Library Progress International
Vol.44 No. 3, Jul-Dec 2024: P.9853-9860

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

An Analysis of Data Privacy Laws: National & International Perspective

Dr. Keshav Madhav[1]; Dr. Papiya Golder[2]; Maitrayae Sadhu[3]; PreyasiDutta[4]; Dr. Annirudh Vashishtha[5]; Dr. Manisha Madhav[6]

[1]Assistant Professor, School of Law, UPES,Dehradun.
[2]Associate Professor, Brainware University,Kolkata.
[3] Assistant Professor, Brainware University,Kolkata.
[4]Assistant Professor, Brainware University,Kolkata
[5] Assistant Professor (SG), School of Law, UPES,Dehradun.
[6]Assistant Professor (SS), School of Law, UPES,Dehradun.

How to cite this article: Keshav Madhav;Papiya Golder; Maitrayae Sadhu; Preyasi Dutta; Annirudh Vashishtha; Manisha Madhav (2024) An Analysis of Data Privacy Laws: National & International Perspective. *Library Progress International,* 44(3), 9853-9660.

Abstract

Most industries, especially the IT related sectors, have experienced colossal growth and the production of information at an incredibly fast rate, making data protection laws an essentialrequirement across national and international realms. This paper aims at comparing the changes in data protection laws and analysing the distinctive features of various national lawsand global standards. It presents important global regulations, including the GDPR in the EU,the CCPA in the USA, and other key national frameworks. Moreover, it considers recent and future changes in the cross border data flows, the nature and scope of harmonisation by International organisations and the consequences brought to the business entities and individuals. Through evaluating these aspects, the paper intends to present systemic analysis as to the current status of data protection legislation and their effectiveness in advancing dataprotection internationally.

KEYWORDS: DATA PRIVACY, GDPR, CCPA, CROSS-BORDER DATA FLOWS, INTERNATIONAL DATA

Introduction

As the society shifts to digitalized, intrinsic privacy has transformed thus requiring frequent and effective data privacy laws. As a result of increased dependencies on the internet and othersocial platforms, business, and general human interactions, a lot of individual data is being produced, assembled, and analyzed in the current world. However, this increased generation ofdata has led to questions regarding the privacy of the individual and abuse of his/her personal information.

Governments at the national level and the international organizations have not remained idle and have developed and amended laws on data privacy in a bid to protect personal informationof the citizens. These laws seek to dictate how data is captured, processed, used and transmittedto other parties, and give individuals the control over their data and guard them against the viceof data usage breach. Several of these regulations have emerged as some of the most influentialones in recent years such as the General Data Protection Regulation enacted by the European Union, or the California Consumer Privacy Act enacted in the United States.

The GDPR was enacted in 2018 and is considered the toughest data protection law globally. Isuggest that it offers detailed provisions on how data should be protected, set significant consequences for violations, and highlights the data subjects' control over their data. The CCPA is another law passed in 2020 that is somewhat comparable to GDPR within the state ofCalifornia, which provided consumers with control over their personal

information, along withcreating significant responsibilities for businesses.

Besides these widely known examples, the overwhelming number of the countries have primary data protection systems that exist due to the various legal, cultural, and economic conditions. Also, various global organizations like the Organization for Economic Co- operation and Development (OECD) as well as the International Organization forStandardization (ISO) have been striving to establish a common alignment of data privacy as a way in the global transfer of data while protecting the same information.

Consequently, the purpose of this paper is to give clarification of data privacy laws from the national and international standpoint. This will look at the basics of the said laws, thedifficulties of its implementation and enforcement and the pursuit of the continuous process ofthe harmonization of these laws around the world. Hence, this paper aims to concentrate on

explaining the trends towards regulation of data privacy and its impacts on individuals, companies, and governments in the connected World.

Major Data Privacy Laws

1. GDPR – General Data Protection Regulation – is a regulation in EU law untouched by Brexit.

Overview: The GDPR has come into force on the May 25th, 2018 and it is widely regarded asthe most advanced data protection law on the global level. It operates across the entire EU territory and concerns the entities that deal with the EU citizens' personal data regardless of the organization's location.

Key Provisions:

I. Data subject rights: Three are; the right of access, the right to rectification, right toerasure and right to data portability.

II. Consent: Invokes a principle of data protection for which consent is precise andimperative to the processing of protocols.

III. Data breach notification: This means that organizations are required to inform theauthorities if a data breach has occurred within a time span of 72 hours.

IV. Penalties: Penalties may not exceed €20,000,000 or 4% of the companies' totalworldwide turnover in the fiscal year preceding the decision.

2. CCPA—California Consumer Privacy Act – USA

Overview: Since 1 January 2020 the CCPA provides new rights to California residents concerning their personal data as well as various requirements for businesses which process and share this data.

Key Provisions:

I. Consumer rights: This holds the right to obtain information as to the processing of thedata, the right to erasure and the right to opt-out of data selling.

II. Data disclosure: The data collected by businesses have to be explained in terms of thecategories of personal data and their purposes.

III. Penalties: Sanctions for the failure to abide by the agreements are prescriptive and involve monetary fines of up to $7,500 for each of an intentional violation and $ 2,500for an inadvertent violation.

3. Canada's Schedule 1 Personal Information Protection and Electronic Documents Act(PIPEDA)

Overview: PIPEDA was passed in the year 2000 to regulate the collection, use, and disclosure of

customer's personal information by the private sector companies that are involved in commercial business throughout Canada.

Key Provisions:

I. Fair information principles: Accountability, identification of the objectives, use ofconsent, limiting data collection, as well as various forms of protection.

II. Rights of individuals: Comprises the right of access to the information concerning theperson and the opportunity to receive this information, as well as contest it.

III. Penalties: The Privacy Commissioner of Canada can sue organizations that are notcompliant; such organizations might end up being charged steep penalties.

4. Data Protection Act 2018 – United Kingdom

Overview: Although this act works together with the GDPR in the UK, it has extra provisionsas well as some aspects not prohibited by the GDPR.

Key Provisions:

I. Enforcement: Establishes the nature of powers that Information Commissioner's Office(ICO) has as regards enforcement.

II. National security: Some of freedoms of speech include; Exemptions: Security anddefense of a country.

III. Penalties: Relates to GDPR penalties with fines of up to £17. 5 million or 4% of theannual turnover across the globe.

5. That is why the Personal Data Protection Act (PDPA) has been established in Singapore.Overview: Implemented from 2014, the PDPA sets the minimum framework of data protectionlaw in Singapore as the rules over the collection, use, and disclosure of personal data by variousorganizations.

Key Provisions:

I. Consent: The consent for the collection, use or disclosure of personal data must be givenby the organization.

II. Access and correction: Data subjects have the right to request the information about thedata processing operations and the right to request the correction of the data concerninghim or her.

III. Penalties: Failure to adhere to the policies leads to fines of up to SGD 1 million.

6. LGPD – Lei Geral de Proteção de Dados – Brazil

Overview: In force since August, 2020, the LGPD is Brazil's general data protection regulationbased on the GDPR aiming to control the treatment of identifiable information.

Key Provisions:

I. Data subject rights: Subsumes rights as those under the GDPR such as the right ofaccess, right of rectification, right to erasure, and right to data portability.

II. Legal bases for processing: Legal grounding for the processing of the personal dataprovided by the GDPR includes consent and legitimate interest.

III. Penalties: PENALTIES can be up to 2% of a companies' turnover in Brazil but arecapped at R$50 million per infringement.

All these laws combined create a very constrictive, dynamic environment of data privacy regulation around the world which although has different priorities and strategies of its own shares the same objectives of protecting personal data and acknowledging the rights of citizens.

Contribution of Indian Judiciary Towards Data Privacy

Indian judiciary has been central in influencing the general provisions of the data privacy lawsin the country. They have been quite instrumental in establishing the right to privacy as a fundamental right as well as laying down precedents for legislation and regulation. Some of

the significant contributions of the Indian judiciary in this regard are:Some of the significant contributions of the Indian judiciary in this regard are:

1. In Puttaswamy vs Union of India AIR 2017 Scrutiny of the case made a clear revelation thatthe verdict was in the favour of the Petitioner.

Landmark Judgment: In a recent landmark judgement the Honourable Supreme Court of Indiahas held the Right to Privacy under Article 21 of the Constitution of India as fundamental right.

Implications: This judgment was a start to all the laws and regulations that have to do with privacy issues. It pointed out the importance of the efficient legislation in the sphere of data protection for people's privacy in the context of the use of the Internet.

2. Shreya Singhal vs. Union of India 2015

Landmark Judgment: Section 66A of the Information Technology Act, 2000 was unconstitutional as it was obscene, Capacious and arbitrary in that it violated freedom of speechand expression as guaranteed under the constitution.

Implications: This case set a focus on the trade-off between security and privacy, and also showed that the judiciary safeguards persons'' rights from expanded legislations' clampdown.

3. Aadhaar Judgment (2018)

Landmark Judgment: Delivering a divided judgment on the Aadhaar scheme, the SC gave a green signal to the Aadhaar Act though with certain riders in the use of Aadhaar number especially with reference to private parties.

Implications: The judgment also underlined strong requirements for data protection measures while stressing the priority of the consent and purpose limitation within usage of the biometricand other personal data.

4. WhatsApp Privacy Policy Case

Ongoing Cases: The Delhi High Court as well as the Supreme court have been involved in cases that seek to stop social media applications such as WhatsApp from infringing on people'sprivacy through implementation of polices that violate the privacy of the people. The judiciary

has been quite active in this respect and demanding compliance with data protection standardsin particular regard to the sharing of users' data with parent companies.

Implications: These cases depict how the judiciary is ever willing to oversee the operations ofthe technological industries and check whether or not they are meeting India's data protectionstandards.

5. S. K. Puttaswamy (Retd. Justice) & Anr. IN THE SUPREME COURT OF INDIA CriminalOriginal Bail Application No. 24 of 2013 Arjun Singh @ Julie vs. Union of India & Ors. (2021)

Landmark Judgment: Concerning the Pegasus spyware scandal, the Supreme Court of India directed **the** formation of the committee for the alleged misuse of spyware on Indian citizens.

Implications: This case clearly illustrates the work of the judiciary in handling modern issues of privacy, particularly those that result from state spying and cybercrime**.**

Legislative Influence

In the case of legislative initiatives towards data protection, the judiciary's proclamations haveplayed a role to a large extent in India. The Personal Data Protection Bill, 2019 now the DigitalPersonal Data Protection Bill, 2022 has been drafted considering the certain judicial pronouncements particularly the recognition of right to privacy.

Balancing Act

The Indian judiciary has also attempted to uphold personal liberties amidst other countervailingrights and interests like security of a nation and order. This tug of war is seen in different decisions where the judiciary has urged for vigorous protection and monitoring measures to SMEs' PII misuse by both government and non-government actors.

Major Challenges in Data Privacy

The analysts have identified countless issues, which can be grouped into legal, technological, operational, and ethical contexts. Below are some of the major challenges related to data privacy:

Below are some of the major challenges related to data privacy:

1. Legal and Regulatory Challenges

Diverse Legal Frameworks: Every country has different rules pertaining to the privacy of dataand this causes a lot of problems as well as confusion for companies that operate internationally. For instance, the GDPR of the European Union is much stricter than any otherregion's requirement making compliance approaches different.

Compliance and Enforcement: It is difficult to maintain data privacy laws since it is a complexand powerful issue that becomes a problem for businesses, especially for SMEs that cannot afford to hire professionals. However, most of such laws can be only partially enforced and assuch there are variations in the levels of data protection.

Cross-Border Data Transfers: Dealing with legal issues related to the cross-border datatransfers is difficult because of diverse regulations as to the protection of data. Instead, issues like international data transfers, processors' liability, or data protection for large-scale data processing projects remain unsolved or are solved in a way that is challenging to operationalize;yet, such mechanisms as SCCs and BCRs were designed to tackle such problems.

2. Technological Challenges

Rapid Technological Advancements: Much the same, the evolution of technology proves to progress at a faster rate as compared to the formation of regulatory measures. New technologiessuch as artificial intelligence, machine learning, and IoT have similarly posed new issues and concerns on data privacy that current laws seem to overlook.

Data Breaches and Cybersecurity: Data Leaks and Cyber-attacks are increasingly becoming common and this

is a great danger to people's data. Having strong cybersecurity measures is crucial, though it may be challenging because threats are diverse and progressively developing.

Big Data and Analytics: If the data is anonymised sufficiently then privacy is not threatened, and consent is no longer necessary; big data and advanced analytics may re-identify the data samples.

3. Operational Challenges

Data Management and Governance: Compliance with regard to data classification, dataretention, and disposal is crucial but often challenging when it comes to tackling the goals in detail. The issues of data's accuracy and consistency when there are multiple sources and databases do exist.

Employee Training and Awareness: It incumbent on organisations to ensure that the staff is briefed, on the appropriate measures that should be followed concerning data privacy. The human factor continues to be one of the primary threats to data security and protection.

Resource Constraints: However, overall measures of data privacy entail costs which are quite high, especially to implementing organizations particularly those of small scale.

4. Ethical and Social Challenges

Balancing Privacy and Innovation: It is always a struggle to achieve a good balance between people's privacy on one side and innovation developments on the other. High codification canalso act as a deterrent to innovation in technology and could slow down any country's rate of economic development.

Consumer Trust and Transparency: Trust of the consumers is something that needs to be developed and maintained throughout the business-space. There is a need for organizations tobe open on how they process personal data and act appropriately regarding the data.

Informed Consent: There is always a challenge in trying to get informed consent from people;the consent is often influenced by lengthy and complicated privacy policies that users hardly comprehend.

5. Emerging Threats

Surveillance and State Intrusion: Surveillance technologies and laws embraced by governmentscan be a huge threat to people's privacy since they allow the state into their data.

Data Localization Requirements: Some countries require that data about its people stays withinthe country thus making it not easy for companies to operate and also restricting data across borders.

6. Judicial Interpretations

Evolving Jurisprudence: As it has been highlighted with the judgements made by the judiciary,legal risks arise because of distinct interpretations of data privacy laws. It is followed by the fact that courts' decisions influence various practices related to data protection and regulatorycompliance.

Recommendations to enhance Data Security

Due to the multifaceted nature of the problem it is necessary to apply a multipronged approachbased on legal, technical, organizational, and ethical frameworks regulating data privacy. Hereare some suggestions to improve data privacy:Here are some suggestions to improve data privacy:

1. Enhancing the Tamil Nadu Legal Consultation Structure

Harmonization of Laws: There is a need to adopt the use of international frameworks to aim atachieving policy convergence to ease the complexity that organizations face in dealing with policies of various Jurisdictions in the world while aiming at protecting consumers' data.

Dynamic Regulations: Collaborate to develop fluid legal statuses that may adapt in order to come across new technologies and other types of privacy perils. This could entail time to timechanges in the data protection laws and the guidelines that accompany such laws.

Enhanced Enforcement: Improve the funding and powers of DPAs for them to be able implement the laws adequately. In this case, there should be increased harsher penalties for data breaches and non-adherence to the policies as a way of discouraging the negligence**.**

2. Advancing Technological Solutions

Privacy by Design and Default: Promote PbD, thereby integrating privacy into the use of IT, network technologies, and business process in the designs and applications.

Advanced Encryption: Advocate for the integration of complex encryption methodologies to combat odds and intercepts of both storage and transfer data.

Anonymization and Pseudonymization: Perform accurate anonymization and pseudonymization of the individuals' data to be used for analytics and research purposes.

3. mproving Operational Practices

Comprehensive Data Governance: Adopt robust policies in the management of data that involves categorizing data, defining how long data should be kept and when it should be destroyed and performing a data audit at prescribed intervals.

Employee Training: Most threats are due to human errors therefore data privacy training for the employees on how to prevent such threats, changes in threats, and future compliance shouldbe conducted frequently.

Incident Response Plans: Manual No.: 108 – Create and update comprehensive writtenprocedures to respond to and contain data breaches and the extent of their compromise.

4. Building Consumers Confidence and Clarity

Simplified Privacy Policies: One should develop effective privacy policies for website users and make them easily understandable so as to make the users understand how their informationis going to be used before they allow it.

Transparent Data Practices: Ensure that the organization's data collection, usage, and sharing processes are transparent. Implement the practice of continuous raising awareness of the consumers on how their data is protected and shared.

Consumer Rights: Enhance and specify consumers' rights within their data, especially to receive, rectify, erase, or transfer their data.

5. It is in exploring the solutions to these aspects that ethical and social considerations areaddressed.

Ethical Data Use: Set up procedures that would protect the individuals' right to privacy whileprocessing the

data and would also make sure that the processing does not negatively affect theindividuals or the society as a whole.

Public Awareness Campaigns: Conduct awareness creation to inform the people concerning data protection, their freedom and the way to go about it in the current world.

alancing Privacy and Innovation: Encourage cooperation between the authorities, businesses, and citizens' protection organizations to minimize the preponderance of privacy on technological advancements.

6. Enhancing Cross-Border Data Protection

International Cooperation: Proposed ways: encourage global interaction and setting up of international standards in the management of data in view of enabling Data localization whileenhancing privacy protection among the international borders.

Data Transfer Mechanisms: Support the use of verified means of transferring data across borders using BCRs and SCCs to enhance the security of the transfers.

7. Judicial Oversight and Interpretations

Judicial Training: Therefore, there is a need to conduct specific sensitisation sessions for the judges particularly within jurisdiction that have embraced the doctrine of data privacy.

Precedent Setting: Explain that it is especially important to make precedents that would help the organization decide on how to ensure data privacy and raise awareness of the uncertaintiesof the existing legal provisions.

Conclusion

Data privacy is an area that is ever in a state of change and Flux because of the technological advancements and the feeling of data privacy globally. This is why comprehensive data protection legal frameworks at the national and the international level play such an important role in protecting people's rights and preserving people's confidence in digital environments. The legislative and executive entities have acknowledged decisions made by judicial organs like the Indian judiciary concerning the privacy right and handled the modern privacy issues with the help of legislation and policy.

However, certain difficulties are still pertinent: legal frameworks may vary across countries, there are technological advancements, and there are issues with the operations of such systemsand ethical questions as well. Solving these issues requires a complex approach with the combination of the synchronized regulations, the development of the technological measures, the improvement of the operation methods, and the promotion of the ethical data utilization.

Therefore, the way forward is through transnational cooperation by the government, other appropriate bodies, firms, and users with the common noble goal of developing and maintaining a safe and privacy-preserving cybersecurity realm. Through supporting rigorous data governance, being transparent, having strict enforcement, removing disadvantages between privacy and innovation and most importantly balancing it, we can construct a resistant model of data privacy that safeguards individual rights and at the same time fosters technologyand economy progress.

Hence, two main remarks can be made In view of the fact that the development of data privacylaws and practices hardly ceases, more attention should be paid to collaboration and flexibility.While trying to solve the quandaries of the contemporary world, it is crucial to adhere to suchvalues as data protection for the privacy of the person and the non-interference of the state in the autonomy of an individual in the context of a digital society.