A Comparative Analysis of Data Privacy Laws across India, EU and USA

By ***Suveer Dubey***

1st Year Masters Student, Amity Institute of Advanced Legal Studies, Noida, Uttar Pradesh, India

Introduction

Statement of Problem:

The research paper aims to address the pressing issue of data privacy laws in India and the European Union (EU) to comprehensively examine the challenges, disparities, and potential areas of convergence within these two distinct regulatory frameworks. In an era marked by the global exchange of personal data and heightened concerns over data breaches and privacy violations, it is imperative to understand the intricate dynamics of data protection in both regions. This research seeks to identify the key problem areas, including discrepancies in legislation, enforcement, and the practical implications for businesses and individuals operating across these jurisdictions. By shedding light on these issues, the study will contribute to a more profound comprehension of the evolving landscape of data privacy laws and their potential impact on international data flows and cross-border business operations.

Research Questions:

a) Whether there are significant differences in the legal frameworks of India and the EU regarding data privacy, and if so, what are the key distinctions?
b) Whether India has any enforcement regulation in case of an invasion of the right to privacy?
c) Whether the present Indian legislative framework effective in addressing the legal issue of data breaches by international entities?
d) Whether data protection laws in India as effective as those in the EU and US?

ISSN 2455 2437
Volume 10 Issue 1 – January February 2024

Research Objectives:

The primary objective of this study is to investigate the impact of data protection regulations on international data flows, with a focus on understanding the differences and similarities in data protection scenarios in India, the European Union, the United States, and the United Kingdom. This research aims to provide insights into how these diverse regulatory frameworks influence data privacy, cross-border data transfers, and business practices, and to evaluate the effectiveness of safe harbor agreements between the US and EU. By achieving this objective, the study will contribute to a deeper understanding of the global data protection landscape and facilitate informed decision-making for individuals and organizations engaging in international data exchanges.

Hypothesis:

European Union's data privacy regulations are more stringent and comprehensive compared to those in India, primarily due to the European General Data Protection Regulation (GDPR).

Indian laws are not comprehensive and sufficient in terms of protection and enforcement as compared to the EU and USA

Origin and Development of Privacy and Data Protection

History of Privacy:

Across the annals of history, the concept of privacy has consistently held a pivotal role in human existence.[i]Safeguarding a degree of personal privacy has remained a steadfast element of human societies, evident in its recognition in religious texts and legal frameworks. An illustrative example is found in the biblical narrative of Adam and Eve, who, after consuming the forbidden fruit, instinctively covered their bodies with leaves to preserve their privacy. This early account underscores the enduring recognition of the fundamental need for privacy among humans, tracing back to the earliest epochs of human civilization.

Maintaining databases is not as challenging a task as preserving their integrity, and in this era[ii] the predominant discourse revolves around innovating effective methods for data protection.

With technological advancements, there has been a shift in crimes, with a significant portion now perpetrated by professionals through easily accessible mediums such as computers and electronic devices. Criminals can effortlessly access secured information with a single click, and the insatiable desire for information is fuelling the growth of cybercrimes[iii].

This poses a significant concern for businesses, financial institutions, and governmental bodies, all grappling with the substantial task of providing ample protection for their extensive databases. In the absence of specific and stringent laws regarding data protection, wrongdoers are honing their skills with each passing day. While the modern world has undoubtedly simplified our lifestyle, it has also introduced certain anomalies, leading to the inadvertent disclosure of data.

Data Protection and Privacy & Need for Protection:

In today's digital landscape, data protection and the preservation of the Right to privacy have assumed critical significance. The proliferation of technology has given rise to diverse forms of data, amplifying the complexities of ensuring adequate safeguards for personal information. This underscores the imperative for robust data protection measures capable of effectively shielding sensitive data from potential misuse, theft, or unauthorized access by malicious online actors.

Every day, an extensive volume of sensitive data, encompassing personal information, financial records, and even medical histories, is generated, and processed. Yet, this abundance of data necessitates the implementation of effective protection measures to uphold privacy and forestall any unauthorized access or misuse. Recent years have witnessed heightened concerns regarding the security of sensitive data, driven by high-profile breaches that exposed the personal information of millions.[iv] This has contributed to an increased awareness of the crucial role in protecting sensitive data from cyber threats like hacking, identity theft, and phishing attacks. It's worth noting that the concepts of data protection and data privacy have sometimes been misconstrued within the broader context of privacy.

India, the second-most populous nation in the world, recently underwent a technological revolution as a result of the massive adoption of web-based services like social media and e-

commerce platforms. The economy has benefited greatly from this shift towards digitalization, including higher production and efficiency. However, it has also made people and organizations more vulnerable to fresh threats from online criminals.

In recent years, there has been a growing demand for a robust data protection framework in India, particularly following the significant 2017 Supreme Court ruling in K.S. Puttaswamy v. Union of India1 ("Puttaswamy")[v]. This ruling affirmed that the right to privacy is a fundamental right under Articles 14, 19, and 21 of the Indian Constitution.[vi] These demands spurred the formation of the Srikrishna Committee[vii], which initially drafted India's first dedicated data protection legislation. Over time, this draft has undergone numerous revisions, with the most recent effort resulting in the Digital Personal Data Protection Bill, 2022 ("DPDP").

The Indian government has introduced substantial changes to the previous version of the data protection bill, which had drawn significant inspiration from the European Union's ("EU") General Data Protection Regulation, 2016 ("GDPR") a widely acknowledged global standard for data privacy among lawmakers.

Legislative Framework of India, European Union And USA

Indian Law:

Our constitution addresses the matter of privacy within the framework of Article 21, but its interpretation has proven to be inadequate in providing comprehensive protection for data. In 2000, the legislature made an effort to encompass privacy concerns related to computer systems under the IT Act of 2000. This legislation includes specific provisions designed to safeguard stored data. In 2006, the legislature also introduced the 'Personal Data Protection Bill' with the aim of securing individuals' personal information.

Under the IT Act of 2000[viii]:

- Section 43 offers protection against unauthorized access to computer systems, imposing substantial penalties, including fines of up to one crore. It covers unauthorized activities like downloading, extraction, and copying of data. Clause 'c' of this section penalizes

the unauthorized introduction of computer viruses or contaminants, and clause 'g' prescribes penalties for aiding unauthorized access.

- Section 65 pertains to computer source code. Deliberate actions such as concealing, destroying, altering, or causing others to do so may result in penalties, including imprisonment or fines of up to 2 lakh rupees, safeguarding against tampering with computer source documents.

- Section 66 provides protection against hacking. Hacking, as defined in this section, involves intentional acts aimed at causing wrongful loss or damage to any individual, with knowledge that such loss or damage will occur to any person. If information residing in a computer resource is destroyed, deleted, altered, or its value and utility diminished, the section imposes penalties, including imprisonment for three years or fines of up to two lakh rupees or both on the hacker.

- Section 72 safeguards against breaches of confidentiality and data privacy. It specifies that anyone granted powers under the IT Act and associated rules to access electronic records, books, registers, correspondence, information documents, or other materials but discloses them to another person, shall face penalties, which may include imprisonment for up to two years or fines of up to one lakh rupees, or both.

The Indian Penal Code primarily deals with offenses that were anticipated until the last decade but does not encompass provisions for addressing the emerging realm of data-related crimes that have become increasingly prevalent today.

The 'Personal Data Protection Bill, 2006'[ix] takes inspiration from foreign laws and was introduced in the Rajya Sabha on December 8th, 2006. The bill's objective is to establish safeguards for personal data and information collected for specific purposes by one organization, preventing its utilization by other entities for commercial or any alternative purposes.[x] Furthermore, it grants individuals the right to seek compensation or damages in

cases where personal data or information has been disclosed without their consent. The bill also addresses related matters and issues incidental to its core provisions.

English Law:

The origins of data protection laws within the European Union (EU) have a long history dating back to the 1980s. In response, the EU introduced regulations in 1995 with the Data Protection Directive. This directive was later succeeded by the GDPR, a comprehensive regulation designed to enhance individual privacy rights and unify data protection regulations across the EU.[xi] Adopted in 2016 and enforced since May 2018, the General Data Protection Regulation (GDPR) stands as the primary legislative framework for data protection law in the European Union. Personal data, according to the GDPR, refers to any information related to an identified or identifiable natural person.

The Data Protection Act (DPA) of the United Kingdom was initially formulated by the parliament in 1984 and subsequently replaced by the 1998 DPA[xii]. This legislation is primarily designed to safeguard and ensure the privacy of individuals' personal data in the UK. It encompasses information that can identify a living person, including details such as names, birthdates, anniversary dates, addresses, telephone numbers, fax numbers, and email addresses. The scope of the Act is limited to data held or intended to be held on computers or other automatic processing equipment, as well as information stored in a relevant filing system.

Under this Act, entities and individuals responsible for storing personal data are required to register with the information commissioner, a government official appointed to oversee the implementation of the Act. The legislation imposes constraints on the collection of data, stipulating that personal data can only be obtained for specified and lawful purposes. Furthermore, such data shall not undergo further processing incompatible with the initially stated purpose or purposes. The Act emphasizes that personal data must be adequate, relevant, and not excessive concerning the specified purpose or purposes for which they are processed.

American Law:

The United States' legal system has undergone significant transformations over its history, especially in the context of data protection. In the current digital age, privacy and security have

gained paramount importance, and data protection in the United States is governed by a collection of laws that encompass a diverse range of subjects, including insurance, computing, children's privacy, and the safeguarding of sensitive personal health information[xiii]. These laws address every facet of privacy and are spread across different pieces of legislation.

At the federal level, the United States has a series of laws dedicated to data protection, including:

- The Privacy Act of 1974
- The Rights to Financial Privacy Act of 1978
- The Electronic Communications Privacy Act of 1986
- The Privacy Protection Act of 1980
- The Computer Matching and Privacy Protection Act of 1988
- The Electronic Communications Privacy Act of 1986
- The Cable Communications Policy Act of 1984
- The Computer Security Act of 1987

While both the United States and the European Union share a common goal of enhancing the privacy protection of their citizens, they adopt distinct approaches to privacy. The United States follows a sectoral approach, incorporating a combination of legislation, regulation, and self-regulation. In the U.S., data is categorized into various classes based on utility and significance, with each class receiving a varying degree of protection[xiv].

To establish a more stable framework for data protection laws in the United States, several Acts have been enacted. For instance, the Privacy Act of 1974[xv] was introduced, outlining standards for determining the reasonability, ethics, and justifiability of government agencies comparing data across different databases. Additionally, the Electronic Communications Privacy Act was implemented to restrict the interception of electronic communications and prohibit access to stored data without the consent of the user or the communication service. These legislative measures reflect the U.S. commitment to addressing privacy concerns through a nuanced and sector-specific regulatory approach.

Comparative Analysis of Data Protection

***Introduction*:**

The Several law for Data protection in the EU, GDPR is the most important regulation which has a huge impact in terms of data protection. It was proposed in 2016 and adopted on the 25th of May 2018.

In India the Proposed legislation has 6 chapters and a total of 30 sections deals with the India does not have comprehensive data protection law, but the Recently Proposed Digital Data Protection Bill, 2022 is a set of regulations for data protection.

The United state has a bunch of data protection laws on the federal and state level.

Definition of Data:

In EU, GDPR Covers the Definition of Data in an exhaustive form not only personal data but also include sensitive personal data[xvi]. It defines Personal Data as the information relating to an identified natural person, identified by name, identification number, location data and online identifier, and specific factor to physical, physical, genetic, mental, economic, cultural, or social identity.

In India, the bill covered the definition of Personal data as - any data about an individual who is identifiable by or in relation to such data, this definition is complex to define[xvii].

In USA, CCPA defines "Personal Information as the "information that identifies directly or indirectly a particular consumer or household.

Cross-border data:

In EU, the GDPR mentions the exhaustive procedure, code of conduct, certificate mechanism, and rules for the cross-border flow of data and the strength of data collected in the country's local servers, which means Data Localisation.

In India, The DPDPB, 2022 incorporates a provision for cross-border data transfers, stipulating that entities must seek permission to utilize data in such circumstances.

In USA, only applicable to the entities doing business in California that collects consumer data or personal information jointly or alone or with other, the business of $25M+.

***Exemptions*:**

In EU, the GDPR includes an exemption that allows data to be processed for national security purposes[xviii], and there is also an immigration exemption for cases involving immigration matters where there may be a potential threat or security concern.

In India, The Bill includes the following exemptions:

- Exemption to enforce any legal right.
- Exemption for cases related to a court or tribunal.
- Exemption for matters related to the prevention, detection, or investigation of certain interests.

In USA, The CCPA categorically does not apply when other specified privacy laws apply, such as information covered by the Health Insurance Portability and Accountability Act of 1996.

The first hypothesis of the research "despite the efforts of comprehensive data protection legislation in form of various data protection bills India still lacks an adequate set of laws and regulation for the data protection" the hypothesis set is not proven correct, because India do have the legislation for the data protection. The second hypothesis "India lacks Indian laws are not comprehensive and sufficient in terms of protection and enforcement as compared to EU and USA" the hypothesis is proven partially correct; India do have the enforcement mechanism for the data protection.

Conclusion

The swift progression of technology has elevated data protection to a pivotal facet of privacy in India. With an increasing number of individuals utilizing the internet and digital devices, copious amounts of personal and sensitive data are generated. The significance of data protection has become paramount in the country, granting individuals control over their lives and shielding them from unwanted intrusions. This ensures the freedom to express opinions

without fear of judgment or reprisal. The evolution of privacy as a legal right is reflected in Article 21 of the Indian Constitution, recognizing the right to privacy as a fundamental right, safeguarding personal liberty and life.

While India evolves into a digitally empowered society and a knowledge-based economy, the Supreme Court's acknowledgment of the right to privacy as fundamental in the case of Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others is noteworthy. Presently, India lacks a comprehensive data protection law. The Personal Data Protection Bill, 2018, and its revised version, the Personal Data Protection Bill, 2019, aim to establish a framework for data management ensuring privacy protection. Despite defining crucial terms and incorporating regulations for consent, data fiduciary relationships, and enforcement, both versions of the proposed bill have yet to materialize into law.

The Digital Personal Data Protection Bill of 2022[xix] emerges as a legislation poised to govern personal information in India, necessitating adherence to its stipulations by all entities handling personal data of Indian individuals. This proposed legislation aligns with international standards for data privacy and protection, drawing parallels with the General Data Protection Regulation (GDPR). Emphasizing the importance of obtaining informed consent before collecting and utilizing personal information, the bill seeks to fortify individuals' rights in the digital landscape.

Recommendation

The Digital Personal Data Protection Bill of 2022 marks a substantial stride in regulating the collection and processing of personal data in the digital domain. Its primary goal is to empower individuals with greater control over their personal data and to hold companies accountable for their handling and utilization of such data. Notably, the bill introduces increased penalties compared to its predecessor and broadens the scope of data subjects' rights. While some adjustments are needed for the bill's implementation, its overarching objective is to establish a safer and more secure digital environment.

The DPDP Bill of 2022 necessitates a revaluation of the definition of personal data. This is essential because both the previous bill and internationally recognized regulations like the GDPR and CCPA provide comprehensive definitions specifying the types of information falling under this classification. The GDPR, for instance, includes provisions for data localization, which India could adopt to effectively monitor data within its borders.

Concerns about the internet's impact on children have grown, presenting a psychological challenge in determining the appropriate age for online activities. Both the GDPR and CCPA have set the age range for children at 13-16 years old. The DPDP Bill extends this scope by including children up to the age of 18[xx]. Recognizing the growing significance of protecting sensitive personal data, which encompasses information like DNA samples, healthcare records, and credit card details, is crucial. However, the current DPDP Bill falls short in acknowledging the importance of safeguarding sensitive personal data. Therefore, a revision of the bill is necessary to align it with the GDPR and CCPA, both of which emphasize the importance of protecting such sensitive information.

Bibliography

Primary Sources:

- Indian Penal Code,1860
- The Constitution of India,
- Information Technology Act 2000
- Personal Data Protection Bill 2006
- Personal Data Protection Bill 2018
- Personal Data Protection Bill 2019
- Personal Data Protection Bill 2021
- Yashraj Bais, Privacy and Data Protection in India: An Analysis, International Journal of law and Management and Humanities, Volume 4 issue 5, 2021
- Solove, D. J. A Taxonomy of Privacy. University of Pennsylvania Law Review 2006, 154 (3), 477-560

- Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, JSTOR, Volume 53 no. 4, 2011
- M. R Konvitz, Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No. 2. (1966) p. 272
- H Nissenbaum,. A Contextual Approach to Privacy Online. Daedalus, 140 (4), 32-48 2011

Web sources:

- https://journals.sagepub.com/
- https://rgnul.ac.in/
- https://www.nlb.gov.sg/
- https://www.researchgate.net/

Endnotes

[i] Solove, D. J. A Taxonomy of Privacy. University of Pennsylvania Law Review 2006, 154 (3), 477-560
[ii] Konvitz, M. R.: Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No. 2. (1966) p. 272
[iii] H Nissenbaum,. A Contextual Approach to Privacy Online. Daedalus 2011, 140 (4), 32-48
[iv] Nivedita Baraily, An Analysis of Data Protection and Privacy Law in India
[v] K.S Puttuswamy Vs Union of India, (2017) 10 SCC 1
[vi] The Constitution of India
[vii] https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy (last visited 10-10-2023)
[viii] Information Technology Act of 2000
[ix] Personal Data Protection Bill, 2006
[x] Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines) Rules, 2011, Gazette of India (Apr. 11, 2011),
[xi] European Data Protection Supervisor, Handbook on European Data Protection Law (2018), https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.
[xii] Hustinx, P., EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf
[xiii] Robert Hasty Et.al, Data Protection Law In USA, Advocates for International Development, https://www.neighborhoodindicators.org/sites/default/files/coursematerials/A4ID_DataProtectionLaw%20.pdf
[xiv]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf, accessed on 20/09/2023
[xv] Privacy Act of 1974
[xvi] Section 4 (1) of GDPR
[xvii] Section 4 of The Digital Personal Data Protecion Bill, 2022
[xviii] Article 26, GDPR
[xix] The Digital Personal Data Protection Bill of 2022

[xx] Article 8, Conditions applicable to child's consent in relation to information society services, GDPR