Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
June 2024 5(6), 1919–1924

DATA PROTECTION IN THE AGE OF SOCIAL REGULATION: A CONCEPTUAL FRAMEWORK

Poorvi Srivastava[1], Dr. Seema Siddiqui[2]

[1] Research Scholar, Faculty of Law, Integral University, Lucknow
[2] Head of Law Department, Integral University, Lucknow

DOI
10.29121/shodhkosh.v5.i6.2024.2756

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

In the current digital landscape, characterized by rapid technological advancements and pervasive social media usage, the intersection of data protection and social regulation has emerged as a critical area of focus. This research paper explores how emerging social norms and regulatory frameworks shape the ways in which personal data is collected, processed, and protected. It critically examines the evolving definitions of privacy and consent, the role of regulatory bodies in enforcing data protection standards, and the implications of social expectations on corporate practices. By presenting a conceptual model that integrates legal, ethical, and societal dimensions, the article highlights the necessity for a multifaceted approach to data protection that transcends traditional legal frameworks. It argues for a collaborative paradigm that engages stakeholders, including individuals, institutions, and policymakers, in the creation of robust data governance solutions. Ultimately, this work aims to contribute to the discourse on building resilient data protection strategies that are aligned with contemporary social values and technological realities. This article aims to analyze the effectiveness of the Personal Data Protection Act of 2023 in ensuring the right to privacy and data protection.

Keywords: Data Protection, Social Regulation, Privacy, India.

1. INTRODUCTION

The freedom from covert surveillance and the authority to choose when, how, and to whom to disclose personal information are two aspects of the right to privacy.[i] Since its inception, privacy has been used both to an individual's advantage and disadvantage. Technology progress has expanded its scope to encompass physical, informational, decisional, and dispositional categories.[ii] If the law is to safeguard people's rights, it must keep up with the rapid advancements in technology. Recent technological advancements and the dynamic legal field have given rise to new perspectives on issues with data protection and privacy. One's right to secrecy is the freedom from interference with the interests of others. Because of technology advancements, privacy has become a concern for everyone, with a focused focus on data security.[iii] Data protection places a strong focus on individual liberty, and these individuals' liberties are threatened by outside intrusion. It is imperative that the stranger's actions to stop interacting with the person. The Constitution of India can be used to confirm any new phenomenon's fundamental legal requirements. Constitution places more emphasis on rights than on duties. The creation of new statutes and many modifications to already existing ones have aided in the evolution of the Indian legal system. The relevance of data security and privacy's constitutionality has increased recently because it is necessary to grant a unique status inside the legal system. To provide a sophisticated

level of privacy protection, evaluating the efficacy of the existing legal system is crucial. It examines how an individual's right has been affected by the intrusion of data protection in connection with other laws. The concept behind introducing this motive is to link India to other nations. The Supreme Court's recent ruling that privacy is a basic right has become a seminal ruling.

2. KEY CONCEPTS OF BIG DATA

Large data sets on human behavior are combined with sophisticated prediction algorithms to create *"Big Data"* which is then used to track, monitor, analyze, and share this information.[iv] Paradoxically, the ability to examine and integrate massive data sets to better forecast future events, actions, and behaviors rather than just its size is what really makes big data unique. Big Data comes from three basic sources. First are organizational records, which comprise business dealings, agreements, and registrations with businesses or governmental agencies, including weddings, births, and deaths. The second is gathered via using websites and consists of browser searches, social media platform exchanges, and e-commerce activities. Images, videos, and text comments on different applications and websites can all include this kind of data.[v]

The third big data source concerns people's actual movements and is gathered by satellites, cellphones, and both public and private surveillance cameras. In order to follow specific motions, these gadgets are now frequently outfitted with facial recognition software, among other technologies. In fact, the possibility of monitoring people is increased by the increasing number of sensors incorporated into locations, bodies, and objects.[vi]

3. THE THREATS OF BIG DATA

There are new ethical and legal concerns associated with the creation and use of big data. It is obvious that it does this by bringing about new kinds of individual visibility that enable the modeling of human behavior and predispositions for various purposes. This is frequently predicated on information gathered from people's somewhat ordinary living environments, such as our online and grocery shopping, Google searches, and our actual city travels. In the sections that follow, we examine two approaches to Big Data that ethics-based research has taken: investigating privacy and surveillance concerns. The influence of Big Data practices on individual rights, including data extraction, disclosure usage, and user permission, access, and privileges, is the main focus of privacy work.[vii] Among the main risks connected to big data are:

- **DATA PRIVACY VIOLATIONS:** Concerns regarding privacy are raised by the gathering and analysis of enormous volumes of personal data. Data misuse can result in violations of people's privacy rights, which can damage confidence and have legal ramifications.
- **RISKS TO DATA SECURITY***:* A higher volume of data also means a higher danger of cyberattacks. Hackers may target big data settings, which might result in data breaches that reveal private information.
- **ADHERENCE TO REGULATIONS***:* Businesses must ensure compliance with increasingly stringent data protection standards, such as the CCPA and GDPR, as governments place more restrictions in this area. Serious penalties and harm to one's reputation may arise from noncompliance.
- **PROBLEMS WITH DATA QUALITY:** Data that is skewed, out-of-date, or inaccurate might produce analysis and decisions that are not sound. Inadequate data quality can cast doubt on the efficacy of Big Data projects and result in false results.
- **INFORMATION OVERLOAD***:* Organizations may get overwhelmed by the sheer amount of data, which makes it challenging to derive valuable insights. Businesses may find it difficult to properly manage and evaluate the data if they lack the right tools and techniques.
- **MORAL ISSUES***:* Big Data usage frequently prompts ethical concerns, particularly in relation to monitoring, profiling, and manipulation. Businesses need to consider the ethical ramifications of their data activities.
- **DATA GOVERNANCE CHALLENGES:** Ensuring data security, accuracy, and compliance requires the establishment of strong data governance structures. Data management procedures might become uneven as a result of poor governance.

4. ASPECTS OF PRIVACY

The multifaceted idea of privacy protection has emerged as a result of the current situation. Therefore, in order to create a strict privacy regime, it is imperative that one take into account the complex aspect of life as it is known to everybody.[viii]

The first concern with privacy is an individual's physical safety.[ix] In daily life, one may observe and encounter this aspect of seclusion. Bodily privacy includes practices like narco-analysis testing and airport frisking.

A man's personal space cannot be invaded by anybody without a valid reason or legal support. Nonetheless, there have been a number of cases in the past where individuals have disregarded this fundamental rule and entered a man's house, both in India and outside. The media is heavily involved in these violations. From tracking a prominent figure's whereabouts and taking pictures of them and their family without permission. For the families, such meddling has even proven to be lethal.[x]

The privacy of personal information, often known as data privacy, is typically associated with personal data that is kept on computer systems. Information that has been acquired about an individual, such as financial, criminal, political, economic, or internet data, as well as medical and other records, must be kept private.[xi] Communication is the industry that has benefited most from technological advancements.[xii] A single landline phone in a community has given way to a smartphone in every person's hand due to fast advancements in technology and accessibility. Recent advancements in the communication industry have multiplied interpersonal interactions, resulting in a reduction of residents' personal privacy. Legislators must thus create a legal framework that guarantees both credible communication security and individual protection in order to assure both national and individual security.[xiii]

An unprecedented quantity of personal data has been generated in recent years due to the spread of social media and internet platforms. This data is gathered, analyzed, and shared by a variety of organizations. As a result, data protection has become a critical concern, and regulatory frameworks have been put in place to ensure the protection of individuals' rights and freedoms.

5. THE IDEA OF DATA SECURITY

Globally, the idea of data protection is becoming increasingly significant. All countries are gradually adopting laws that control the use and misuse of personal data and embracing the ideas of data protection. The German word *'Datenschutz'* is where the term *'data protection'* originated.[xiv] The idea of data protection is somewhat related to personal privacy.[xv] Generally speaking, it is reserved for a system of standards that support more interests than only privacy protection.[xvi] For data protection, factors other than privacy are taken into account. A number of other, somewhat related ideas have also been brought forth, most notably "freedom," "liberty," and "autonomy."[xvii] The primary consideration for the individual in this regard is whether or not data protection is a right. In this field, a growing question is how far these rules ought to safeguard people and organizations. Regarding the protection of an individual's information, this data protection notion is largely acknowledged. The protection of information laws to "data subjects"[xviii], who are strictly defined as "living individuals", is another aspect of data protection.

THE ROLE OF SOCIAL REGULATION IN DATA PROTECTION

The terms "right to privacy" and "data protection" are becoming more interchangeable. Only until the invasion of privacy is ended can "data protection" be achieved. Informational privacy in particular, and privacy legislation in general, have always been strongly related to technological advancement.[xix] The use of social norms, values, and practices to control behavior and accomplish desired results is known as social regulation. Social regulation is essential for influencing people's behavior and promoting ethical data handling procedures in the milieu of data protection.

GUIDING STRATEGY ON DATA PROTECTION IN INDIA

The legal systems of many, if not most, countries have a variety of legislation that either directly or indirectly contribute to the fulfillment of basic ideas frequently found in data protection treaties. Examples of rules include those pertaining to intellectual property, computer security, defamation, and breach of confidence. The following summary, however, is mostly interesting since it shows how much each country has embraced a set of regulations that directly support data protection. The extent to which nations allow for the creation of independent organizations explicitly tasked with supervising the application and/or continued improvement of these regulatory frameworks is also of great significance. The formal normative basis for data protection laws primarily comes from lists of fundamental human rights found in a number of multilateral instruments, including:

- the International Covenant on Civil and Political Rights (I.C.C.P.R.)[xx],
- the European Convention on Human Rights and Fundamental Freedoms (E.C.H.R.)[xxi],
- the American Convention on Human Rights[xxii], and the Universal Declaration of Human Rights (U.D.H.R.).[xxiii]
- the African Charter on Human and People's Rights.[xxiv]

These documents all unequivocally recognize privacy as a fundamental human right.[xxv] Not all lists of human rights from non-Western liberal-democratic countries exclude privacy, as the African Charter does. For example, everyone's right to privacy is explicitly recognized in the Cairo Declaration on Human Rights in Islam.

The right to privacy under these instruments is closely linked to the objectives and principles of data protection law, even though other human rights, such as the freedom from discrimination and the right to free expression, are as significant. As a basic part of its legal explanation, data protection laws frequently place a high priority on maintaining the right to privacy, highlighting the special importance of this right in this context.[xxvi]

The most common method for protecting privacy and personal data in India is the regulatory framework of laws, regulations, and processes that minimizes the invasion of people' privacy as a result of the collection, storage, and dissemination of sensitive personal data.[xxvii] The interpretation of Article 21 of the Indian Constitution, which addresses the fundamental freedoms of life and liberty, has taken the right to privacy into account. However, as stated in Article 19(1)(a), privacy may be included into the constitutionally guaranteed right to free speech and expression, much like other fundamental rights already in place.[xxviii] The relevant national law governing the collection, sharing, and use of personal data is comprised of certain provisions of the Information Technology Act when read in conjunction with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The main objective of the IT Act is to protect electronic data, which by definition encompasses both non-electronic records and information as well as information that has been, is being, or will be handled electronically. The IT Act also covers other aspects of information technology, such cybercrimes and internet trade.

The Contract Act of 1872, the Indian Copyright Act of 1957, the Indian Penal Code of 1860, and the Credit Information Companies Regulation Act of 2005 are the primary pieces of legislation that provide data protection, in addition to the IT Act and the implicit right to privacy guaranteed by the judiciary under the Constitution.[xxix]

The Digital Personal Data Protection Act, 2023 (hereinafter referred as DPDP) is a historic law designed to safeguard the individuals' personal information. In response to the rising concerns about data security and privacy in the digital era, the Act was introduced. Although the PDP Act is a good place to start, but there are still a lot of problems and inadequacies that need to be resolved. But there are some flaws in this legislation such as the Act defines personal data as *"any data about an individual who is identifiable by or in relation to such data."* However, this definition does not explicitly cover sensitive data, such as genetic information, biometric data, or financial information. Sensitive data protection may become less effective as a result. Organizations that process personal data in India are governed by the Act, no matter where they are situated. However, applying the Act to organizations based outside of India would provide jurisdictional challenges.

6. CHALLENGES IN DATA PROTECTION

Even if data privacy is crucial, there are a few issues that must be resolved:

- **DATA PRIVACY FATIGUE:** People are less inclined to take action to secure their personal data due to the rising frequency of cyberattacks and data breaches.
- **TRANSPARENCY:** A lot of businesses don't give out precise, understandable information on how they gather, handle, and utilize personal data.
- **INSUFFICIENT DATA PROTECTION FRAMEWORKS:** Given the complexity of contemporary data protection challenges, it's possible that the regulatory frameworks in place are neither sufficient nor effective.
- **INTERNATIONAL COLLABORATION:** Concerns regarding international cooperation and the capacity to implement data protection regulations are raised by the spread of private data across state boundaries.

7. OPPORTUNITIES FOR DATA PROTECTION

Despite the challenges, there are a number of approaches to improve data security:

- **GROWING AWARENESS***:* There is a greater need for improved data protection methods as a result of people being more aware of data protection concerns.
- **TECHNOLOGICAL DEVELOPMENTS:** New developments in artificial intelligence and device culture, for instance, can enhance data protection by making security threat identification and monitoring more effective and efficient.
- **GLOBAL COOPERATION***:* Agreements and collaboration between nations can assist create uniform data protection regulations and make it easier to exchange best practices.

- **PERSONAL EMPOWERMENT:** People now have the ability to demand greater protection and take control of their personal data appreciations to the growth of social media.

8. THE BEST DATA PROTECTION PRACTICES

In the era of social regulation, companies should use the following best practices to guarantee efficient data protection:

- **STRICT PRIVACY POLICIES:** Clearly define your privacy rules and the procedures for gathering, using, and processing personal data.
- **PERFORM SECURITY AUDITS ON A REGULAR BASIS:** Conduct security audits on a regular basis to find gaps and vulnerabilities in information safety systems.
- **MAKE THINGS TRANSPARENT:** Give material about the collection, processing, and use of individual information in a clear and transparent manner.
- **PUT INCIDENT RESPONSE STRATEGIES INTO ACTION: CREATE** incident response strategies so that you can react to security incidents or data breaches promptly and efficiently.
- **ENCOURAGE GLOBAL COLLABORATION:** Work together to create uniform data protection standards with international organizations and stakeholders.

9. CONCLUSION

Human rights, which are fundamental and unalienable, have been reduced to a visible and enforceable instrument on a national and international level.[xxx] Certain rights are mentioned explicitly in these agreements, while others are introduced through an interpretive tool since they are inextricably linked to other rights. Among all the human rights, the right to privacy is one of the most important and well-known. It makes it possible for people to spy on other individuals. The right to privacy is included in the Universal Declaration of Human Rights, the Convention on the Rights of the Child, and international covenants on civil and political rights. One of a person's most basic rights is the right to privacy. In India, this right is acknowledged as an essential part of the freedom of expression as well as the right to life and liberty.

In the current digital era, data protection is a vital concern, and social regulation is essential in influencing people's behavior and promoting ethical data management techniques. Even while there are obstacles to overcome, there are also chances to improve data protection via raising awareness, developing new technologies, collaborating internationally, and empowering individuals. Organizations may guarantee the integrity and confidentiality of personal data and foster trust and confidence in online interactions by implementing best practices for data protection. Despite being a good first step in the right direction, the Personal Data Protection Act, 2023 still has a lot of problems that need to be resolved. To ensure that the Act is effectively implemented and enforced, it is imperative that definitions be strengthened, clear processes for permission and data transfer be provided, enforcement mechanisms be strengthened, and accountability and transparency be increased.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Lindsey Norman, An Overview of the Changing Data Privacy Landscape in India 919 (2018).

Payal Thaorey, "Informational Privacy: Legal Introspection in India" II ILILR 160 (2019).

Mohd Faiz Khan and Dr. Naseem Ahmed, "The Erosion of Privacy in the Face of State Surveillance: A Digital Dystopia" 29 (1) Madhya Pradesh Journal of Social Sciences 438-448 (2024).

S. Lohr, "The age of big data" New York Times, February 11, 2012.

D. Boyd and K. Crawford, Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon" 15(5) Information, Communication & Society 662–679 (2012).
M.H. Miraz, M. Ali, et.al., "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano things (IoNT). In Internet Technologies and Applications (ITA)" IEEE 219–224 (2015).
Antoinette Rouvroy A. Rouvroy, "Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data" Centre de Recherche Information, Droit et Societe, 09 REV (2015).
Mohd Faiz Khan and Dr. Naseem Ahmed, "Defending Individual Privacy against State Surveillance" 12 (4) AJASRA 140 (2023).
Janet Zandy, Universal Declaration of Human Rights" 113 Radical Teacher 54 (2019).
Cayce Myers, "Digital Immortality vs. The right to be Forgotten: A Comparison of U.S. and E.U. Laws Concerning Social Media privacy" 16 Romanian Journal of Communication and Public Relations 47 (2016).
See Graham Greenleaf, "Data Protection: A Necessary Part of India as Fundamental Inalienable Right of Privacy
Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India" SSRN Electronic Journal (2018).
Robert C Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere" 67 Duke Law Journal 981 (2018).
Fahd Al-Dosari, "Security and Privacy Challenges in Cyber-Physical Systems" 08 Journal of Information Security 285 (2017).
S. Smitis (ed.), Bundesdatenschutzgesetz 62–63 (Nomos Verlagsgesellschaft, 8th edn., (2014).
Lutha R. Nair, "Data Protection Efforts in India: Blind leading the Blind?" 4 IJLT (2008).
See Lee A. Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits (Springer, 2002).
Alan F Westin, Privacy and Freedom (Atheneum, New York, 1967).
Dr. Naseem Ahmed, Dr. Yashfeen Ali, et.al., Emerging Trends in Technology & its Impact on Law 79 (Nitya Publications, 2022).
Graham Greenleaf and Sinta Dewi Rosadi, "Indonesia's Data Protection Regulation 2012: A Brief Code with Data Breach Notification" 122 Privacy Laws & Business International Report 24-27 (2013).
U.N. General Assembly resolution 2200A (XXI) of 16th Dec. 1966; in force 23rd March, 1976.
European Treaty Series No. 5; opened for signature 4th Nov. 1950; in force 3rd Sept. 1953.
O.A.S. Treaty Series No. 36; adopted 22nd Nov. 1969; in force 18th July 1978.
United Nations (U.N.) General Assembly resolution 217 A (III) of 10th Dec. 1948.
O.A.U. Doc. CAB/LEG/67/3 rev. 5; adopted 27th June 1981; in force 21st October 1986.
See U.D.H.R., Article 12; I.C.C.P.R., Article 17; E.C.H.R., Article 8; A.C.H.R., Article 11. See also Article V of the American Declaration of the Rights and Duties of Man (O.A.S. Resolution XXX; adopted 1948).
See, The Council of Europe Convention on Data Protection, art. 1, supra note 51.
Dhiraj R. Duraiswami, "Privacy and Data Protection in India" 6 (1) Journal of Law & Cyber Warfare 166-186 (2017).
Mirza Juned Beg, "Right to Privacy is an Integral Part of Right to Life and Personal Liberty" XV Legal Desire International Journal on Law (2018).
M.P Sharma v. Satish Chandra, AIR 1954 SCR 1077; Kharak Singh v. State of Uttar Pradesh, AIR, 1963 SC 1295; R. Rajagopal v. State of Tamil Nādu, (1994) 6 SCC 632; Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
Prakash Shah, "International human Rights: A perspective from India" 21 (1) FILJ 24- 38 (1997).