The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 2 | February 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Administrative Law Response to Emerging Technological Challenges and its Role in Safeguarding Data Protection Laws in India

Sahana Patil

3rd Year Law Student at School of Law, CHRIST (Deemed to be University)

Email: sahana.patil@law.christuniversity.in

ARTICLE DETAILS

Research Paper

Accepted: 28-02-2025

Published: 14-03-2025

Keywords:

Data Protection, Administrative Law, Technological Challenges, Digital India, Privacy Rights

ABSTRACT

With the rapid progress of technology, especially the internet, data movement across borders has been altered so much that data is essentially part and parcel of life. From social media to banking, or retailer services, increased reliance on data has brought new and complex issues regarding privacy and data protection. In response, India, as one of the fastest-growing economies around the world, has introduced the Digital India program and implemented several legislative measures in the form of protection of personal data and individual privacy rights. However, it is still concerned about whether these laws are keeping up with the dynamics of technology in terms of their effectiveness. It evaluates the present Indian legislative and administrative structures regulating data protection. This paper, titled Administrative Law Response to Emerging Technological Challenges and its Role in Safeguarding Data Protection Laws in India, aims at detecting the efficiency of these laws, pointing out grey areas, and identifying the requirements of digital natives who are demanding change in the laws. This paper explores how administrative law can respond to these shifting technological challenges in a way that makes data protection regulations robust, adaptive, and adequate for safeguarding personal data in this increasingly digitized world.

DOI: https://doi.org/10.5281/zenodo.15065493

INTRODUCTION

As the pace of digitalization is growing day by day, Internet and technology seem to seep into every life in India. With increasing sectors ranging from healthcare to education, there has been a rising demand for data security and cybersecurity measures as a measure to safeguard citizens and companies at large from cyber hacking and data breaches undertaken by the state. Presently with a population of 1.3 billion, India is the second-largest internet market and the rapid digital growth has arisen with serious concerns over data privacy and security issues. Modern economies increasingly rely on data because of globalization and the growth of international trade, thereby transforming data from a source of information into an economic asset. Public and private organizations are daily compiling large amounts of personal data on individuals through even outdated means, complicating already meagre efforts to protect individual privacy in an internet-bound world without borders. One old right, such as privacy, is simply assumed to exist but is today very dangerous because of misuse that comes about from the constant exposure of personal information in the digital age. In light of all these, governments around the world, including India are responding by enforcing full data protection regulations that should control how businesses collect, store, and process user data. The importance of reconciling the rights respectively of privacy with innovation is now very critical as digital privacy issues continue to pose threats across various sectors.

India's digital transformation is ushering in a growth pattern never witnessed before. However, along with all this transformation comes its fair share of challenges, particularly in data security and data protection. As the second largest internet market globally, India has witnessed rising tides of cyberattacks and data breaches. In fact, the notoriety of Aadhaar leak case in 2018-the one which unveiled personal details of more than 1.1 billion citizens across the country-was very much there as a stark reminder of vulnerabilities within its digital infrastructure. The Global Risk Report of the World Economic Forum 2019 commented on this incident as being among the biggest data breaches anywhere in the world, and, once again, the calls for a holistic approach towards cybersecurity and data protection have been growing in India. As long as India's digital economy is going to boom, it is quite obvious that its legislations need more than the Information Technology Act 2000, even with its amendments as done in the year 2008, to today's acceptable standards. Provisions on data protection and cybersecurity have been criticized for being very shallow as they are not attuned to the complexity of the digital environment as it is known in today's world. This created a hole, prompting the Indian government to launch the Personal Data Protection Bill in 2019, which sought to restructure and overhaul the country's

existing data protection legal framework. Among other things, the Digital Personal Data Protection Bill, 2022 specifies a variety of core principles including data minimization, purpose limitation, and accountability, not forgetting a Data Protection Authority-the regulatory body which will enforce the Act and hold businesses and government agencies responsible for violating data privacy. But this again creates a very prominent gap in India's regulatory scene--and a rather contrasted view when measuring against other countries that keep on updating their data protection laws. Legally, in accordance with regulation, the Indian government has launched several initiatives to address cybersecurity concerns. Initiatives like the 2017-launched Digital India program aim to "power a digitally empowered society and economy" through the creation of safe digital infrastructure and "increased awareness about cybersecurity." The Data Security Council of India (DSCI), a self-regulatory organization that works with the government and other stakeholders, has been instrumental in defining best practices for data protection. This context is intimately related to the continued innovations in technology that call for a more robust administrative and legal framework. This explores how India's regulatory system, comprising legislative bodies and regulatory authorities such as the proposed DPA needs to transform to meet the challenge in the complex data privacy and security issues of this digital era. The research will concentrate on an analysis of the efficacy of responses given by the current administration, identify the gaps, and outline the possible reforms that will conform to international standards on data protection.

Technological advancement in India relates to the significant digital transformation of the country that further signifies the drastic evolution in need of robust data protection mechanisms. However, such comprehensive legislative mechanism, especially focused on the collection, processing, and storage of personal data, is still missing in the country. The main legal framework applicable under cyber activities and data breaches is IT Act 2000. IT Act 2000 does not provide full-fledged protection for most of the modern-day challenges propelled by emerging technologies in this present scenario. The enacted IT Act, 2000, focuses primarily on electronic commerce and digital signatures. Enacted on October 17, 2000, it provided legal recognition for electronic records and digital transactions. Subsequent provisions are based on cybercrime and data protection, which was included in the amendments of 2008. These amendments, however, remain lacking in dealing with data protection complexities of this digital age, especially against the backdrop that there is no clear distinction between personal and sensitive personal data contemplated under the Act. Section 2(o) of the IT Act defines data as "the formalized representation of information, knowledge, facts, concepts, and instructions processed in a computer system or stored in computer memory," while Section 2(v) defines information broadly to include

messages, texts, images, audio, and computer-generated content. However, the Act does not define personal or sensitive personal data, leaving a significant gap in India's regulatory framework for data protection. This gap is more crucial in the wake of such widespread data breaches, such as the shameful Aadhaar leak, which brought forth vulnerabilities in Indian systems of data management and protection. The emergent technologies not only beget challenges but also necessitate an enhanced administrative law response. It appears that the Digital Personal Data Protection Bill, 2022, in its attempt to deal with such challenges at the administrative agency level seeks to envision the rise of a Data Protection Authority that would regulate the collection, processing, and storage of data but makes requisite evolution of administrative agencies to respond to rapid technological change and ensure that all such advancement does not mark the rising quest for privacy rights among individuals. The role that administrative law plays in safeguarding data protection in India becomes, therefore, more important. As technology needs to grow, so must the legislative and administrative framework. The administrative bodies will not only have to enforce the laws but also, at times, offer the necessary flexibility for adaptation according to the emerging challenges posed by technological advancement itself, thus ensuring that laws dealing with data protection are robust and responsive to the evolving digital ecosystem.

Data protection and right to privacy in India

The definition of privacy is one that has been fundamental to human life since the earliest civilizations and continues to evolve with societal and technological changes.[1] In ancient societies and up to modern times, such a recognition of private space and information constitutes a mainstay of relevant legal systems and religious texts. In ancient society, for instance, the Greeks and Romans protected the sanctity of the home and personal space, that illustrates one of the earliest recognitions of privacy as a social good. The Romans even built private chambers called "cubicula" to preserve privacy within the confines of their homes, thus showing the deep-seated nature of the right. Jump forward to the 19th century, but technological innovations like the Eastman Kodak camera that George Eastman invented in 1888 revolutionized the very way people conceptualize privacy. These new developments were enough to make them call for utmost grave concerns over surveillance because a person was constantly exposed to the risk of photography without consent, especially at very intimate moments. Such amendments in law over privacy were made as legal systems proved unable to adapt to changes brought about by some of the latest technological breakthroughs. Pavesich v. New England Life Insurance Co became the landmark decision in privacy law where courts recognized that the unauthorized use of an individual's

photograph violated his right to privacy, thus opening the way for future legal developments.[2] The landmark essay by Warren and Brandeis in 1890 formally ushered privacy law into being as an independent legal right. These lawyers believed that people should have legal rights to protect their right to privacy, especially with the increasing rates of technological change and mass media expansion. This seminal essay paved the way for modern privacy law and influenced the legal thought all over the world, including India, wherein the last few decades, data protection and privacy have emerged as critical legal concerns. In the mid-20th century, American legal scholar Dean William Prosser further refined the extent of privacy law through dividing the four basic torts into two categories: intrusion upon seclusion and appropriation of likeness.[3] This codification of privacy within the realm of tort law therefore granted privacy the same capacity for seeking legal redress in case of infringement as others did. In the United States, several landmark cases such as Griswold v. Connecticut in 1965[4] and Roe v. Wade in 1973 had improved the constitutional right to privacy, not constitutionally defined but inferred from the Bill of Rights, with such cases laying down legal precedence in matters of autonomy over personal affairs that include marriage, contraception, and medical decisions. Although the law of privacy was developed across the world, India's development in comprehensive privacy protection legislation was relatively at the nascent stages. The county essentially drew heavily on the information technology Act of 2000 that was essentially a UN Model Law in electronic commerce. This act touched upon many potential issues concerning cybercrime and data breaches but had little to say on personal privacy or data protection. Amendments were made to the Act in 2008, which did introduce cybersecurity provisions, but it was not yet enough to tackle the issues life with new machines posed, especially in safeguarding one's personal data. Incidents such as that of the Aadhaar breach, in which data of millions of Indians were leaked, really highlighted an incipient need for clear data protection laws. It then became glaringly apparent that current legal instruments are not prepared to handle newly emerging technological challenges and protect citizens' rights over privacy in cyberspace. In today's high- rise digital technologies and rising fears about data privacy, it is administrative law that will cope with these challenges. A practical step taken by the Indian government through its proposed Digital Personal Data Protection Bill, 2022, hints at redefining the gaps. However, administrative bodies must not only enforce these laws but also adapt to the rapidly changing technological facets of vigilance regarding the safeguarding of individuals' data privacy. In other words, administrative law should frame its responses to emerging technological challenges so that it has an abreast legal structure that can protect the citizen and regulate new forms of data usage.[5] Therefore, in Indian modernization with information technology, agencies become an indispensable element in enforcing and updating data protection laws. Lessons gleaned from the overall

perspective of historical development in privacy law-from ancient societies to modern judicial rulings-against the latest technological realities drive the evolution of these frameworks.

Judicial Intervention

Early Judicial Position on Privacy: Privacies as fundamental right: The debate started in the case of *M.P. Sharma vs. Satish Chandra*, AIR 1954 SC 300[6] at page 308: The Supreme Court held that the right to privacy has not been mentioned explicitly under the Constitution. It was a case of search and seizure action, but the action was not held violative of constitutional rights because the right to privacy was not of similar ambit as the U.S. Fourth Amendment.

Kharak Singh v. State of U.P. (1962): While deciding legislation on police surveillance in the case of Kharak Singh, the Court held that privacy was not a constitutional right. However, it was the dissent of Justice Subba Rao who recognized the right to privacy as falling within "personal liberty" under Article 21 which provided an early impetus in the development of this notion.[7]

Evolvement Through Later Cases: R. Rajagopal v. State of Tamil Nadu (1994), commonly referred to as the "Auto Shanker case, that further consolidated the right to privacy by explicitly declaring it to fall within the ambit of Article 21. In this regard, the Court ruled that persons have a right to be let alone and such a right should comprise personal and family life. The Court further protected privacy vis-a-vis state surveillance, especially telephone tapping, when it ruled in People's Union for Civil Liberties v. Union of India that the same violated Article 21 and was only permissible under exceptional circumstances involving national security threats.[8]

Gobind v. State of M. P. (1975): In Gobind, the Court recognized privacy as implicit in individual autonomy and liberty but held that it was not absolute and could be restricted for compelling public interest. It set up the judicial recognition of privacy as a multifaceted right, including spatial, informational, and decisional aspects.[9]

K.S. Puttaswamy v. Union of India (2017): The landmark K.S. The Puttaswamy case, also known as the Aadhar case, was settled at last where it conclusively determined that the Right to Privacy stands as a right under Article 21. A nine-judge bench of the Supreme Court overruled the decisions in M.P. Sharma and Kharak Singh and proclaimed that privacy is part and parcel of the right to life and personal liberty. The Courts tied privacy to personal data protection, therefore shaping the need to involve people in consent given before their data was collected and limiting surveillance of the State.[10]

Judicial interventions in this series further reflect how administrative law have conformed to the emergent technologic challenges to supervise and protect privacy and regulate data protection. These are the data protection laws India is crafting under the aegis of privacy as a fundamental right, ensuring that personal details from citizens do not spill outside the digital realm into the wrong hands. Thus, the Indian courts have been continually evolving privacy jurisprudence and, by doing so, have indeed crafted a robust legal framework to steer the complex world of data protection in an increasingly inter-connected world.

Key Features of the Personal Data Protection Bill, 2018

The Personal Data Protection Bill, 2018, was India's first major legislation aimed at data privacy and protection. With significant technological advancements on the horizon and exponential rise in digital data in the future, it was necessary to build an effective legal framework for protecting personal information and creating the right to privacy. Though it has not led to an Act, the drafting of this Act established the framework for subsequent amendments. This Bill, 2019, is also one of the crucial constituting parts of the development in the administration law to answer to the challenges posed by the emerging technologies in the matter of the effective implementation and enforcement of data protection in India. The role of administrative law is therefore the balancing act of exercising power over the enforcement and operation of data protection laws on one hand with technological innovation and individual rights. Under such laws, what is proposed in the form of a Data Protection Authority (DPA) is the power of regulatory bodies expected to monitor the degree of compliance, enforce rules, and impose penalties on violators. [11]These agencies show how administrative law could be used to protect confidential personal data from the myriad risks arising because of relentless crimes, including cybercrimes and unauthorized data breaches. Below are some of the major features of the Personal Data Protection Bill, 2018, and how they relate to this administrative oversight. The Bill covered very wide coverage in that it covered Indian companies, Indian citizens, and bodies of persons incorporated within India.[12] The Bill further extends its application to all companies not physically within Indian territory but process the personal data of Indian citizens. This would thus suggest it is the intention of the Bill that cross-border data flows as well as international entities fall within the purview of Indian data protection law-this is a very important step toward regulating the exchange of data across the globalized digital economy. The Bill provided clear definitions of important terms like consent, data, data fiduciary, data principal, data processor, personal data, sensitive personal data, and even transgender status. Such definitions would form the bases of understanding the roles and liabilities of various stakeholders

involved in the data protection ecosystem.[13] Administrative law happens to be one of those tools meant for clarification of these terms and of so doing carry out interpretations and enforcement onto consistent grounds. Bills and Obligations A bill imposed concrete obligations on data fiduciaries, namely the persons or organizations engaged in processing, upon the collection, processing, and storage of personal information. New concepts like collection limitation, lawful processing, and accountability of the data fiduciaries entered the picture. Administrative law imposes all the obligations with penal consequences in case of non-compliance, thereby holding companies to proper safeguards and responsible data management practices in place. The processing of personal and sensitive data differed, with this Bill giving special attention to the data of vulnerable groups such as children. Special provisions for the processing of children's sensitive data were introduced, agreeing with the fact that additional protections needed to be put in place. It is, thus, one of the pertinent areas where administrative law intervenes to ensure stronger enforcement and specialized regulations for sensitive data types. Data Processing Exemption: The Bill provided some specific exemptions for data processing in respect of certain fields, which include national security and journalistic purposes while in the pursuit of legal proceedings. The administration of law under DPA would bear an important responsibility regarding the application of such exemptions that is detect and prevent their misuse as guided by the framework of law. One of the most important features of this Bill was the proposal for the establishment of a Data Protection Authority. It would suppose the data fiduciaries, monitor compliance with norms of data protection, and enforce those norms. Under administrative law, its functioning would confer upon the DPA regulatory power to investigate violations, impose appropriate penalties, and ensure compensation to affected parties.

Cross Border Data Storage and Transfer Rules was made to govern cross-border transfers of personal data with a copy of these categories of data to be available in India. This is the primary administrative concern in that outsourcing data storage to foreign entities becomes a source of risks. Compliance with such requirements would be the central task of the DPA.

Data Protection Bill, 2019

The Data Protection Bill, 2019 was a draft attempt that aimed at making a comprehensive framework for protecting personal data in India based on the earlier 2018 Bill. It brought out the increasing necessity for governmental regulation and administrative control over the enormous amounts of data which are processed in the current digital era. The Bill reflects the central role of administrative law in shaping and implementing data protection measures to respond to the challenges emanating from those emergent

technologies. Below are its key features, connected to the broader issue of administrative oversight in the face of technological change: Applicability the Bill would apply to any entity that is in India as well as entities outside India, if they deal with or otherwise process personal data of or related to Indian citizens or Indian businesses. Such broad applicability will ensure that both domestic as well as international entities process data in India are covered under the regulation gaze, thus mirroring the administrative necessity to enforce cross-border data protection standards. Personal and Sensitive Personal Data Under the Bill, personal data means any information relating to an identifiable natural person; an identifier such as name, location or online identifiers shall directly or indirectly enable the identification of the natural person; this includes special categories of data that are considered sensitive, these include health data, genetic data and financial data.[14] The framework of administrative law elucidates these terms and helps enforce the proper degree of protections based on the degree of sensitivity of data involved Grounds for Processing Personal Data The following grounds allow the processing of personal data: consent, or if it serves to fulfil a legal obligation. The proposed DPA would be an administrative agency, required to play an important role in monitoring whether the provisions are met and personal data is processed in such a way that it is legitimate and respectful and not for misuse. Rights of Data Subjects: The Bill equips persons with rights to crucial rights, among them their access to data, correction of inaccuracies, the right to be forgotten, and portability of data. These rights empower citizens to control personal information, and administrative law recognizes enforcements of such rights through regulation frameworks of complaints and enforcement by the DPA. Data Protection Authority the Bill establishes the Data Protection Authority, an enforcement agency with the responsibility of administrating provisions, investigations into contraventions, and imposition of penalties. This authority will be the cornerstone of administrative law to ensure protection of personal data; compliance is overseen in enforcing penalties and issuing guidelines in individual and organizational levels. Cross Border Transfer of Personal Data: The Bill controls cross-border personal data transfers, which means individual consent or authorization by DPA is required in such circumstances. Hence, this will not mis utilize personal data and there will be sufficient protection in other jurisdictions.[15] Penal provision: Secondly, the Bill imposes penalties for non-compliance very seriously such that entities are faced with legal consequences when they commit an act which violates the norm of data protection.[16] These administrative penalties therefore serve to deter and make sure that organisations take adequate safeguards over personal data. Thus, it can be concluded that the Data Protection Bill, 2019 happens to be a landmark administrative effort that tries to grapple with the country's technology challenge of data protection.[17] It is here that the role of administrative law becomes more vital in ensuring that the

provisions of this Bill are implemented or acted upon fully since the regulator would essentially be the Data Protection Authority, exercising oversight and pulling violators up in the ever-evolving digital landscape.

India's Digital Personal Data Protection Bill, 2022, is a timely administrative move toward answering the needs of changing times digitally. This Bill is very crucial to safeguard digital personal data, and here, the role of administrative law in regulating and ensuring compliance becomes paramount. Below are the main features of the Bill, relevant to the topic of how administrative law can address technological challenges and enforce data protection laws:

Territorial Application: The Bill shall extend to the processing of digital personal data in India and has an extraterritorial jurisdiction over the parties processing data outside India that relates to Indian residents. Such a character of extraterritorial application illustrates the administrative law's role in ensuring that Indian regulations are complied with even where international entities may be involved in handling Indian data. Such applications of the law are crucial in terms of regulating cross-border data flows and finding solutions for problems associated with the processing practices at a global level in such an age of modern technology.

Mechanism of Consent: Consent forms one of the backbones of the Bill, which requires processing of data only if it finds explicit approval of the data subject-the "data principal."[18] It goes on to further elaborate on the mechanism of prior notice, stating purposes and use of personal data, showing how the administrative law forces transparency and accountability in extracting data. In addition, the Bill explicitly clarifies that in certain events, like legal duties, national security, or public welfare, there would not be a need for consent. The approach would ensure balance in the development of the administrative frameworks to make provision for situations concerning immediate or essential data processing in the interest of the public.

Rights and Duties of the Data Principal: In the Bill, there are different rights accorded to data principals, meaning people whose personal information is being processed, including but not limited to the right of access, correction, and erasure of personal data and the right to appoint a person to exercise those rights in their own incapacity or death. The Bill also imposes duties on data principals, on false claims or impersonation, which attracts a fine. These two sides of rights and obligations reflect how administrative law balances individual freedom with responsibility, being fair and protecting against the abuse of data rights.

Duties of Data Fiduciaries: The Bill brings various liabilities upon data fiduciaries, in which parties involve themselves in defining the purpose as well as the process in collecting data. Ensure that the correctness of data is maintained and be able to develop some kind of security measures as such incidents are reported to the Board of India's Data Protection Board. It is here that administrative law plays a vital role, as it requires check and balance and directs compliance and ensures the fiduciary safeguards personal data and becomes transparent. The fiduciary is also governed by the principle of data minimization and limitation of storage. This is in line with international standards in data protection.

Transfer of Personal Data outside India: The Bill governs the cross-border data transfer. In this, the Indian government has identified countries to which data can be transferred. This administrative control over international data movement is essential so that the measures of data protection remain uniform even though the personal data is processed outside Indian jurisdiction. It depicts how, through legislation, the administrative bodies may manage the cross-border challenges emanating from global data processing activities.

Exemptions: It further grants exemptions: the obligations of data fiduciaries and the rights of data principals are not applicable, mainly in cases relating to national security, public order, legal rights enforcement, or research. These exemptions will avoid an administrative law that cannot find exceptions in the public interest, and turn, prevent important state functions from being thwarted while preserving core data protection principles.

Data Protection Board of India: The Bill aims to put in place the Data Protection Board of India-an administrative authority which shall oversee and ensure compliance with the laws, investigate breaches, and ensure penalties are levied against those breaching this authority.[19]

The powers given to the Board in the Bill, including issuing directions in case of breaches and complaints from data subjects, fall in line with the role that administrative bodies have played in overseeing and implementing regulations, since administrative law tries to deal with issues of new technological challenges.

Penalties: The Bill also imposes stringent punitive provisions in the event of non-compliance, which may reach an amount of up to Rs 500 crores for significant breaches like failure to take measures regarding security. Such strong deterrents are through the enforcement mechanism managed through the Data Protection Board, thereby ensuring compliance with the law. This also underscores that the role of

administrative law would also be vital in matters of accountability and obedience to the regime for data protection in the digital era On the whole, the Digital Personal Data Protection Bill, 2022 may be seen as a holistic response from the administrative wing to the emerging threats posed by technology in the protection of personal data.

Conclusion

Rapid innovation in technology has made data protection an intrinsic element of privacy in India. The growth of privacy as a legal right under Article 21 of the Constitution depicts the growing role of administrative law in dealing with challenges arising from the digital world. Programs like Aadhaar have improved identification in India, and judicial interventions like the K.S. The Puttaswamy v. Union of India case and data protection have thus strengthened the right to privacy as a fundamental right. India has made commendable steps in formulating laws intended for the safety of data, including what it has proposed with the Personal Data Protection Bill, 2019, and the Digital Personal Data Protection Bill, 2022, which deal with essential issues concerning consent, handling of data, and rights of individuals. Nevertheless, it is still in the developing stages as far as a comprehensive data protection framework is concerned. The newly proposed Digital Personal Data Protection Bill, 2022 represents India's further response to the vicissitudes created by the digital era as shown by aligning to international norms such as GDPR while focusing mainly on the principles of informed consent and accountability. Therefore, the said hypothesis that India does not have good data protection laws is not correct. Administrative law has been a vital source of response to technological challenges and, even though the completely all-inclusive legal framework is still in the offing, India's consistent effort does present a very good commitment toward protecting data protection in approaching emerging technologies. The legislative developments symbolize that India is moving towards developing a more structured and effective data protection regime.[20]

References:

[1] Solove, D. J. A Taxonomy of Privacy. University of Pennsylvania Law Review 2006, 154 (3), 477-560.

[2] Konvitz, M. R.: Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No.

2. (1966) p. 272

[3] J. P Balsdon,. V. D. Roman Private Life and Its Survivals. In Roman Civilization: Selected Readings; Kagan, D.; Viggiano, G., Eds.; Columbia University Press: New York, 1960; pp 231-248.03.

[4] H Nissenbaum, A Contextual Approach to Privacy Online. DAEDALUS 2011, 140 (4), 32-48.

[5] Samuel D. Warren, and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5 (1890): 193-220. https://harvardlawreview.org/wp-content/uploads/2012/12/1939-1940_4_1930-1939.pdf#page=136.

[6] M.P. Sharma vs. Satish Chandra AIR 1954 SC 300.

[7] Kharak Singh v. State of U.P (1997) AIR 568.

[8] Rajagopal v. State of Tamil Nadu (1994) 6 SCC 632.

[9] Gobind v. State of M. P (1954) S.C.R. 1077.

[10] Justice K. S. Puttaswamy (Retired.) and another. v Union of India and others, (2017) 1 SCC 10.

[11] Ministry of Electronics and Information Technology, Digital Personal Data Protection Bill, 2022.

[12] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (under IT Act, 2000).

[13] Nivedita Baraily, An Analysis of Data Protection and Privacy Law in India.

[14] Upasana Sharma & Aniket Singhania, The Personal Data Protection Bill, 2019: An Overview, Mondaq (Jan. 13, 2020),

[15] PSR legislative research on, Joint Parliamentary Committee

[16] Data Security Council of India https://www.dsci.in/ (last visited 25/04/2023)

[17] Chapter VI of Personal Data Protection Bill, 2019

[18] National Institution for Transforming India. (2020). Data Empowerment and Protection Architecture (DEPA): A Policy Framework for Empowering Residents with Control over their Personal Data. New Delhi: NITI Aayog. https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf.

[19] Upasana Sharma & Aniket Singhania, The Personal Data Protection Bill, 2019: An Overview, Mondaq (Jan. 13, 2020),