Page 539 - 551 **DOI:** *https://doij.org/10.10000/IJLSI.112618*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 3

2025

A Comparative Study of Data Protection in the Digital Age between India and the United States

GOWSALYA R[1]

ABSTRACT

The digital era has brought rapid technological advancements, transforming personal data into a highly valuable resource. This study examines how data protection and privacy rights are upheld in the United States and India.. Both nations face challenges in protecting individuals' privacy as technologies like mobile apps, sensors, and online platforms increasingly collect, store, and use personal data. In India, privacy has gained recognition as a fundamental right, but laws specifically addressing data protection remain underdeveloped. This creates a technology-driven environment where data is widely shared and used. Meanwhile, the United States has a longer history of addressing privacy through specific laws and regulations, though these are often focused on particular industries rather than providing comprehensive protection. This study compares how the two countries approach privacy and data protection, examining their responses to issues like data collection, online behavior tracking, and misuse of personal information. It highlights the need for clear laws that protect individuals while supporting technological and economic growth.

Keywords: *Data Protection, Fundamental rights, Rights to privacy, United States, India*

I. INTRODUCTION

Technology is one of the essentials needed in a society. In today's world of technology, where everything is linked and privacy has become most important and sensitive,. Later on, it was merged into legal regulations as a fundamental in each individual liberty. These factors have led to technological advancements in a number of fields related to the management of personal data in the digital era. The United States was essential, and the results of its numerous laws, agreements, and standards regarding privacy are significant. Laws in the US, such as the 1974 Privacy Act, it denote rights and protection for individual information held by government agencies. There is always a need to defend privacy and data protection in a world where personal data is valued and more susceptible, while comparing the notion across nations will

[1] Author is an Assistant Professor at Central Law College Salem, India.

 [ISSN 2581-9453]

yield results regarding its extent and the efficacy of privacy and data protection.

II. MEANING OF DATA

The term "data" encompasses both real-world and electronic information. In the context of real-world information, data can refer to any factual information or observations collected through various means, such as surveys, interviews, or physical measurements.[2]

Conversely, digital data is the electronic form of information that is comprehensible by computers and other devices. It's made up of 0s and 1s, which are like the building blocks that computers use to store and process data.[3] Therefore, Electronic data refers to digital information stored and processed by computers or electronic devices. This type of data includes text, numbers, images, videos, and any other form of digital content.[4] Electronic data is often generated and collected through online interactions, sensor readings, transactions, social media activity, and more.

One key distinction between real-world data and electronic data is the medium through which they are collected and processed. Real-world data originates from physical observations or measurements,. The line between the two kinds of data is, however, getting more hazy in reality as more parts of our physical environment are being digitalized and as electronic devices gather information from interactions in the actual world.[5]

III. DATA PROTECTION

Data protection and privacy are closely related ideas that are necessary to preserving individual liberty and human dignity. In the digital age, individuals often share their data, both personal and non-personal, without a full understanding of the consequences. This issue is exacerbated by the pervasive use of electronic devices like smart phones and an increasing number of internet-connected gadgets. These technologies facilitate the rapid collection, storage, and transfer of data, often without explicit consent or awareness.[6]

As a result, there is an urgent need for robust frameworks that prioritise transparency, consent, and accountability in data management practices.[7]

---

[2] Joseph Antel et al., *"*Effective Competition in Digital Platform Markets: Legislative and Enforcement Trends in the EU and US", 6 *European Competition and Regulatory Law Review* 37 (2022).
[3] Egnyte, https://www.egnyte.com/guides/governance/digital-data (last visited April 20 2024).
[4] Law Insider, https://www.lawinsider.com/dictionary/digital-data (last visited April 20 2024).
[5] Ibid.
[6] Harriet Moynihan, "The Vital Role of International law in the framework for Responsible State Behaviour in Cyberspace" 6 *Journal of Cyber Policy 395-397* (2021).
[7] David Kuechler, " The Evolution of E-commerce Research: A Stakeholder Perspective", 6 *Journal of Electronic Commerce Research* 262-264 (2005).

 [ISSN 2581-9453]

Educating users about the implications of their online activities, promoting digital literacy, and implementing stringent data protection regulations can help mitigate these risks. Society may achieve a balance between privacy protection and technological innovation by encouraging a culture of responsible data usage and giving people more control over their information.[8]

Meaning of Data Protection

Data protection is widely regarded as one of the most abstract concepts in the realm of law, lacking a concise, one-line definition. Legal scholars describe "data protection" as an umbrella term encompassing all aspects of handling and processing personal data. Sweden's Data Act, the country's first data protection law, was passed in 1973, over fifty years ago, and went into effect the following year. This ground-breaking regulation forbade people and organisations from managing personal data on any information system without a license, and it was supervised by the Swedish Data Protection Authority.[9]

In Sweden, a nation renowned for its progressive stance, the Act was created in response to rising public concerns about the expanding gathering and storage of personal data in the late 1960s.[10]

Two fundamental ideas form the basis of data protection laws: "personal data" and "processing." These pillars serve as the cornerstone for the goals and tenets of these laws., warranting significant attention in their interpretation and application. The term "processing" is broad, covering the entire spectrum of activities within data protection, and must be interpreted expansively to ensure the protection offered by these laws is comprehensive and inclusive.[11]

IV. RIGHT TO PRIVACY

Privacy has evolved everywhere in one's individual life, and most importantly, it is the ability to keep information private; every citizen is entitled to privacy protection. But there is a limit to privacy and it is not always perfect due to the digital age of technology as of now a new world with higher information exchange, internet usage and its evolution has advantages and disadvantages, In August 2017 the apex judicial authority declared the "Right to Privacy" to be a fundamental right. People use social media to communicate and gather information from

[8] Supra note 1 at 394.
[9] Dhiraj R. Duraiswami, Privacy and Data Protection in India, 166 *Journal of Law & CYBER WARFARE* 169-72 (2017).
[10] Ibid.
[11] Umang Joshi, "Online Privacy and Data Protection in India: A Legal Perspective", 7 *NUALS Law Journal* 101-103 (2013).

others to build up their relationships easily. People's privacy has been used for several purposes in the same way the digital age serves as a place for conducting business, getting new information and pursuing their interests.

Data is generated everywhere and in almost everything we do in our daily life, which results in many benefits towards the data, although the information two ways, which we eagerly want to disclose and on the other hand, there have been many new apps that increase the depth of technological progress. In today's scenario, "people have control over how other people access technology and use their data". The Indian Constitution's Article 21 recognizes the "Right to Privacy" as a fundamental component and promotes fairness and openness regarding personal data. Interplay between data protection and its relation with the right to privacy.

The relationship between the right to privacy and data protection laws is undeniable and closely interconnected. While these concepts may differ in theory, they share a concrete link.[12]. The Court declared the right to privacy as an integral part of the right to life and liberty under Article 21 of the Indian Constitution, prompting the government to establish a data protection framework.[13]

In India, however, privacy jurisprudence is still evolving, and there is no clear definition of the right to privacy for data protection purposes. This ambiguity has both advantages and disadvantages. On one hand, it allows flexibility for courts to interpret privacy broadly, adapting to rapid technological changes. On the other hand, a lack of precision can create challenges in crafting effective legislation. A robust data protection law must clearly define privacy while allowing room for adaptability.[14]

The connection between privacy and data protection often revolves around the idea of "informational self-determination," which empowers individuals to control how, when, and to what extent their information is shared, Instead, effective regulations aim for balanced and regulated oversight. Historically, privacy has also been understood as the "right to be let alone," encompassing secrecy, anonymity, and solitude. Seminal works, such as those by Samuel D. Warren and Louis D. Brandeis, laid the foundation for this perspective, emphasizing the protection of personal thoughts, emotions, and creations from unwanted exposure.[15]

---

[12] Silvia Lucia Cristea & Viorel Banulescu, "The Right to Personal Data Protection. The Right to Privacy. A Comparative Law Approach", 64 *ANALELE STIINTIFICE ALE UNIVERSITATII ALEXANDRU IOAN CUZA DIN IASI STIINTE JURIDICE* 03-05(2018).

[13] KS Puttaswamy v. Union of India, 2019 (1) SCC 1.

[14] Orla Lynskey, "Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order", *63 International & Comparative Law Quarterly* 577-81 (2014).

[15] Edward J. Eberle, "The Right to Information Self-Determination", *Utah Law Review* 969-971 (2001).

However, advancements in technology and Big Data have blurred the lines, making even non-sensitive information potentially revealing when processed in specific ways. This highlights the need for adaptable and forward-looking data protection frameworks.[16]

V. INTERPLAY BETWEEN DATA PROTECTION AND ITS RELATION WITH THE RIGHT TO PRIVACY

There is no denying the intimate connection and interdependence between data protection regulations and the right to privacy. Despite their theoretical differences, these ideas have a tangible connection. The Supreme Court of India has emphasized how data protection rules are based on the acknowledgement of privacy as a fundamental right. According to Article 21 of the Indian Constitution, the Court ruled that the right to privacy is a necessary component of the right to life and liberty, which prompted the government to create a framework for data protection.[17]

However, India's privacy jurisprudence is still developing, and the right to privacy for data protection is not well defined. There are benefits and drawbacks to this ambiguity.. On one hand, it allows flexibility for courts to interpret privacy broadly, adapting to rapid technological changes. On the other hand, a lack of precision can create challenges in crafting effective legislation. A robust data protection law must clearly define privacy while allowing room for adaptability.[18]

The concept of "informational self-determination," which gives people the ability to decide how, when, and to what degree their information is shared, is frequently at the centre of the relationship between privacy and data protection. This concept aligns with democratic values but acknowledges that no law can guarantee complete control over personal data. Instead, effective regulations aim for balanced and regulated oversight. Historically, privacy has also been understood as the "right to be let alone," encompassing secrecy, anonymity, and solitude. This viewpoint was established by seminal publications like those by Samuel D. Warren and Louis D. Brandeis, which emphasised the need to shield private ideas, feelings, and creations from unwelcome publicity.[19]

But as technology and Big Data have advanced, the distinctions have become more hazy, and

[16] Eva Fialova, "Data Portability and Informational Self-Determination",8 *Masaryk University Journal of Law and Technology* 456-51 (2014).
[17] KS Puttaswamy v. Union of India, 2019 (1) SCC 1.
[18] Orla Lynskey, "Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order", *63 International & Comparative Law Quarterly* 577-81 (2014).
[19] Edward J. Eberle, "The Right to Information Self-Determination", *Utah Law Review* 969-971 (2001).

even non-sensitive data may become revealing if handled in certain ways. This highlights the need for adaptable and forward-looking data protection frameworks.[20]

A. Evolution of Data Protection Laws

1. Legislative framework of data protection in India

In India, the idea of privacy has its origins in long-standing customs and legal precedents, which illustrate its importance in many facets of life. Hindu scriptures that stressed privacy in private areas, such as the Ramayana, Manusmriti, and Arthashastra, penalised trespassing, interfering, or entering without permission. House building regulations mandated proper distances between houses and covered openings to ensure privacy. Additionally, secrecy in state affairs was upheld, with confidential decisions disclosed only on a need-to-know basis.

Muslim jurisprudence prioritized privacy in both cultural and legal norms, further distinguishing between the public and private domains. The Bible similarly emphasises privacy as an essential aspect of human dignity. Collectively, these references from ancient Indian traditions and global religious texts highlight that privacy, although not explicitly termed, was deeply ingrained in societal norms and legal frameworks, serving as a precursor to its modern legal recognition.

2. Constitution of India

The Indian Constitution's Preamble affirms the people's determination to establish India as a Sovereign, Democratic Republic and to guarantee its citizens equality, justice, liberty, and brotherhood. It was later acknowledged as the fundamental component of the Constitution after first not being regarded as such. It was adopted on November 26, 1949, and it embodies the framers' intention.[21]

In *Sajjan Singh v. State of Rajasthan*[22], Justice Mudholkar emphasised the structure of the written Constitution, which upholds fundamental rights and divides authority among three governmental entities. Chief Justice Sikri noted that while the Preamble cannot override clear constitutional language, it aids interpretation when ambiguity arises. Similarly, in *L.C. Golak Nath v. State of Punjab*[23], According to Article 368, the Preamble served as a guiding principle but was not a source of amending authority..

[20] Eva Fialova, "Data Portability and Informational Self-Determination",8 *Masaryk University Journal of Law and Technology* 456-51 (2014).
[21] A. Manoj Krishna, "Privacy", 41 *The Academy Law Review* 1-2(2000).
[22] *Sajjan Singh v. State of Rajasthan,* 1973 4 SCC 225.
[23] *L.C. Golak Nath v. State of Punjab* AIR 1967 SC 1643.

In Re *The Kerala Education Bill, 1957*[24], In keeping with constitutional goals, the Supreme Court invoked the Preamble to support the value of education in promoting ideas, opinions, and speech.

3. Indian Telegraph Act, 1885

Unauthorized entry into government telegraph offices and obstruction of authorities are punishable by up to a year in jail and/or a fine under Section 24 of the Act. Intentional damage to telegraph systems is punishable by up to three years in prison and/or a fine under Section 25 of the Act. The Act's Section 30. punishes dishonestly keeping misbelieved messages for up to two years in jail and/or paying a fine..[25]

4. The Indian Penal Code (IPC), 1860

Section 292 criminalises selling or possessing obscene materials. Section 509, Punishes insult to a woman's modesty or privacy with up to one year of imprisonment and/or a fine. [26]

5. The Indian Evidence Act, 1872

Section 122, provides Spousal privilege protects confidential communications, except in cases of offences between spouses. Section 126, Mandates attorney-client privilege, with some exceptions. Section 129, Prevents disclosure of confidential communication unless ordered by the Court. Section 130, Protects privacy by exempting third parties from producing documents unrelated to a case.[27]

6. The Code of Criminal Procedure, 1973

Section 26 States Cases under IPC Sections 376, 376(A-E) (e.g., rape) should be presided over by a female judge whenever possible. Section 164(2) states that Magistrates must inform accused persons that their confession is voluntary and may be used against them. Section 164(3) states that if the accused refrains from confessing, detention in police custody is not permitted.[28]

7. The Information Technology Act, 2000

Corporate negligence in preserving personal data that results in improper loss or gain is punishable under Section 43a. Violations of confidentiality in legitimate contracts are

[24] In Re. *The Kerala Education Bill,* A.I.R. 1958 S.C. 956
[25] Indian Telegraph Act, 1885 (Act 13 OF 1885), ss. 24, 25 & 30.
[26] The Indian Penal Code, 1860, (Act 45 of 1860), ss. 292 & 509.
[27] The Indian Evidence Act, 1872 (Act 1 of 1872), ss. 122, 126, 129 & 130
[28] The Code of Criminal Procedure, 1973 (Act 2 of 1974), ss. 26, 164(2) & 164(3).

 [ISSN 2581-9453]

punishable by up to three years in prison and/or a fine of up to ₹5 lakh under Section 72a.[29]

From its historical customs and cultural norms, India's right to privacy has developed, highlighting its significance for physical areas, personal dignity, and intangible elements like information and reputation. These values have been carried forward into modern legal frameworks, highlighting the balance between individual rights and societal needs. Privacy is deeply embedded in the constitutional framework, ensuring liberty, dignity, and equality. Judicial interpretations have consistently emphasized the importance of privacy as a guiding principle to uphold constitutional objectives and personal freedoms. Legislative measures address various aspects of privacy, such as protecting personal data, preventing misuse of confidential information, and safeguarding professional and personal relationships. These laws also guarantee the preservation of individual rights in both public and private domains, encourage gender-sensitive judicial procedures, and offer procedures to handle privacy violations..

8. Data Protection Bill, 2019

The 2019 Data Protection Bill sought to protect digital privacy with regard to personal information, create rules for the movement and use of such data, and promote trust between people and organizations that handle their data. Individuals were granted certain rights, such as the ability to request that erroneous, incomplete, or out-of-date personal data be corrected. The bill suggested establishing a Data Protection Authority to supervise and control how Indian-based businesses handle personal data.

9. Digital Personal Data Protection Bill, 2022

The updated Digital Personal Data Protection Bill of 2022 addresses problems in the previous, more complicated draft and focuses exclusively on personal data. This updated version introduces stringent penalties for non-compliance while easing cross-border data transfer restrictions, which could benefit major technology companies. It also simplifies compliance requirements for start-ups. The new law has a more flexible approach to data localization than the previous one, which required data storage within India. It promotes international commercial agreements and international cooperation by enabling the movement of data to worldwide destinations.[30]

[29] Protection of Civil Rights Act, 1955 (Act 22 of 1955), ss. 3 & 4.
[30] Divyanshi Kausal, "The Digital Personal Data Protection Bill, 2022" 3 *Jus Corpus Law Journal* 747(2023).

B. Legislative framework of Data protection in the United States

There isn't a consistent, standardized legal framework for data protection in the US.. Instead, it relies on various laws designed to protect individuals' data rights to the greatest extent possible. These laws are highly specific, targeting particular industries and issues, and have a limited scope. While this discussion cannot cover all federal and state-level data protection laws in order to evaluate the degree of protection offered to people in the United States, it will highlight important themes and cases.[31]

The idea of the "right to be left alone" is implied by the U.S. Constitution in addition to certain data protection legislation.. In *Katz v. United States*[32] The Supreme Court ruled that the Fourth Amendment shields people from government interference, not simply physical places, in a sweeping interpretation. The Court did not, however, specifically acknowledge privacy as a separate right.

It was in *Whalen v. Roe* that privacy was recognised as a separate fundamental right by the Supreme Court. The Court distinguished two essential components of privacy: the right of the individual to make decisions on important personal issues on their own and the right to prevent the publication of personal information. Since then, these ideas have impacted how the American legal system views privacy rights more broadly.[33]

1. Fair Credit Reporting Act (FCRA)

Retail credit bureaus and consumer credit agencies that have access to the credit histories of millions of Americans are governed by the Fair Credit Reporting Act. These organisations use a variety of background data to determine a person's creditworthiness. These credit scores are frequently used by banks and other financial institutions to approve loans. Because so much sensitive data is involved, there are serious privacy dangers in this sector.[34]

The FCRA introduced key protections for consumers, notably providing remedies against inaccurate credit reports. Before the Act, consumers had no way to challenge incorrect information or unauthorized disclosures from credit agencies. The FCRA requires these agencies to notify consumers about the information in their reports, allowing them to review and dispute it if needed.[35].

[31] Serge Gutwirth, Yves Poullet & Paul De Hert, Data Protection in a Profiled World 210 (Springer, Europe, 2010).
[32] Olmstead v. United States, 277 U.S. 438.
[33] Samuel D. Warren & Louis D. Brandeis, “Right to Privacy”, 4 *Harvard Law Review* 193 (1890).
[34] Fair Credit Reporting Act of 1970.
[35] Watwood v. Stone's Mercantile Agency, 194 F.2d 160 (D.C. Cir. 1952)

2. The Children's Online Privacy Protection Act (COPPA)

Since children are one of the greatest demographics of internet users today, the Children's Online Privacy Protection Act, which was passed in 1998, addresses the need to protect children's online privacy. Many websites for gaming, chatting, and education cater primarily to children, who often lack the awareness to understand the consequences of sharing personal information online. This makes them vulnerable to privacy breaches.

The Children's Online Privacy Protection Act, which governs the gathering, storing, and processing of children's personally identifiable information, is the result of the drive for stronger federal laws to protect children's privacy. The Act highlights how crucial it is to get parental approval before gathering this kind of information. Its creation was spurred by a Federal Trade Commission investigation into KidsCom.com, which revealed significant risks in how children's information was handled online. This highlighted the urgent need for clear regulations to protect children's privacy and involvement in data disclosures.

Websites and online services are required by the Children's Online Privacy Protection Act to notify parents and children about their data collection, storage, and processing practices. In addition to enforcing appropriate compliance standards for data security, it requires parental approval before collecting children's information and gives parents the ability to examine and limit it.[36] The Act classifies websites as "directed at children" if they target or appeal to children, and it defines "operators" broadly to cover all commercial online service providers. Names, contact data, social security numbers, and persistent identifiers (like cookies) are all considered personally identifiable information (PII). To avoid intrusions, operators must maintain confidentiality and put strong security measures in place, such as firewalls and encryption.[37]

3. Electronic Communications Privacy Act (ECPA)

One of the main pillars of privacy protection in the United States for a long time has been the Electronic Communications Privacy Act (ECPA). It was among the first legislation to provide a thorough framework for protecting the privacy of internet users. Concerns regarding third-party access to recorded conversations arose with the proliferation of emails and digital communication, particularly after courts determined that material freely given for commercial

[36] Dawn A. Edick, "Regulation of Pornography on the Internet in the United States and the United Kingdom: A Comparative Analysis", 21 *Boston College International & Comparative Law Review* 437 (1998)
[37] Thomas B. Nachbar, "Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character", 85 *Minnesota Law Review* 215(2000).

purposes was not protected by the Fourth Amendment..[38]

An Office of Technology report exposing the hazards to individual privacy in the digital age served as the impetus for lawmakers to adopt the ECPA in reaction to the growing use of digital communication. The Act sought to give electronic communications the same privacy protections as traditional letters. However, with rapid technological advancements since its enactment in 1986, the ECPA's relevance in addressing modern online threats has been increasingly questioned. This section explores the Act's origins and evaluates its effectiveness in adapting to current challenges.[39]

4. Health Insurance Portability and Accountability Act (HIPAA)

People's ownership over their personal information, including their medical records, is guaranteed by the right to privacy. The purpose of the Health Insurance Portability and Accountability Act is to prevent unauthorized disclosure of patient health information. Healthcare practitioners are required by HIPAA to get patient consent before disclosing any personal health information. The Act's main provisions include:

- When people request it, healthcare professionals are required to furnish them with protected health information in a timely manner.
- PHI may be disclosed for treatment and payment purposes.

Despite not acknowledging privacy as a basic right, HIPAA offers robust safeguards against unauthorized disclosure of private health information. It recognizes how crucial it is to protect medical records, which are extremely private and intimate..[40]

The Health Insurance Portability and Accountability Act governs certain connections, mostly between "covered entities," such as health plans, health maintenance organizations, and healthcare providers. These entities must comply with the Act's provisions and appoint a compliance officer to ensure the privacy of patient information. Business associates, such as lawyers and accountants, also have access to health data when necessary for their work. The Act does not prevent the sharing of health information for legitimate purposes, such as coordinating patient care, but it aims to curb the misuse of medical information.

5. The Federal Trade Commission Act

The CAN-SPAM Act, Gramm-Leach-bliley Act, Equal Credit Opportunity Act, and Fair Credit

[38] Electronic Communications Privacy Act of 1986.
[39] Ibid.
[40] Samuel D. Warren & Louis D. Brandeis, Right to Privacy, 4 Harvard Law review 193 (1890-1891).

Reporting Act are just a few of the federal privacy laws that the Federal Trade Commission, which was founded by the Federal Trade Commission Act of 1914, is empowered to implement. Section 5 of the Act gives the FTC the authority to combat unfair competition and deceptive conduct that affect commerce. The Act also enables the Commission to penalise entities for violations such as false advertising, which can harm consumers. To safeguard consumer privacy, the Federal Trade Commission employs a range of tools, including policy initiatives and educational efforts aimed at both consumers and businesses, raising awareness of evolving data privacy issues. With its extensive experience in data protection, the Commission also works with federal, state, and international agencies to help improve the country's data protection framework.[41]

6. Video Privacy Protection Act

The goal of the 1988 Video Privacy Protection Act is to safeguard individuals' privacy when it comes to renting, buying, or receiving video content. The Act prevents video service providers, like streaming platforms, from disclosing personal information about users, such as what videos they've rented or watched, without their consent. Despite changes in technology, the Video Privacy Protection Act remains relevant because courts have interpreted it broadly. For example, in a case involving Hulu, a court ruled that online streaming services fall under the same category as traditional videotape providers.

However, there have been concerns with the Act's wording, especially regarding who can sue under it and what qualifies as "personally identifiable information" (PII). The VPPA also allows some exceptions. For example, providers can share information if it’s necessary for regular business operations. However, the Act doesn’t specify penalties for violations, as shown in the case Austin-Spearman v. AMC Network Entertainment LLC[42].

In a landmark case, Camfield v. City of Oklahoma City[43],When police took a movie rental record without a warrant, they were in violation of someone's VPPA rights. The significance of privacy rights in video rentals was underscored by the court's decision to award the individual $2,500 for violating the Act.

VI. CONCLUSION

Given their distinct legal, cultural, and technological environments, India and the US take rather different stances on data protection in the digital age. With the passage of the Personal

[41] The federal Trade Commission Act 1914.
[42] Austin-Spearman v. AMC Network Entm't, LLC, 98 F. Supp. 3d 662.
[43] Cf Camfield v. City of Oklahoma City, 248 F.3d 1214.

Data Protection Bill, 2019, India has made strides in recent years toward a more organised and thorough data protection system with the goal of offering strong protection for personal data. This measure, which is impacted by foreign norms like the European Union's General Data Protection Regulation, acknowledges the right to privacy as a basic right under Article 21 of the Indian Constitution.

The Personal Data Protection Bill, which reflects worries about data sovereignty and national security, places a strong emphasis on data localization and mandates that some sensitive data be kept inside India's borders. Additionally, India gives people the right to access, amend, and remove their data and requires their express consent before processing it.

In contrast, the US lacks a cohesive national framework and instead uses a sectoral and disjointed approach to data protection. The Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, and the Electronic Communications Privacy Act are among the industry-specific legislation that regulate privacy protection in the United States. These laws do not guarantee individuals broad, cross-sector privacy protection; instead, they only offer protection in certain areas, such as credit data, health information, and children's internet privacy.

The main distinction is in how individual rights and data sovereignty are handled. The sect oral model of the United States, where data protection varies by industry and is more focused on commercial interests than comprehensive individual protection, contrasts sharply with India's emphasis on data localization and a rights-based approach. Because there isn't a single federal law in the US, there is fragmentary legislation that is frequently criticized for not being enough to address the problems of the digital age, particularly in light of the emergence of big data, artificial intelligence, and ubiquitous surveillance technology.

Additionally, the US model favors technical advancement and economic interests, which frequently gives businesses greater latitude in managing customer data. India's developing framework, on the other hand, places more of an emphasis on personal data ownership for individuals and acknowledges privacy as a fundamental right that needs to be safeguarded in the face of swift technological advancements. While both countries must adjust their legal systems to the digital era, India's focus on a human rights-based, holistic framework provides a more thorough approach to data protection, while the US sect oral model might find it difficult to keep up with the difficulties presented by new technologies.

*****

 [ISSN 2581-9453]