative Study of India United States of America and United Kingdom, Manupatra, 185 (2025)

comprehensive federal data protection law means that no universal set of rights is guaranteed across the country, leading to varying levels of protection depending on the jurisdiction and type of data involved.

ENFORCEMENT AND PENALTIES

Enforcement and penalties play a crucial role in ensuring compliance with data protection laws and in deterring violations; however, the effectiveness of enforcement mechanisms varies across jurisdictions. In India, enforcement is entrusted to the Data Protection Board of India, which has been empowered to impose significant penalties for non-compliance. Under the law, serious violations may attract fines of up to ₹250 crore (approximately USD 30 million), reflecting a strong deterrent intent. However, concerns have been raised regarding the independence, capacity, and overall effectiveness of the Board, as the enforcement framework is still in its developmental stage and evolving in practice.[7]

In contrast, the United States follows a decentralized enforcement model, with no single authority responsible for overseeing data protection. Enforcement is primarily carried out by the Federal Trade Commission (FTC), particularly in matters relating to consumer protection, while state attorneys general also possess the authority to take action under state-specific laws. High-profile cases, such as the imposition of a $5 billion fine on Facebook in 2019 for privacy violations, demonstrate the potential severity of penalties[8]. Nevertheless, enforcement in the U.S. is often criticized for being inconsistent and largely reactive rather than proactive, due to the fragmented nature of its regulatory framework.

SPECIAL PROVISIONS AND CONSENT MODELS

Special provisions relating to consent models and the protection of minors form an essential part of any data protection framework, and a comparison between India and the United States highlights key differences in their approaches. In India, a stricter standard is adopted for children's data protection, as individuals below the age of 18 are required to obtain verifiable parental or guardian consent for the processing of their personal data. This higher age threshold, compared to global norms, may have implications for digital platforms catering to younger

[7] The Digital Personal Data Protection Act,2023, No.22, Acts of Parliament, 2023 (India)
[8] Vaibhav Shanker, An Analysis of Data Protection Laws and Right to Privacy A Comparative Study of India United States of America and United Kingdom, Manupatra, 186 (2025)

users. In contrast, the United States follows a more limited approach under the Children's Online Privacy Protection Act (COPPA), which applies only to children under the age of 13, requiring organizations to obtain parental consent before collecting or processing their personal information.

With respect to consent models, India follows a notice-and-consent framework that emphasizes informed and explicit consent. Data fiduciaries are required to provide clear notice regarding the purpose and nature of data processing, and consent must be obtained prior to such processing. Additionally, individuals must be able to withdraw their consent easily, and such withdrawal must be promptly respected. On the other hand, the United States largely follows an opt-out model, particularly under laws such as the California Consumer Privacy Act (CCPA), where individuals are given the option to opt out of certain data practices, such as the sale of personal data, rather than providing prior consent. This reflects a more flexible but less stringent approach compared to India's emphasis on prior, informed consent[9].

CONCLUSION

The comparative analysis of data protection laws in India and the United States reveals significant differences in their legal structures, enforcement mechanisms, and underlying philosophies. India's Digital Personal Data Protection Act, 2023 represents a progressive step towards establishing a unified and comprehensive framework for data protection, grounded in the recognition of privacy as a fundamental right. However, certain limitations, such as broad state exemptions, limited data subject rights, and evolving enforcement mechanisms, indicate that the framework is still in its developmental phase.

In contrast, the United States adopts a fragmented and sector-specific approach, characterized by a combination of federal and state laws. While this model provides flexibility and industry-specific regulation, it lacks uniformity and leaves gaps in protection. Enforcement in the U.S., though sometimes stringent, remains inconsistent due to its decentralized nature. Both jurisdictions face the common challenge of balancing individual privacy with technological advancement, economic growth, and freedom of expression.

Ultimately, the study suggests that India has the opportunity to refine its data protection regime

[9] Vaibhav Shanker, *An Analysis of Data Protection Laws and Right to Privacy: A Comparative Study of India United States of America and United Kingdom,* Manupatra, 187 (2025)

by addressing its existing gaps and learning from the strengths and weaknesses of the U.S. model. A balanced approach that ensures strong individual rights, transparent governance, effective enforcement, and accountability will be essential for safeguarding personal data in the digital age while promoting innovation and maintaining democratic values.