Lucknow Law Review

Short Article

A Study on Emerging Data Privacy Law: Towards an Advance Framework

Saloni Singh & Vaibhav Singh Chauhan[1]

[1]*University of Petroleum and Energy Studies, Dehradun*

Published on: September 7, 2021
Page No.: 69 – 78
Manuscript No.: 2021/LNLR/07069
Editors: Piyush Patel, Prithivi Raj

Cite as: Saloni Singh & Vaibhav Singh Chauhan, A Study on Emerging Data Privacy Law: Towards an Advance Framework (2021) 1(2) LKO. L. REV. 69

Find here: *https://www.lucknowlawreview.org/saloni-vaibhav*

Abstract: *Privacy is an essential fundamental right. It underpins individual dignity and different values such as liberty of federation and freedom of speech. Nevertheless, privacy is remaining questioned in the networked civilization. The application of modern technologies threatens this power because it promotes the accumulation, accommodation, processing, and alliance of individual data by protection bureaus and institutions. This analysis note gives the knowledge and plan of the recent commence research perceptive, which directs at re-conceptualizing the notion of privacy and increasing means for the estimation of privacy consequences. We essentially are the characters that create this data positively necessitate security as to how aforementioned produced data is concocted or practiced. We necessitate transparency comparatively to the system our data is obtained. The aforementioned is wherever data protection laws develop into the statute. Certain laws are holding enacted simultaneously by many nations for the security of data and it is created by their residents. This article reviews the current circumstances of data protection laws in India & throughout the world. This article also concentrates on the Indian jurisprudence features of data protection and privacy. This article will present you with the nature of data protection and privacy laws that standardize the way input is processed, interpreted, and applied.*

Keywords: *Data Protection, Privacy, Personal Data, Data Theft.*

Copyright © 2021, Lucknow Law Review.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Concerns about privacy have prompted the development of privacy legislation in many different countries like United States including Europe, other parts in the world. Privacy laws set requirements aimed at preventing the acquisition or use of information in ways that are incompatible with the data subject's expectations. Except with their approval, data subjects' authority over individual private data can't be avoided and refused. Each time personal data is gathered in the United States, a contract is made that regulates the data's subsequent use. The rules of the game are shifting for those in charge of ensuring that privacy regulations are followed.

Privacy law puts to a test that company is able to integrate any business, law, including technology in the logical design moreover implementation of their information systems. Technology CEOs are being asked to take on more legal compliance responsibilities in a variety of legal environments. Contracts and other legal tools are becoming increasingly important in the development of solutions that provide a competitive advantage.

2. The Evolution of Data Privacy

The Data Protection Directive of the European Union comes into force in October 25, 1998. The Directive largely follows the COE Convention and OECD Guidelines' essential "fair information criteria". It makes no distinctions on the basis of the industry in which the data collectors and processors work. The Data Protection Directive of European Union is based on the concept that the regulations would be decided by the nature of the data rather than its intended purpose (E.U.)[1] Data subjects may be required to take affirmative action that results in a report of their "unambiguous permission" for the collection and processing of private data in specific circumstances. Firms will not be able to collect and utilize information without consent from the data subject, even if they opt-out, according to the European Union.

2.1. United States Law

In response to industry-specific limits, requirements for the acquisition or dissemination of personal information have been created. The generic architecture is in stark contrast to this segmented strategy. There are distinctions made between industries, data sources, and the social sector in which the data is acquired or used. According to David Frum, US law is particularly indifferent to the rising global economy's dimension.

[1] Information Technology Act 2000, sec 43A

He claims that administrative agencies are in charge of establishing implementing regulations in accordance with established legislation. Personal data is expected to transcend borders, according to U.S. and European architecture. He claims that "the federal government has not opted to supersede the states' right to regulate privacy".

3. Politics with Policy

Talking about disparity within methods between European Union as well as United States has become a source of worldwide political attention. The European Union Directive restricted the sales of individual data to countries in competent data protection regulations received little attention in the United States. The European Union Directive, according to American corporations, is a massive non-tariff trade barrier that threatens vital industries. The authority is promoting self-managed by relying on non-administration organizations for imposing appropriate requirements on participating businesses.[2] Companies that are subject to clear government restrictions surrounding personal information privacy, such as HIPPA.

The differences between Europe and United States, according to David Frum, are symbolic of the larger elements of a growing body of international privacy legislation. Frum Political conflicts put massive economic investments at risk, since systems increasingly operate without regard for geographic considerations. He believes it is past time for the US to reexamine its data protection policies. Privacy legislation is increasing traction as a prospect important disruptor for the development moreover implementation of effective IT practices. Economic competition among governments and regions can obstruct the development of effective systems that manage personal data in a meaningful way.[3]

While Europe including the US fought to reach an agreement for Safe Harbor plans, other countries have not shied away from the privacy issue. The European Union is watching as its vision of effective privacy protection spreads around the globe. Enacting privacy legislation is substantially easier in many countries where less friction within the public including private areas. Numerous countries including common regulation traditions, including Hong Kong, and Canada, have passed legislation. Other countries are considering proposals. While the adoption of European open data sources, the enacted statutes are very similar. In this regard, the European Union is seeing its vision of effective privacy regulation successfully exported. In other

[2] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
[3] BLAPL No. 4592 of 2020

aspects, as some pro-EU activists point out, this may not be the best outcome. The directive's partiality for intra-European data transfer activities was given a lot of weight.

It is vital to note that, the current status of the Department of Commerce's proposed Safe Harbor Principles implementation. According to David Perry, "American companies are realizing that just because Congress has passed federal legislation does not mean that outlining a path ahead for managing personal data can be successfully executed". The Clinton administration pressed Congress to pass new laws that would allow customers more control over their personal information shared with financial companies. The deadline for adopting the Gramm-Leach-Bliley sequestration provisions has been moved back by 7 months due to the final regulations. The Federal Trade Commission is in charge of implementing consumer protection laws and prosecuting unfair or deceptive trade practices in the United States.

Approximately 80% of state legislatures are now debating privacy-related legislation. State privacy laws that are more consumer-friendly than federal legislation is not forestalled by the Gramm-Leach-Bliley law. Many of these state initiatives would require consumers to opt-in before financial organizations could yield their data among third parties. Apart from any individual data that can be transferred to several companies, that can be affiliated, a measure within New York State would require the affirmative written consent of data subjects. A proposal in Arizona would restrict the acquisition of private data to that is "reasonably necessary to complete the transaction". Any firm providing direct Internet connection in California would be required to provide notice and choice earlier to any substitution of individual information.

The fact that trade organizations representing large portions of the US financial services sector declared that they would not support Clinton-era legislation unless national preemption of national privacy legislation was "on the table" underscores the relevance of this action at the state level. If such preemption were to be implemented, enormous benefits in terms of legal uniformity and lower compliance costs would be realized inside the US domestic market. Privacy advocates, on the other hand, are vehemently opposed to laws like preemptive regulation.

4. The Principles of Self-Regulation

A significant source of fuel for the Internet's growth has been a government commitment, particularly in the US, for encouraging self-regulation as an efficient approach for responding to the interests that generally cause the passage of new laws. In July 1997, President Clinton issued a Structure for Global Electronic Commerce, pledging his administration's commitment to a self-regulatory system. Industry activities in the area of privacy

are one of the few policy areas where they have gained traction, however their efficacy in deterring new laws appears to be limited.

TRUSTe and BBB Online are two nonprofit organizations' self-regulatory programmers. The Electronic Frontier Foundation financed TRUSTe, while the second program is based on the Better Business Bureau's self-regulatory programs. Each program allows organizations, especially those conducting business online, to disclose their agreement with specific privacy standards and agree to specific inquiry including implementation processes. Both programs, for illustration, specify qualifying conditions for the privacy procedures of Internet-based businesses. Both programmers encourage consistencies in behavior. There are two distinct aspects of these self-regulatory processes. For starters, qualifying registered businesses can use the program's logo or emblem on their websites. Customers will see this logo as a "seal of approval" for the company's privacy policy. Second, organizational repercussions are the only way to enforce privacy standards. There is no recourse to recognized venues such as the courts in the event of noncompliance. The Safe Harbor Principles have identified and endorsed self-regulatory programs as a compliance option as a result of the TRUSTe program. On the other hand, practical success has been uneven.[4]

A consortium of ninety percent of Internet advertising companies created the Network Advertising Initiative (NAI) in July 2000. The NAI was established in response to a private disagreement that had a detrimental impact on the stock price of Double Click, a major Internet advertising firm. The debate centered on Double Click's plan to combine massive amounts of non-personally identifiable data collected regarding millions of Internet users' web surfing habits with individually identifiable profiles of these users' offline purchasing habits, which was amassed by market research firm Abacus Direct as well as acquired by Double click (1999). Despite a previous promise that no such scheme would be developed, Double click went ahead and did so.

The NAI is a self-regulatory organization for the Internet advertising industry that establishes basic standards of conduct, such as the need that non-personally identifiable data be combined with personally identifiable data only with the consent of the data subject ("opt-in").[5] The NAI was commended by the Clinton Administration as a promising step toward successful self-regulation, but laws to fund the program and bring firms that had not joined into line with its principles were still favored.

[4] *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* Case C-311/18
[5] *Balu Gopalakrishnan v State of Kerala WP* (C) 9498/2020

5. In India, is the Right to Privacy a Fundamental Right?

As per the Article 21 of the Indian Constitution, a nine-judge Supreme Court judgment determined "the right to privacy" to be a basic right. As a result, the government has launched a series of activities aimed at enacting Personal Data Protection[6] legislation. Before deciding on the main case, Justice K.S. Puttaswamy[7], a bench of five justices to assess whether privacy is a right.

5.1. Current laws prevailing in India

Personal data including information shared in spoken, written, and electronic form are not protected by a stand-alone personal data protection law. The ITA (Information Technology Act), 2000 (SPDI Rules), India's primary law dealing with cybercrime and internet trade, contains the most notable clauses. It only applies to data shared electronically, not to data received via non-electronic communication. The IT Act and Rules have a limited scope and breadth. The immense preponderance of the requirements only applies to "sensitive personal data and information" gathered by "computer resources". Hence, is no mechanism for information localization that was the main source of concern moreover the cause for the Chinese applications' prohibition in India. India requires a robust data privacy law to meet these restrictions.

5.2. The Personal Data Protection Bill, 2019

After the Supreme Court's historic ruling in the Justice KS Puttaswamy case, which declared that privacy is a fundamental right, the MEITY constituted a 10-member delegation led by former Supreme Court judge B.N. Srikrishna to offer recommendations for a drafting Bill on personal data protection[8]. After a year of study, the committee delivered its report, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians", as well as a draft bill on individual data protection. On December 11, 2019, the modified Personal Data Protection Bill, 2019 was introduced in the Lok Sabha by Mr. Ravi Shankar Prasad, Minister for Electronics and Information Technology.

5.2.1. The Remarkable Characteristics of the Bill

Following the prohibition on Chinese applications, a person would usually be concerned regarding the security of their personal information that was circulating. An individual would like to comprehend what safeguards,

[6] Personal Data Protection Bill 2019
[7] *Justice K.S. Puttuswamy v Union of India* (2017) 10 SCC 641
[8] *M.P. Sharma v Satish Chandra* AIR 1954 SC 300

as well as standards, are required by the Bill on data collection and processing, moreover cross-border data transfer:

a. Reinforcement of the Law to processing of Individual Data – The law regulates the process of individual information that is received, revealed, given, and contrarily prepared within India's borders. It will not apply to anonymized data that has gone through the anonymization process. Anonymized data refers to the irreversible act of altering or turning personal data into a form that makes it impossible to identify a data principal.

b. Kinds of Individual Data - Data is divided into three categories under the bill; individual data, sensitive private data, and critical particular data. Individual data refers to information about an individual's qualities, traits, or attributes. Biometric data, financial data, religion, caste or political convictions, and any other type of data particularized by the state are all instances of sensitive personal data.

c. Obligations of Data Fiduciary - Only precise, unambiguous, and lawful purposes can be used to process personal data. Every individual who processes a data principal's data must do so fairly and reasonably while also protecting the data principal's privacy. Personal data shall only be gathered to the extent that it is required for the personal data process. The data fiduciary is responsible for ensuring that the personal data processing is concluded, precise, not misleading, including current. The Data Principal has the power to eliminate individual consent at any time during the processing process. Individual data or information may be handled only if it is necessary to meet the aim for which it was gathered.

d. Restriction on transfer of Personal Data outside India - Sensitive Personal Data should be stored in India and may be transferred outside of India for processing if the data principle has given his or her explicit approval. Any vital personal data can only be given to a person or entity that provides health or emergency services if the transfer is required for immediate action.

e. Exemptions - The central government has the authority to exempt any of its agencies from the Act's restrictions. It has the authority to exempt them for reasons of national security, public order, India's sovereignty and integrity, and good ties with foreign countries. Personal data must be processed for a precise, explicit, and lawful purpose, with appropriate security protections.

f. Offences - Bill has been passed by the House of Representatives in Delhi, India. It includes offences under which a person can be punished for re-identifying data that has been de-identified by a data fiduciary or a data

processor. Offences under this Act are cognizable and non-bailable. They include; Re-identification of personal data without the consent of the data processor and re-interfering with such data.

g. Penalties - Contravening express terms of the Code are condemned by a penalty of Rs. 15 crores either 4% fiduciary's yearly turnover, which is greater and if fail to undertake a data audit is penalized by a fine of Rs. 5 crores instead of 2% of the fiduciary's yearly turnover, that is greater.

h. Corrections to Different Laws - Bill abolishes the elements of the Information Technology Act of 2000 that require firms to pay compensation if they fail to preserve individual information (Section 43A).

6. Conclusion

The US administration of Commerce has discussed in support of the SH Principles that existing US legislation, collectively with the rules specified in the Safe Harbor documents, offers enough protection for private data. However, the Commerce Department's credibility is greatly harmed by the ongoing presentation or design of added codes in the US. The political attraction of introducing privacy laws in a democratic context cannot be underestimated; nonetheless, the sectoral strategy to American lawmaking remains to establish different privacy rules. In the US, just several proposals commit. As a result, the legal environment is becoming increasingly unstable, while higher and more established rules and guidance approach and pass their useful dates. Corporations that deal with private data meet a lot of uncertainties when it comes to developing responsive systems and business practices. Businesses that fail to establish compliant policies in accordance with current legislation may incur criminal or civil penalties. However, for many, the legal landscape's unpredictability makes large infrastructure expenditures in privacy acquiescence challenging to maintain in the absence of a deeper knowledge of the regulating standards. "We don't really care", one executive said quietly.[9]

Despite the fact that the legal framework for privacy legislation is in a state of flux, determined substantive theories are developing that are completely applicable to any juridical explication (We differentiate "substantive" principles from "process" difficulties like agreement, which are considered in Clause III.). Certain substantive concepts can be found in the architecture of the COE Convention including the OECD Guidelines, and they are unmistakably mirrored in the circumstances of the EU Directive plus the US association of Commerce's Safe Harbor Principles. At the identical period, many contemporary US moreover

[9] *Kharak Singh v State of Uttar Pradesh* 1964 SCR (1) 332

non-European legislation programs embody these ideas, frequently to a significantly greater extent than they are in Europe.

Any firm wanting to create improved personal information management procedures and systems must first establish these basic concepts. Companies can best place themselves within their own type of safe harbor by focusing on the deployment of practices that are consistent with the key principles. An organization that has performed to the Safe Harbor is better placed to perform compliant procedures than others in the event of current juridical or administrative improvements. In the long term, companies several able of performing the first clarifications responding to new supervisory guidance will most likely gain a competitive edge.[10] The interdependence of an information economy boosts the leadership's potential benefits. Despite certain situations where agencies are required to approve particular technology resolutions, most utmost powers, notably in the US, favor technology indeterminate structures that give regulated firms the versatility to create their resolutions.[11] As a result, firms who demonstrate initiative in improving privacy administration practices on the basic policies are likely to be the first to propose resolutions toward others to follow. This allows them to avoid being questioned by many people.

The key principles stress the fact that privacy law is founded on contracts. A contract is made up of an offer and an acceptance in both common and civil law systems. When studying the key principles, it becomes clear that their purpose is to ensure that each entity involved in the acquisition or control of data demands particular steps that are effectively a list of proposals including acceptances. As a result, personal information regulation can be rethought as a particular subset of contract law. Data methods can then be created furthermore achieved more in line with common exchange methods in this context. Whatever makes this deal unique is that the deal's asset is the perk.

[10] Sara Salinaa, 'Full Text of Apple CEO Tim Cook's Keynote in Brussels' (CNBC, 24 October 2018) <https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html> accessed June 25, 2021

[11] Personal Data Protection Bill 2019, p 156