International Journal of Civil Law and Legal Research

E-ISSN: 2789-8830
P-ISSN: 2789-8822
Impact Factor (RJIF): 5.62
IJCLLR 2026; 6(1): 15-22
www.civillawjournal.com
Received: 10-11-2025
Accepted: 13-12-2025

Sunil Sudhakar Varnekar
Research Scholar, Alliance, School of Law, Alliance University, Bangalore, Karnataka, India

Upankar Chutia
Associate Professor, Department of Law, Alliance School of Law, Alliance University, Bangalore, Karnataka, India

Correspondence
Sunil Sudhakar Varnekar
Research Scholar, Alliance, School of Law, Alliance University, Bangalore, Karnataka, India

Privacy in the digital age: A comparative study of India's legal gaps and U.S. data protection frameworks

Sunil Sudhakar Varnekar and Upankar Chutia

DOI: https://www.doi.org/10.22271/civillaw.2026.v6.i1a.180

Abstract
The ever-growing rate of the spread of digital technologies in India has required creating a strong legal framework to protect the information that can be considered personal. The Indian government reacted to it by passing the Digital Personal Data Protection Act, 2023 (DPDP Act), a major legislative action towards controlling the processing of personal data in the digital environment. Although the Act provides many fundamental principles that include consent, limitation of purposes, and duty of data fiduciaries, it also demonstrates several vital weaknesses. These are the fact that its definitions are vague and plentifully exception-ridden on the State side, it has little enforcement capabilities, over depends on the consent process, and did not include concrete individual redress channels. This paper takes a critical look at these gaps in the DPDP Act of India and how some of the issues generated by these gaps have been handled in the context of the developing state-level regime of data privacy in the United States. The absence of the federal privacy law leaves the U.S with a patchwork of estimates such as California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), and the recent bills as enacted in Tennessee, Minnesota, Maryland, Indiana, Kentucky, and Rhode Island. These laws provide us with good lessons on how to strengthen consumer rights, the definition of sensitive data, restriction of data sales, and how to enforce the same by using independent authorities. Using comparative legal analysis, the research paper finds possible regulatory practices in the U.S. practice that can be used to help shape a more accountable, transparent and citizen-centred data protection regimes in India. It proposes amendments to make DPDP Act more readable, curb government snooping without checks, and provide data principals with rights that they can enforce and institutional independence. These results indicate that there is necessity to make India adapt its privacy regime to global best practices to achieve adherence to the values enshrined in the constitution and promote the development of trust in the digital economy.

Keywords: Data privacy, data protection, comparative analysis, digital personal data protection act

Introduction
The era of all-pervasive digitization has brought about the new oil, Personal data to power the innovative processes, governmental and business activities. Nevertheless, the revolution has brought new levels of threat to privacy, misuse of information, and spying. In response to these issues, India passed Digital Personal Data Protection Act, 2023 (DPDP Act) [1], its first overarching statute limited specifically to protection of personal data. The Act aims to guide collection, processing, storage, transfer of personal data with references to principles of consent, data minimization and accountability.

Although an important piece of legislation, the DPDP Act has been criticised by the scholarly community, civil society and legal experts all citing the numerous gaps in the Act relating to its ambiguity in use of terminologies, ineffective protective measures against state snooping and lack of an effective implementation, and a defunct provision of individual rights. Such flaws question the ability of the law to be able to successfully uphold the fundamental right to privacy as confirmed by the Supreme Court of India in Justice K.S. Puttaswamy v. Union of India (2017) [2].

This is vital now that India is pursuing a goal of becoming a digital superpower, so it is necessary to question the effectiveness of its regime of data protection in comparison to

[1] Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice. Retrieved from https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023
[2] Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1. Retrieved from https://indiankanoon.org/doc/91938676/

international standards. The present paper therefore examines the limitations with the structure and practice of data protection in India and how potentially better practice can be made by looking through the prism of comparative experiences of the United States, particularly by the state level data protection acts, such as the California Consumer Privacy Act (CCPA) [3] and California Privacy Rights Act (CPRA) [4].

A detailed comparison of data privacy laws in India and USA is crucial to identify their divergent and convergent aspects. Similar analysis between regulations allows businesses to maintain compliance with all applicable laws to prevent expensive legal penalties. Businesses gain complete control over their data privacy protocols by comprehending individual law requirements thus they can build consumer trust and protect sensitive data effectively. Focusing on data privacy proactively at once reduces organizational risks while showing dedication to moral business conduct and effective data management.

With this background the current study aims to conduct a Comparative Analysis of Data Privacy Act in India and USA. The first section of this research article presents the background of the study, the second section highlights the existing literature on the Data privacy law. Research methods are states in the third section of this article. The results and discussion are presented in the fourth section followed by the conclusion.

Literature Review

Yadav and Yadav (2021) Detailed that Justice BN Srikrishna's team drafted the 2019 Personal Data Protection Bill. It owes a great deal to GDPR and draws heavily from it in its development. The Data Protection Rules and Regulations from before suggest that this measure will have a significant positive impact, even though Parliament has not yet approved it. All things pertaining to data storage, collecting, processing, fines, compensation, and the code of conduct are covered in the 2019 Personal Data Protection Bill. There are three distinct categories of information defined by the Personal Data Protection Bill: general, sensitive, and critical. Examples of sensitive personal data include passwords, health records, and gender identification information [5].

According to Gupta and George (2025) Strong personal data protection laws in India are more important than ever in this age of the fast developing digital economy. The country's data governance has entered a new era with the passage of the Digital Personal Data Protection (DPDP) Act, 2023. Businesses, especially those operating in the digital realm, will find the Act's many provisions and their consequences analyzed in this chapter. The DPDP Act's requirements are in line with global data protection standards, and they lean more towards the "conditional" model of data protection. Since the DPDP Act does not mandate data localization and permits unfettered cross-border data flows, its beneficial effects on businesses are clear [6].

Lim and Oh (2025) expressed that there are legitimate worries regarding people's right to privacy in light of the Fourth Industrial Revolution's heavy use of big data and AI. Because of this, several nations' privacy protection acts have been revised or passed entirely. Despite this, and particularly in light of recent legislative developments, there is a dearth of research that compares these laws across other nations. This research addresses that knowledge vacuum by comparing and contrasting personal information protection statutes in five key areas: the EU, the US (with a concentration on California), China, Japan, and South Korea. The research delves into the various ways in which different regions' distinct political, cultural, and historical circumstances have shaped their approaches to privacy protection. As an example, the General Data Protection Regulation (GDPR) of the European Union (EU) places an emphasis on personal rights that have been shaped by past misuses of personal data. Also, reflecting the tech-driven economy of the state, the California Consumer Privacy Act (CCPA) [7] places an emphasis on consumer rights within a framework of self-regulation. This study delves into the following legal frameworks: the Personal Information Protection Law (PIPL) [8] in China, which places a premium on national security; the Act on the Protection of Personal Information (APPI) [9] in Japan, which deals with the conflict between personal privacy and social norms; and the Personal Information Protection Act (PIPA) [10] in South Korea, which reflects Confucian principles by balancing personal autonomy with a feeling of community. This report adds to the continuing conversation about global data privacy regulation by highlighting the strengths and weaknesses of data protection laws in different regions. To help stakeholders and legislators negotiate the data economy's intricacies while maintaining strong privacy protections, it provides helpful insights [11].

A new idea known as big data has arisen as a result of scientific and technological progress. Both public and private entities, including businesses and nonprofits, have shown interest in it due to its practicality. However, it has also brought up certain questions of morality, law, and ethics. In this research, researchers examine how big data poses risks to people's privacy. This study seeks to provide a solution to protect individuals' privacy from such dangers by comparing the privacy and data protection regulations of the United States with those of India. Researchers used a variety of research methods, including the doctrinal, armchair, exploratory, analytical, and comparative approaches. Adopting appropriate technological standards, managerial practices, and the force of legislation, according to the

[3] State of California. (2018). California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. Retrieved from https://leginfo.legislature.ca.gov

[4] State of California. (2020). California Privacy Rights Act of 2020, Cal. Civ. Code § 1798.100 et seq. (Amending the CCPA). Retrieved from https://oag.ca.gov/privacy/ccpa

[5] Yadav, A. and Yadav, G., 2021. Data protection in India in reference to personal data protection bill 2019 and IT act 2000. Int. Adv. Res. J. Sci. Eng. Technol, 8(8).

[6] Gupta, N. and George, A., 2025. Digital Personal Data Protection Act, 2023: Charting the Future of India's Data Regulation. In Data Governance and the Digital Economy in Asia (pp. 34-53). Routledge.

[7] California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa

[8] Personal Information Protection Law (PIPL), https://personalinformationprotectionlaw.com/

[9] Act on the Protection of Personal Information (APPI) in Japan https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en

[10] Personal Information Protection Act (PIPA), https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01

[11] Lim, S. and Oh, J., 2025. Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. IET Information Security, 2025(1), p.5536763.

authors, is the only way to guarantee individuals' privacy. It is also recommended that businesses and other organizations implement self-regulating policies and procedures. In this study, "privacy" refers only to personal information and does not encompass issues of national security or corporate secrets. In order to safeguard personal information, the authors also propose and propose a framework that India can adopt [12].

The literature review revealed that there are very few studies which directly compare and contrast the data protection provisions between India and USA. The comparison between Indian and US data protection laws requires enhanced research because of their respective legal regulations and cultural elements. Learning about these disparities between Indian and American laws allows officials as well as business entities to determine the best approaches for handling privacy regulations across both countries. An exploration of these regulatory distinctions should analyze their effects on worldwide data exchange procedures and diplomatic data collaboration treaties in order to develop global data protection strategies.

Research Problem

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a major move towards regulation of usage and collection of personal data in India. Nevertheless, the legislation has numerous structural, theoretical and procedural gaps that could make it ineffective in safeguarding the informational privacy of individuals. Among those are various uncertainties of definitions, overdependence on consent without sufficient protective measures, extensive exemptions in the favor of the State, deficient institutional independence of Ethics of Data Protection Board, and the shallow rights of data principals.

Meanwhile, the international trends in the privacy law, especially in such countries as the United States provide an opposing example of what should be improved in India. The laws at the state level of the United States with the example of the California Consumer Privacy Act (CCPA) and its renewal in the form of the California Privacy Rights Act (CPRA), offer models with more powerful enforcement mechanisms, well-defined consumer rights, and industry-specific accountability measures. Although the U.S. does not have a federal comprehensive privacy law, such subnational models show legal creativity that may teach a lesson to India.

The underlying issue that the research aims at resolving is:

How well does the Digital Personal Data Protection Act, 2023, of India serve to protect personal data, and how a comparative study of the U.S legal system can help us understand the lacunas and the possible amendments needed in the Indian legal framework to bring it on par with the international Industry best practices as regards data privacy?

The research problem is also based on the increasing significance of the cross-border data flows, the worldwide tendency to create the unification of privacy standards, and the necessity to ascertain that the legislature of India not only ensures the rights of individuals but also legally safe harbor its digital economy.

Research Objectives

- To distinguish and examine the main gaps in Digital Personal Data Protection Act 2023, such as loopholes of obtaining consent, vagueness of definitions, independency of regulatory authorities, and exemptions of States.
- To assess the main data privacy laws in the United States, especially in California, including the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).
- To compare the techniques of legal protection of data under Indian and the U.S. law
- To make some suggestions on enhancing the DPDP Act to meet the best practices adopted internationally concerning the enhancement of regulatory accountability, transparency, and privacy of data principals.

Research Hypothesis

"The Digital Personal Data Protection Act, 2023 does not cover all aspects of data privacy protection in India with important legal gaps and such gaps could be effectively overcome through the introduction of key principles and mechanisms of the U.S. data privacy laws, especially California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)."

Research Methods

This research performs a doctrinal evaluation[13] of specific data protection guidelines that exist in India and the USA. The employed research methodology allows for an extensive evaluation of privacy legislation throughout India and the USA.

Results and Discussion

India - The Digital Personal Data Protection Act, 2023

Data protection in India lacked a unified framework or regulation until 2023. This data protection framework was based on the Information Technology Act, 2000 (IT Act) [14] and the guidelines that were announced under it. The 2011 Privacy Rules and the Information Technology (Reasonable Security Practices and Procedures) Rules were part of this package.

Article 21 of the Indian Constitution guarantees citizens the right to life and liberty, including the right to privacy. In the case of Justice K. S. Puttaswamy (Retd.) v. Union of India [Writ Petition No. 494/2012] [15], a nine-judge constitutional bench of the highest court in India affirmed this right in 2017. Because of this, a thorough data protection framework for India was developed. The Digital Personal Data Protection Bill (DPDP Bill) was released in 2022 by the Ministry of Electronics and Information Technology (MeitY), Government of India, after multiple drafts of data protection legislation had been released and various stakeholders' recommendations had been considered.

[12] Rautdesai, R., Nandekar, U., Kedari, A. and Patil, Y., 2019. Big data and privacy-a legal perspective and comparative study of the USA and India. International Journal of Process Management and Benchmarking, 9(2), pp.250-275.

[13] MD, P., 2019. Legal research-descriptive analysis on doctrinal methodology. International Journal of Management, Technology and Social Sciences (IJMTS), 4(2), pp.95-103.

[14] THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000), https://eprocure.gov.in/cppp/rulesandprocs

[15] AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, (2018) 12 SCALE 1, (2018) 4 CURCC 1, (2018) 255 DLT 1, 2018 (4) KCCR SN 331 (SC), AIRONLINE 2018 SC 237

Both chambers of the Indian parliament subsequently approved an amended DPDP Bill that differed significantly from its initial draft. The Digital Personal Data Protection Act, 2023 (DPDP Act), which will serve as the regulatory framework for personal data protection in India, was published by the Indian government on August 11, 2023. When it comes to digital personal data, the DPDP Act brings a number of compliances regarding collection, processing, storage, and transfer. Still, the government has to do more to make the DPDP Act a reality. That includes giving notice of the relevant provisions of the act, doing away with the Privacy Rules, and giving notice of the rules and regulations needed to put the act into effect and enforce it. No non-personal or non-digital data is regulated by the DPDP Act; it only applies to digitally stored personal information. This being the case, there are presently no regulations in place in India regarding the gathering and processing of non-personal data [16].

To be more specific, the IT Act and the Privacy Rules constitute the present privacy framework. Despite the publishing of a draft of the rules under the DPDP Act by the Government of India, the Act's provisions have not yet been enforced.

Rules

A draft of the Digital Personal Data Protection Rules, 2025 (Draft Rules) [17] was posted by MeitY on January 3, 2025, and stakeholders and the general public were invited to submit comments until February 18, 2015. After this deadline, the government will examine the feedback that was received. It is anticipated that the rules pertaining to the Data Protection Board of India's establishment and operations would be published in the Official Gazette and will likely take effect immediately (after the implementation of the DPDP Act). The remaining regulations may be given more time for companies to comply with them before they take effect. The Draft Rules do not include a timeframe.

Scope and Applicability

The DPDP Act is relevant to data processing in India involving digital personal information, including cases where the data is (i) acquired digitally or (ii) acquired non-digitally and thereafter transformed into digital form. Processing personal data in a format other than digital is thus exempt from the DPDP Act. Any information pertaining to a specific identifiable individual is considered "personal data" under the DPDP Act's expansive definition. Personal information stored digitally is likewise defined there [18].

Foreign entities that provide goods and services to Data Principals situated within India's territory and process personal data in relation to such activities are also subject to the DPDP Act, which is applicable to entities in India that process personal data but also has extra-territorial applicability. I data used for private or household purposes; and (ii) data knowingly made public by the Data Principal (the person or organization to whom the data pertains) or any other entity required by law to make such disclosure. Neither of these categories are covered by the DPDP Act.

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023) [11th August, 2023.] [19]. A law to regulate the handling of personally identifiable information in digital form in a way that balances people's right to privacy with the necessity of processing such data for legitimate business objectives and things related thereto or incidental thereto. Hereby is declared by Parliament to be the law of the Republic of India in its 74th year:

Digital Personal Data Protection (DPDP) Act, India's inaugural data protection law, was enacted in August 2023. Both online and offline processing of personal data is governed by the DPDP Act.

Key features

- The DPDP Act offers individuals greater agency over their data.
- It safeguards personal data from unlawful or unauthorized processing, accidental loss, or damage.
- It mandates that data fiduciaries respond to data breaches.
- Data subjects have rights under the law, including the ability to access, rectify, or erase their data as well as file a complaint.
- Data subjects under the age of 18 or with disabilities must have their parents' or guardians' permission before their data can be processed.

Other provisions

- Data processing inside and outside of India is governed by the DPDP Act.
- The state is exempt from the act for specific processing objectives, such investigating and preventing violations.
- To aid data principals with giving, managing, reviewing, and withdrawing consent, it has Consent Managers.

Related rules

The Digital Personal Data Protection Rules, 2025 have been prepared by the Ministry of Electronics and Information Technology to put the DPDP Act into action.

Data Privacy Act in USA

The Privacy Act of 1974, ADPPA [20], and state legislation are among the several data privacy statutes that exist in the US.

Privacy Act of 1974

Federal agencies are required to publish notices in the Federal Register when they create or modify systems of records. Individuals are given the right to know what information is collected, how it is used, and to request corrections. The law also protects individuals' privacy by setting rules for how federal agencies collect, use, and disclose personal information.

American Data Privacy and Protection Act (ADPPA) [21]

[16] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023), https://www.meity.gov.in/static/uploads/2024/06/2bf1ftDTyUJuWvjrG3pKWVwg8RB5YYfuxdo5.pdf

[17] Digital Personal Data Protection Rules, 2025 (Draft Rules), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/jan/doc202515481101.pdf

[18] Id.

[19] Id.

[20] Privacy Act of 1974, as amended, 5 U.S.C. § 552a, https://www.justice.gov/opcl/privacy-act-1974

[21] H.R.8152 - American Data Privacy and Protection Act, https://www.congress.gov/bill/117th-congress/house-bill/8152

Would mandate that businesses use security measures to safeguard personal data. Would outlaw firms from discriminating based on personal data. Would create consumer data safeguards, including the ability to view, rectify, and erase personal data

State data privacy laws

The following data privacy laws were enacted in 2024:

- The New Hampshire Privacy Act in New Hampshire, which will be effective in 2025 [22];
- The Nebraska Data Privacy Act in Nebraska [23]; and
- A comprehensive data privacy legislation in Kentucky [24].

The ADPPA was introduced in the House in 2022.

United States privacy legislation is a complicated mix of national, state and local privacy laws and regulations. The US does not have a comprehensive privacy law. On the other hand, there are a plethora of privacy and data security rules in the United States, both federal and state/local. Many of these laws are tailored to certain industries. As of 2018, the first state to propose and pass its own comprehensive privacy law was California. Changes in the political atmosphere, industry involvement, and the growing complexity of privacy problems have hindered attempts to enact an omnibus measure, despite the introduction of bipartisan draft bills (such as the American Privacy Rights Act of 2024). As a result, the passage of a nationwide privacy law covering all bases is unlikely to happen anytime soon.

Federal and State Privacy Laws and Regulations

Financial institutions, healthcare providers, telecommunications firms, credit reporting agencies, driving records, telemarketing, biometrics, and communications privacy laws are all part of the federal rules and regulations.

Numerous state statutes pertaining to data protection and privacy may intersect with federal statutes; however, although some of these state statutes are partially pre-empted by federal statutes, others are not. When it comes to data security, secure destruction, social security number privacy, online privacy, biometric information privacy, and data breach notification laws, some US states have regulations and laws that apply across sectors and go beyond what is required by federal laws. Each of these states has its own set of rules that govern the handling of private information pertaining to individuals or events taking place within its borders. Consequently, a plethora of state privacy and security statutes and regulations need compliance for many US-based enterprises.

California residents will have an easier time erasing their personal data stored by data brokers according to the "Delete Act," which the CPPA enforces and goes into effect on January 1, 2024 [25]. The Delete Act mandates that the CPPA create an easily accessible deletion mechanism no later than January 1, 2026. The goal of this system is to make it possible for customers to request the deletion of their data from data brokers and any related service providers or contractors with a single, verified request.

Businesses that fall under the CCPA's "business" definition and offer online services to users under the age of 18 are subject to the California Age-Appropriate Design Code (CAADC) [26], which was approved by the state legislature in August 2022 and was scheduled to go into force on July 1, 2024. On the other hand, the law was blocked from taking effect on September 18, 2023, by an injunction issued by a California District Court on First Amendment grounds. The status of the statute is now uncertain, as it was appealed to the Ninth Circuit by the office of the California Attorney General. The California Age-Appropriate Design Code can be found online for further details.

Likewise, Connecticut's Consumer Data Protection Act was revised to incorporate comparable safeguards for children's personal information, and Maryland's "Kids Code" was also passed. Additionally, the FTC enacted substantial revisions to the federal Children's Online Privacy Protection Act (COPPA) in January 2025 [27]. Despite the fact that the FTC conducts regular reviews of the COPPA rule, these revisions mark the first update to the rule since 2013. In an effort to make the internet a safer place for kids, the FTC claims that the final regulation update takes into account technology developments since the last time COPPA was revised. The revised rule can be found online in more detail. A more secure digital environment, with children's privacy protected in an ever-more-connected world, is the goal of joint efforts by federal and state regulators.

While not identical, these state privacy laws are very similar to one another in most areas. The CCPA is the only exception; however, they may vary in scope, disclosures of privacy notices, rights to privacy, and particular definitions. Information gathered and handled in the course of an employee's or client's relationship with a company is typically exempt from these state rules as well. Despite sharing certain practical similarities with these state laws, the CCPA takes a far more nuanced approach with its definitions, criteria, and prohibitions. What's more, it applies to personal information acquired from California citizens in both employment and business-to-business settings, which is rather noteworthy.

In 2023, Washington passed the historic My Health My Data Act (MHMD) [28], which marked the beginning of major advancements in the health data arena. Although the law is supposed to exclusively apply to consumer health data, the fact that it has very wide definitions and a private right of action means that it could end up affecting data that many corporations wouldn't normally consider "health" data. The MHMD Act can be read in its entirety on the internet. A number of states have enacted legislation to safeguard consumer health data since MHMD. For example, on March 31, 2024, Nevada's Consumer Health Data Privacy Law took effect as a result of senate bill 370, and on October 1, 2023, Connecticut revised its Consumer Data Privacy Act to incorporate comparable safeguards.

[22] Eight New State Privacy Laws Take Effect in 2025 - Are You Ready? https://www.duanemorris.com/alerts/eight_new_state_privacy_laws_take_effect_2025_are_you_ready_1224.

[23] Id.

[24] Id.

[25] https://www.clarkhill.com/news-events/news/california-privacy-protection-agency-shuts-down-data-brokerage-through-delete-act-enforcement/

[26] California Age-Appropriate Design Code (CAADC), https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false

[27] Maryland Kids Code Signed Into Law, But May Face Legal Challenges, https://www.techpolicy.press/maryland-kids-code-becomes-law/

[28] My Health My Data Act (MHMD), Protecting Washingtonians' Personal Health Data and Privacy

Last but not least, state privacy laws have been passing at a record rate as of late. The following states have passed or introduced privacy laws that are either very similar to or comprehensively address privacy:

- Tennessee- To take effect July 1, 2025 - Tennessee Information Protection Act provides the right of the consumer to access, delete, and correct their personal data as well as withdraw participation in targeted advertising. It is imposed on big data processors and requires data protection testing, to which enforcement is possible by the Attorney General.
- Minnesota- July 31 2025 - The Minnesota Consumer Data Privacy Act grants individuals the rights to access, correct, delete and opt-out of profiling and sales. It is the only system to regulate automated decision-making and insists on the businesses to have their internal data inventories.
- Maryland -November 1, 2025 - The Maryland Online Data Privacy Act places a high value on data minimization and exposes the consent of processing sensitive personal data. It provides wide consumer rights and requires transparent privacy notices, which is enforced by the Maryland Attorney General.
- Indiana - Applies January, 1, 2026 - Indiana Consumer Data Protection Act is a copycat of Virginia and it extends granting access, delete, correct and opt out rights. It also contains a 30-days curative clause against breaches and has to be applied to companies that have a massive amount of resident data.
- Kentucky -effective January 1 2026 - The Kentucky Consumer Data Protection Act provides the right of consumers to their personal data and restricts discrimination of exercising rights. It not only excludes the HIPAA-covered information but also enforces it against the attorney general with a remedied cure provisions.
- Rhode Island -January 1, 2026 - Rhode Island Rhode Island Data Transparency and Privacy Protection Act covers mid-size processors and requires profiling and data sales opt-outs. It incorporates punishment against defiance and demands a declaration of AI-generated materials.

However, there is no universal federal law in the United States similar to the GDPR that exists in the European Union. In the U.S. it is regulated by the federal laws and state laws as well as specific sector laws like CCPA and HIPAA respectively. This fall is due to the fact that it offers more flexibility and opportunities to innovate because different states may have different requirements; this can be viewed as a strength. Also, the U.S. framework usually focus on economic development and such things as inventions, whereas businesses usually are given more freedom in how they want to approach the data in comparison to more rigid regulations.

The American laws are considered to be more effective, as they are flexible and allow for the greatest degree of adjustment to the conditions, providing for the specific development of technologies and the economy. In essence, the sector-specific form enables the performance of specialised regulations that are required to fit particular business areas. Nevertheless, it means that there may be gaps and inequalities in the protection and consumers can be covered to a lesser extent compared to, for example, India's proposed bill or the GDPR.

Comparative analysis - India and USA

Table 1: Comparative analysis - India and USA

Framework	India	USA
Regulatory Framework	Particularly, the regulatory framework for data privacy in India is the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 201". The most noteworthy and mainly proposed legislation is the Digital Personal Data Protection (DPDP) Act, which is intended to create a similar legal body to the GDPR as in the European Union. This has been streamlined and it is still on the word works awaiting a legislation to follow through and make it law of the land.	Regulatory Framework: Currently, the USA does not have one central federal data protection law as provided for by the GDPR or the proposed Personal Data Protection Bill of India. It is only substantiated by numerous federal and state laws. Health information is under the Health Insurance Portability and Accountability Act (HIPAA), information relating to kids under COPPA, and information from unfair or deceptive practices under the Federal Trade Commission Act.
Enforcement agency	Proposed that is the Data Protection Authority of India (DPAI) to enforce and monitor the data protection law.	There are other state laws on privacy, as we have seen earlier, the CCPA & CPRA which give an ideal privacy remedy to the residents of California. They play significant role in determining the privacy laws across the country.
Data Localisation	Indian law is rather protective of this concept in a way that some certain data must be stored in India. The role of this is aimed at ensuring that data is more secure and to cover sovereignty of the particular country.	Currently, there is no extensive law that compels the localization of data within the USA; data is transferable across borders.
Consent and Data Processing	The Act puts focus on the legal requirement of obtaining authorization of an individual prior to processing his/her data coupled with the circumstances under which an authorization can be rescinded.	There are different laws for consent and different types of consent based on the context. For instance, COPPA obligates that personal information from children under 13 years should only be collected after getting the permission of the parents or guardians.
Data Subjects' Rights:	Provides them general rights like the ones provided by GDPR where the data principals can access, rectify and delete their data.	The rights that are accorded to individuals will also depend on the law to be applied. For instance, the CCPA shares the same freedoms as the GDPR freedoms such as the freedom to know the data being collected and the freedom to request for deletion.

Despite the geographical shift of their jurisdiction, it is clear that there are many differences between data protection legislation in India and that of the United States especially with regard to the DPDP Act 2023 in India and the collection of federal and state laws in The United States of America. The DPDP Act goes a long way in the elaboration of a legal framework of data protection in India with a focus on consent, purpose limitation and localisation, wherein the data has to be stored in India. Nonetheless, the U.S. has a sectorial legislation approach where certain laws such as the CCPA and HIPAA afford considerable protection, though in certain areas of operation. Comparatively, the U.S. system is more developed and flexible and has many judicial decisions and higher enforcement capacity to meet its goals. Further, the similar laws present certain feature of flexibility and innovation friendly than that of UK laws which in turn help in growth of business. Despite the DPDP act being an efficient attempt for strengthening data protection in India, the American approach is relatively stronger and provide broader coverage and flexibility in addressing the new challenges coming up in the digital world.

Suggested Amendments to the DPDP Act, 2023 according to U.S. Privacy Law

1. Empower Autonomy and Accountability of the Data Protection Board

Indian problem: The Data Protection Board is formed and governed by the central Government, which leads to the question of its independence.

Proposed Amendment

Create a Data Protection Authority that is both judicially independent and who is accountable before parliament, but with operational independence as the California Privacy Protection Agency (CPPA) has.

Place a fixed tenure, a clear system of selection criteria and prohibit executive interference in the decisions.

2. Closer State exemptions and make Judiciary more vigilant

Problem in India: The DPDP Act offers wholesale exemptions to the government (e.g. Section 17) undermining data privacy protection against surveillance.

Proposed Amendment

Make exemptions more specific with the provision of extraordinary protection, encompassing the need to access and monitor data only prior judicial consent.

Implement the Sunset Clauses and Time-limit to laws granting any exemptions taken in the name of sovereignty, or the public order.

Make exemptions and carve-outs consistent with the U.S. example in which even nation-security surveillance (e.g. under FISA) is afforded legal safeguards and Congressional oversight.

3. Set more Rights to Data Principal

Indian Problematic Area: Data principals do not have much rights, e.g., access, correction, and erasure have unclear mechanisms of operations.

Proposed Amendment

A Right to Data Portability (a provision in CCPA and GDPR) must be added.

Identify an opt-out right in sharing or transferring data to third parties.

Control non-discrimination, thus people are not refused delivery of services because they exercise their right to privacy--in the example of the CCPA, this would be CCPA Section 1798.125.

4. Position Sensitive and High-Risk Classes of Data

Problem in India: The Act has removed a distinct legal framework on such sensitive or critical personal data as compared to the earlier drafts.

Proposed Amendment

Raise again and de-mystify Sensitive Personal Data (SPD) and Critical Personal Data (CPD).

Institute strict regimes of consent, security in storage and scrutiny of cross border transfers of such data, basing it on U.S. models such as the HIPAA standard (on health data) and the COPPA standard (on children data).

5. Write prescriptions of Minimum Security Controls and Breach Reporting Timeframes

Problem in India: Security practices that a fiduciary will have to engage in, defined as reasonable security practices, is undefined, and placed under the discretions of fiduciaries.

Proposed Amendment

Implement minimum technical requirements (e.g. encryption, two-factor authentication, multi-tenancy access).

Make breach notification mandatory and give a time limit of 72 hours as in CCPA and CPRA.

Have consumer remedies on breach or misuse such as statutory damages.

6. Guarantee a Limitative right to private Action

Indian Problem: The Act does not allow people to file lawsuits against the violation of data.

Proposed Amendment

Data principals should have the right to take civil action where its breach or misuse is substantial.

This can be modeled on CCPA with its narrowly defined private right of action, which only applies where there is negligence-related unauthorized disclosure.

7. Increase Broader Coverage than the Digitally Processed Data

Problem in India: The Act is limited to digital personal information leaving behind any offline information which can subsequently be digitalized.

Proposed Amendment

Broadening the scope of the law to cover offline data that would be digitised in time, e.g. in line with U.S. laws that apply to the collection of online and offline data (e.g. CPRA extends to employee and business-to-business data).

8. Comply with Informed Consent, Granularity, and Revocability

The Problem in India: Consent is a one-time, blanket authorization and can be corralled or lost in alternate configurations.

Proposed Amendment
Require fine-grained, specific-purpose consent of various forms of processing.
Foster revocancy in an easy and cost-free manner.
Make privacy notices comprehensible by using plain language as in case of CCPA with regard to its notice at collection.

9. Make Notions Clear and Less Vague
Problem in India: There are ambiguous words in the problem like; public order, harm and anonymization.

Proposed Amendment
Give definite statutory definitions of key terms and make them internationally harmonized.
Provide a statement of explanatory notes or legislation direction to curtail administrative choices.
Such amendments would make the DPDP Act of India more friendly to international best practices, individual rights enhancement, corporate responsibility, and guarded against abuse particularly on part of the State. Notably, a rights-based and independent governance structure on data protection would increase the convenience in the Indian digital economy and equip it better towards international digital cooperation.

Conclusion
The digital economy depends heavily on continual development of privacy protection standards which should be enhanced regularly for India and USA because both countries need stronger measures to shield individual rights and digital trust. Both countries need to maintain cooperative partnerships to resolve emerging security and privacy concerns in data protection because policymakers together with businesses and individuals must put privacy and security first to protect the digital environment. The implementation of global data privacy standards will affect entire nations together with the worldwide community. Security of all digital users' rights requires portant stakeholder cooperation to establish advanced data privacy regulations in modern times.
Research activities must remain active because they provide the necessary strategy to anticipate upcoming threats targeting privacy and security of data. Stakeholders can strengthen their data protection measures by regular assessments which allow them to uncover vulnerable areas to develop required improvements. The changing technology environment coupled with expanding data usage requires ongoing analysis as well as research to maintain data privacy as the main concern across all involved parties.

Author statement
All authors contributed equally to this work.

Declaration of Competing Interest
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability
Data will be made available on request.

Acknowledgment
We extend our sincere gratitude to the administration of Alliance University, Alliance School of Law, for their continuous support, encouragement, and academic guidance throughout the course of this research. Their unwavering assistance has been instrumental in the successful completion and submission of this paper.

References
1. Prasad MD, Menon CS. The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law. International Journal of Law and Information Technology. 2020;28(1):1-19.
2. Duraiswami DR. Privacy and data protection in India. Journal of Law & Cyber Warfare. 2017;6(1):166-186.
3. Saha S, Mukhopadhyay S. A new age of data privacy laws in India: review of Digital Personal Data Protection Act, 2023. IJLS. 2024;10:84-84.
4. Rai N. Right to privacy and data protection in the digital age—preservation, control and implementation of laws in India. Indian JL & Just. 2020;11:115-115.
5. Burman A. Will India's proposed data protection law protect privacy and promote growth? Washington (DC): Carnegie Endowment for International Peace; 2022.
6. Boyne SM. Data protection in the United States. The American Journal of Comparative Law. 2018;66(Suppl 1):299-343.
7. Determann L. Adequacy of data protection in the USA: myths and facts. International Data Privacy Law. 2016;6(3):244-250.
8. Digital Personal Data Protection Act, 2023 (India).
9. Information Technology Act, 2000 (India).
10. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).
11. Personal Data Protection Bill, 2019 (India).
12. Constitution of India, Article 21.
13. General Data Protection Regulation (EU) 2016/679.
14. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
15. Consumer Protection Act, 2019 (India).
16. E-commerce Rules, 2020 (India).
17. Health Insurance Portability and Accountability Act of 1996 (USA).
18. Children's Online Privacy Protection Act of 1998 (USA).
19. California Consumer Privacy Act of 2018 (USA).
20. Washington Privacy Act (USA).