LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

The Interplay Between the Right to Privacy and Data Protection: An Analysis of the Digital Personal Data Protection Act, 2023

Author
Shubham Aggarwal
Dr Prateek Deol

The Interplay Between the Right to Privacy and Data Protection: An Analysis of the Digital Personal Data Protection Act, 2023

Shubham Aggarwal
SRM university Delhi NCR

Dr Prateek Deol
Associate professor
SRM university Delhi NCR

Abstract

The rapid expansion of digital technologies and data-driven governance has brought the relationship between the right to privacy and data protection into sharp constitutional focus in India. This research paper examines the interplay between these two closely connected yet distinct concepts, particularly in light of the Digital Personal Data Protection Act, 2023. It traces the constitutional foundation of privacy as a fundamental right under Article 21, as affirmed in Justice K.S. Puttaswamy (Retd.) v. Union of India, and analyses how data protection has evolved as a statutory mechanism to operationalize this right in the digital era.

The study critically evaluates the key features of the 2023 Act, including consent-based data processing, obligations of data fiduciaries, rights of data principals, and the role of regulatory authorities. It highlights the Act's attempt to balance individual autonomy with state interests such as governance, security, and economic development. However, the paper also identifies significant concerns, including broad state exemptions, limitations on user rights, and potential gaps in enforcement and accountability mechanisms, which may dilute the substantive protection of privacy.

By situating the Indian framework within comparative global standards, the research underscores the need for a robust and rights-oriented data protection regime that meaningfully enforces privacy safeguards. It argues that while the Digital Personal Data Protection Act, 2023 marks a significant legislative step, its effectiveness depends on principled implementation, judicial scrutiny, and continuous refinement. The paper concludes that a harmonious integration of constitutional privacy and statutory data protection is essential to ensure individual dignity, informational autonomy, and trust in the digital ecosystem.

Keywords: *Right to Privacy, Data Protection, Digital Personal Data Protection Act, 2023, Informational Privacy, Consent, Data Fiduciary, Constitutional Law, Puttaswamy, India.*

Data Privacy

We depend on facts rather than subjective beliefs, as they are more trustworthy and predictable. Utilizing the existing data, one can forecast results, derive insights for enhanced corporate performance, and formulate improved strategies. Nonetheless, improper data management can be equally detrimental. Data possesses significant power; nevertheless, legal frameworks necessitate that it is substantiated by proof. Consequently, regulations for data protection and privacy have been established, and India has ultimately ratified its long-awaited legislation in this domain. [1]

The two elements involved are privacy and data protection. The timing, method, and volume of personal data shared and exchanged by a consumer with third parties are key determinants of data privacy. Specific information is classified as personal data, including an individual's name, residence, ethnicity, telephone number, and marital status. With the increasing number of internet users, there is an urgent necessity for legislation to safeguard personal information. Data privacy is not a recent phenomenon. In 1984, privacy was formally acknowledged in Article 12(4) of the UDHR. In 1980, the OECD promulgated rules for the secure transference of personal information across international boundaries. Germany commenced the development of national data privacy legislation in 1970, with various other nations.

The pivotal General Data Protection Regulation (GDPR) established new standards for the protection and privacy of personal information upon its implementation on May 25, 2018. In the discourse around privacy, several Indian courts have affirmed its status as a fundamental right protected by Article 21 of the constitution, whilst others have questioned this assertion. In 2017, the landmark case of ***K.S. Puttaswamy v. Union of India***[2] (2018) recognized the right to privacy as a fundamental right protected by Article 21. Several privacy-related statutes, like the Information Technology Act of 2000 and the Indian Penal Code of 1860, exhibit significant challenges. However, there was no singular, comprehensive statute that addressed the matter. On August 9, 2023, India enacted a comprehensive data protection and privacy law following three unsuccessful efforts and seven years of deliberation. On August 1, 2023, the Indian Parliament enacted the Digital Personal Data Protection (DPDP) Act, 2023.

---

[1] Adriana-Maria Sandru & Daniel-Mihail Sandru, 'Humanitarian Law and Personal Data Protection' (2018) *Pandectele Romane* 58, 61.

[2] AIR 2017 SC 4161

Only one Over five years of consideration were devoted to enacting the new legislation. It protects personal information in a manner unprecedented by any prior legislation in India.2. The primary inquiry of this paper is whether the protracted deliberations culminated in a "good" law, defined as one that adequately protects personal data while reconciling "the right of individuals to safeguard their personal data" with "the necessity to process such personal data for legitimate purposes," as articulated in the law's preamble.

The document commences by delineating the principal characteristics of the law and juxtaposing it with earlier iterations, including the official 2019 draft presented by the administration to Parliament. In the subsequent section of the study, the DPDP Act is examined from two distinct perspectives. The document commences by delineating certain potentially problematic aspects of this regulation to facilitate comprehension of its implications for enterprises, consumers, and the Indian government. Secondly, it situates the regulations within the framework of the discussions and advancements that have occurred over the past five years. The 2023 legislation, presented as the second version of the proposal to Parliament, is the fourth in total. In 2018, a consortium of specialists released an initial draft for public discussion following its development.

The government's iteration of the bill, the Personal Data Protection Law, 2019, was introduced to Parliament in 2019. Following an investigation by a parliamentary committee, which revealed its findings in December 2021, the government retracted the bill and presented a new draft, the Digital Personal Data Protection bill, 2022, for public commentary in November 2022.

In comparison to the earlier drafts, this version is markedly distinct. This proposal is the basis for most of the 2023 legislation. Nonetheless, it has certain supplementary regulations relevant to the issues our research aims to address. The four versions were preceded by the 2017 ruling of the Indian Supreme Court in the matter of Justice K.S. Puttaswamy and Anr. v. Union of India and Ors.7. The ruling asserts that the right to privacy includes both the right to life and the right to privacy. The decision, however, did not specify the precise extent of the right to privacy or the particular methods necessary to safeguard this right. The government initially presented the Personal Data Protection Bill, 2019, to Parliament in December 2019. The Data Protection Authority (DPA), a comprehensive data protection body, was intended to oversee cross-sectoral, economy-wide data protection legislation in this extensive version. The 2019 Act established the foundation for prevention.

It mandated specific responsibilities for companies that gather personal data, including notifying individuals and acquiring their consent, securely maintaining

accurate data, and utilizing it just for the purposes outlined in the notice. Besides eradicating data after its utilization, firms were required to permit users to view, delete, and transfer their data. This law mandates businesses to implement grievance procedures, enforce "privacy by design" regulations, and uphold security and transparency standards. Additionally, it introduces a new occupational category called "consent managers," who serve as intermediaries between individuals and businesses to obtain and provide consent.

The legislation created distinct classifications of personal data and required enhanced safeguards for "sensitive" and "critical" data. Certain companies were suggested to be classified as "significant data fiduciaries," with supplementary responsibilities including completing data audits, assessing data impact, and registering in India. The DPA possesses the right to levy fines on enterprises that fail to adhere to these standards. The suggestion additionally suggested criminalizing the act of deanonymizing users from anonymised databases. A segment of the 2019 legislation eliminated the requirement for notification and consent for specific organizations and individuals to perform lawful state functions, deliver medical and health services during epidemics or emergencies, reestablish public order, process employment-related data, prevent and detect unlawful activities, promote whistleblowing, and restore credit[3]

A component of the 2019 bill granted the government authority over non-personally identifiable data. In accordance with its stated guidelines, it authorized the government to solicit certain nonpersonal data from private firms. The 2019 legislation instituted a comprehensive, cross-sectoral framework cantered on the rights of individuals or consumers (termed "data principals") and the preventative responsibilities of enterprises (designated "data fiduciaries"). The Srikrishna Committee, established by the Ministry of Electronics & Information Technology in July 2017 and chaired by Justice B.N. Srikrishna, a retired Supreme Court judge, was the principal source for the 2018 bill draft that formed the foundation of this regulatory framework. Significant regulatory modifications that the group developed gained traction and became the foundation of its recommendations. The General Data Protection Regulation (GDPR) of the European Union (EU) was particularly notable. While the foundational preventive framework of the 2019 bill received commendation, its broad extent presented challenges. Both large and small firms in the economy would have experienced the repercussions of the extensive compliance duties it mandated. It also advised establishing a DPA with comprehensive regulatory and supervisory authority. These regulations would have further elucidated the law's already comprehensive compliance requirements. Due to the bill's distinctiveness and the lack of prior

[3] Addison Litton, 'The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression' (2015) 14 *Washington University Global Studies Law Review* 799, 720.

experience in implementing a data privacy law of this nature, there were significant risks of either overregulation or under regulation.[4]

Article 21

Confidentiality, anonymity, and seclusion have broadened the fundamental definition of privacy beyond only limiting access to oneself. Privacy enables decision-making, establishing personal boundaries, and managing shared information. The extensive adoption of technology in contemporary times has engendered significant privacy issues, prompting global regulatory efforts to protect personal data. However, enacting effective legislation is challenging when technological advancements, such as AI-generated deepfakes, occur at an accelerated rate. This necessitates the acknowledgment of India's Right to Life and international privacy regulations inside the constitution to protect persons from exploitation and uphold their dignity. A multitude of circumstances has highlighted the necessity for statutory protections of privacy rights to guarantee that individuals retain control over their personal data and the parameters of their relationships.

The capacity to maintain personal information confidentiality and to exercise autonomy in decision-making without external interference is essential to human dignity and individual freedom. Secondly, these safeguards inhibit unauthorized entities from accessing, utilizing, or revealing personally identifiable information, hence fostering responsible data stewardship. Thirdly, they reconcile individual privacy with social demands for accountability and security. Moreover, legal systems include mechanisms for the protection of individual rights and the seeking of remedies for infringements via civil litigation or complaints submitted to regulatory authorities. Regulatory regimes must adapt to handle emerging privacy problems resulting from technology improvements. The absence of sufficient legal frameworks protecting data privacy rights endangers personal freedom and democratic values globally. As the right to privacy evolves to include data protection in an increasingly globalized and technologically advanced society, it is essential that these rights be enshrined in the constitution to affirm their significance. The democratic nations now advocating for the establishment of this right as fundamental are those from whence this concept comes. The primary problem will be reconciling individuals' fundamental right to privacy with the requisite limitations imposed to maintain public safety and order.

This necessitates appropriate policy responses irrespective of a nation's legal structure. Two significant international treaties that affirm the notion of an

[4] Aimee Boram Yang, 'China in Global Trade: Proposed Data Protection Law and Encryption Standard Dispute' (2018) 4 *ISJLP* 897, 901.

inherent right to privacy for all individuals are the UDHR and the ICCPR. The Universal Declaration of Human Rights (UDHR) was ratified by the United Nations General Assembly in 1948 and contained the following stipulation: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his integrity and reputation." This stipulation unequivocally established privacy as an inviolable human right, protected from arbitrary intrusions. [5]

Article 17 of the 1966 ICCPR states, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor and reputation," so augmenting the UDHR and providing more details regarding the right to privacy. The ICCPR emphasizes the significance of safeguarding individuals' residences, private life, communications, and personal information from unlawful and arbitrary invasions. Article 17 of the ICCPR mandates that all ratifying governments protect the right to privacy. In accordance with international law, they are required to safeguard inhabitants from illegal intrusions into their private life.

The UDHR and ICCPR exemplify the UN's dedication to preserving freedom, autonomy, and human dignity globally through their recognition and protection of privacy. These international agreements recognize privacy as a fundamental human right and emphasize the necessity of personal autonomy, confidentiality, and protection from unwarranted intrusion into one's business. The incorporation of privacy rights in the UDHR and ICCPR illustrates a deliberate endeavour to protect individuals' right to privacy, which is essential for a just and equitable society. The Right to Privacy as a Fundamental Right in India the Indian judiciary has established crucial rulings that have entrenched the right to privacy as a fundamental right, significantly contributing to its evolution over time. Prior to explicitly designating privacy as a separate right, the Supreme Court acknowledged its intrinsic existence within other constitutionally safeguarded rights, including the right to life and personal liberty as articulated in Article 21. A significant turning point occurred in the PUCL vs. Union of India lawsuit in 1997, commonly referred to as the telephone tapping cases. This was subsequent to the 1975 landmark ruling by the Supreme Court in ***Gobind v. State of MP***,[6] which established the compelling state interest test. It emphasized the necessity of well-justified state aims superseding individual liberties. This ruling reinforces the constitutional standing of privacy rights by clearly affirming that persons possess a right to privacy concerning the content of their telephone conversations.

---

[5] Alan F. Westin, *Privacy and Freedom* 33 (1967); Andrew J. McClurg, 'Kiss and Tell: Protecting Intimate Relationship Privacy through Implied Contracts of Confidentiality' (2006) 74 *University of Cincinnati Law Review* 887, 901

[6] 1975 (1) ALL LR 752

The 2017 ruling in Justice K.S. Puttaswamy v. Union of India recognized privacy as a fundamental right. The Supreme Court established the foundation for protecting the right to privacy, deeming it essential to life and individual liberty under Article 21, by its unanimous ruling. The rights of freedom of religion, speech, and equality were emphasized, with the interrelation of privacy. The Court emphasized the significance of privacy and its rightful regulation, akin to other rights, underscoring the necessity for balanced governance. Restrictions on personal privacy, as articulated in the Declaration, must be legitimate, proportional, and essential. These decisions have guaranteed that people' private interests are recognized and protected by establishing a robust framework for safeguarding privacy rights from exploitation by governmental and non-governmental actors.

Protection of Indian consumers' personal information has been compromised by many breaches impacting millions in recent years. A multitude of data breaches in recent years has impacted millions of individuals in India. The Indian Computer Emergency Team (Cert-In) is investigating a concerning case involving allegations that an automated Telegram account disseminated personal information, including passport and Aadhaar numbers, of individuals who registered on the COVID-19 vaccination portal (the "COWIN" portal). The Employees' Provident Fund Organization, BSNL consumers, and corporations such as Air India and Reliance are purported victims of a corrupted database that was disclosed on Github. The resolution of these breaches and the safeguarding of individuals' personal information by authorities remains ambiguous. Furthermore, it has been revealed that the personal information of 110 million clients from the mobile wallet and payment application MobiKwik was sold on a website operated by dark web hackers. This extensive dossier comprises Know Your Customer documentation, credit card information, Aadhaar numbers, and mobile devices linked to MobiKwik wallets. The incidences have significantly impacted data security and privacy in India. Numerous Indian regulations inadequately safeguard both personally identifiable and anonymous information. The Information Technology Act of 2000 encompasses various regulations pertaining to data security and preservation. The BN Srikrishna committee introduced the Personal Data Protection Bill in 2017 as a result of data protection activities. Before its retraction, it was amended and renamed the Data Protection Bill 2021. It was formerly referred to as the PDP Bill 2019. Reintroduced in 2023, it was ultimately ratified as the Digital Personal Data Protection Act; nonetheless, criticism emerged due to insufficient legislative discourse. All types of digital personal data, encompassing identifiers and pseudonymized information, are regulated by the Digital Personal Data Protection Act of 2023 in India.[7]

[7] Alex B. Makulilo, 'The Quest for Information Privacy in Africa' (2018) 8 *Journal of Information Policy* 317, 337.

Data managed within India and data processed externally are both governed by its jurisdiction when products or services are offered to Indian citizens. Conversely, data that is publicly accessible or employed for personal use is exempt from this regulation. The Act strongly emphasizes the concepts of limiting goals and decreasing data. Data minimization prevents unnecessary data collection by ensuring that only pertinent information is gathered and processed, while purpose limitation stipulates that personal data may only be utilized for specified, lawful purposes with informed consent. This law grants data principals, referred to as users or consumers, specific rights, including the right to access their personal data, the right to request repairs or updates to their data, and the ability to file complaints over data misuse. Furthermore, they should refrain from fabricating complaints. Officials responsible for the collection, storage, and processing of personal information must comply with rigorous regulations, including notifying appropriate authorities in the event of a security breach, deleting data upon an individual's request, and securing consent prior to using information related to minors.

Specific start-ups, national security issues, certain legal and international transactions, and non-individualized researchers may receive exemptions from governmental authorities. The Data Protection Board of India (DPB) have significant powers to administer the Act, including a multi-tiered appeals mechanism, investigation and sanctioning of violations, and the requirement of remedies for breaches. The Act exemplifies India's dedication to data protection in the digital age by balancing privacy and information dissemination. However, persistent dialogue and modifications are essential to guarantee its effectiveness and continual improvement. To keep pace with rapid technological advancements, numerous countries have established legislative frameworks to safeguard people' personal information, including the European Communities Data Protection Act of 1998 and the European Union General Data Protection Regulation (GDPR). Self-regulation activities may also enhance the privacy issue. The judge should expand the right to privacy to include data privacy, as politicians have neglected this responsibility. [8]

The issue of international data protection regulations that inhibit individuals from pursuing privacy claims beyond their jurisdiction necessitates the establishment of a fundamental right to data protection, rather than relying on judicial resolution. For instance, Sweden possesses constitutional safeguards against unwarranted intrusions into privacy, included in its enumeration of fundamental liberties and rights. A new data protection clause has been incorporated into the Portuguese Constitution. A similar modification may occur with Article 21 to

[8] Alina Savoiu & Catalin Capatina Basarabescu, 'The Right to Privacy' (2013) *Annals Constantin Brancusi University of Targu Jiu Juridical Science Series* 89, 101.

integrate conventional privacy standards with contemporary data protection methodologies. To enhance its usability and adaptability, India may consider implementing comprehensive data protection regulations. Approximately one hundred thirty-seven nations have implemented the General Data Protection Regulation (GDPR) established by the European Union, according to UNCTAD. Just as people has the right to access, rectify, transfer, and delete their personal information, businesses are also obligated to adhere to the same regulations on access to their customers' data.

European legislation is presently being implemented on a supranational level. For instance, companies worldwide, not exclusively in Europe, may encounter repercussions if they improperly handle the personal data of their citizens. The General Data Protection Regulation (GDPR) and the European Charter of Fundamental Rights demonstrate Europe's commitment to safeguarding personal information. These policies empower citizens by providing a robust tool and a contingency plan for violations, thereby establishing elevated standards for compliance. Data protection was among the initial fundamental rights established by an international document, the European Union Charter of Fundamental Rights. It has been ratified by all members of the European Union. Initially, it came in the form of mere declaration and became binding upon the states later. Although prior to this charter, the EU already had a comprehensive law on this subject in place, but it was not constituted as a constitutional right which was sone after the Lisbon Treaty was put into effect in 2009 to constitutionalise the data privacy in the primary EU law. The specific article of the charter which entails this right is Article 8, which states that "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority".[9]

These developments have led to the position of EU legislation as one of the most updated and innovative in the world with respect to data protection. The ECJ's rulings have been crucial in structuring legislation by interpreting the law and elucidating its intent, which is to safeguard individuals' fundamental right to privacy in the digital realm. The cases Commission v. Austria and Commission v. Germany illustrate the importance of the right to data privacy by holding National Data Protection Authorities accountable when their charters and directives violate this right. The European Court of Justice (ECJ) has embraced a

[9] Antonio Tavares Paes, 'Privacy and Data Protection in Brazil' (2018) 5 *Journal of Law & Cyber Warfare* 225, 220.

stringent interpretation of the right to data privacy to eliminate any potential loopholes, particularly when assessing member state policies that may violate this right or scrutinizing the actions of state agencies. Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others was a case that deemed the entire Irish Act illegal. The General Data Protection Regulation (GDPR), owing to its transnational nature, applies extraterritorially to non-EU organizations that access the data of EU persons. This has highlighted the necessity for an international viewpoint and cooperation. One method to achieve this is by enacting legislation that prioritizes data privacy, similar to the approach of the European Union. The anticipated and likely result of such EU legislation is the convergence of laws, particularly with the United States. Consequently, the legislative frameworks of specific US states have increasingly aligned with those of the EU.

The European Union has taken the initiative in addressing data privacy legislation issues by establishing and implementing a "gold" standard. Germany has adopted a novel strategy by integrating federal and state data privacy legislation. The German Federal Constitutional Court has often emphasized the need to constitutionalize informational self-determination and the importance of data protection organizations. Germany has been a forerunner in this domain for other federations, including the EU. Efforts have been made to establish a compromise between data privacy and national security or law enforcement in governing government entities with contemporary legislation appropriate for the digital age. Particularly regarding the constitutional recognition of data privacy rights, adherence to these rights has fallen short compared to Germany, the EU, and other member states. Although these rights are safeguarded by legislation, they are not regarded as fundamental rights in the same manner as they are in the United States, Canada, India, and other nations. Regrettably, the United States does not possess a cohesive data privacy regulation due to its fragmented approach to the matter. This difference elucidates why data privacy regulations are most lenient in the corporate sector. Certain personal information is safeguarded by legislation, including the Privacy Act of 1974 and the Computer Matching and Privacy Act; nevertheless, these statutes pertain exclusively to federally maintained data and do not extend to private individuals or entities. Restrictions concerning commercial enterprises are unique to the industry rather than being part of the overarching data privacy policy. [10]

This has resulted in a widespread belief that the US tradition is predominantly self-governing. Several states have enacted laws designed to safeguard the privacy rights of people and consumers, representing a commendable

[10] Anupam Chander & Molly Land, 'United Nations General Assembly Resolution on the Right to Privacy in the Digital Age' (2014) 53 *International Legal Materials* 727, 735.

advancement. Nonetheless, a policy gap persists, prompting the Senate to likely engage in further discussions about the establishment of domestic and international data protection policies. Given the challenges posed by the rapid advancement of technology, it is evident that the right to privacy regarding personal information should be clearly enshrined in the constitution. In conclusion, this analysis demonstrates that nations are grappling to reconcile data privacy with other fundamental rights. Numerous democracies contend that ensuring this right would conflict with other traditional governmental objectives, such as national security, and hence have opted not to incorporate it into their constitutions. Upholding democratic values while maintaining this privilege is of utmost importance. This initiative aims to address possible privacy issues associated with breakthrough technologies such as AI, and it is not an inherent right. Furthermore, opportunities to include previously absent laws during their enactment are now present. [11]

The right to privacy can similarly be enhanced in this manner. The significance of data protection is escalating due to the rapid expansion of personal data and technical advancements. To confront the problems of the digital age, democracies must endeavour to alter their constitutions and enact laws that accord this right the significance it warrants. Each statute offers differing levels of protection. To prevent such differences, the optimal approach to managing data privacy is to implement universally accepted regulatory frameworks. Countries should seize the opportunity to examine progressive legislation in other jurisdictions and cultivate a more inclusive, equitable, and accessible internet, particularly in light of the increasing significance of this right as evidenced by their own actions.

Violation of Confidentiality and Privacy

The phrase "data breach" refers to the unlawful access to personal information. Thus, a data breach may transpire if confidential, sensitive, or protected information is disclosed. In November 2021, 86.63 million Indian consumers experienced data breaches, positioning India as the third-highest country globally for this metric. A data breach may inflict considerable damage to both financial resources and security, therefore becoming a significant worry. Bank fraud and counterfeit identification card schemes are but two instances of the numerous unlawful applications of publicly accessible information. Electronic devices, including smartphones, tablets, and computers, have become essential in contemporary society. Data becomes readily accessible to everyone subsequent to a consumer downloading an application. Information including age, educational attainment, gender, residence, interests, and Aadhar number is often provided.

[11] Asang Wankhede, 'Data Protection in India and the EU: Insights in Recent Trends and Issues in the Protection of Personal Data' (2016) 2 *European Data Protection Law Review* 70, 73.

This typically incurs a substantial expense. Therefore, rigorous legislation is essential to prevent data breaches and unlawful dissemination of information. In the occurrence of a data breach, various categories of information may be disclosed, including: Financial data encompasses invoices, bank account information, tax returns, credit card numbers, and financial statements. Personal health information, or medical records, is defined under the US HIPAA standard as "information created by a health care provider [that] pertains to the past, present, or future physical or mental health or condition of any individual." Personally identifiable information (PII) denotes any data that can identify, contact, or locate an individual. Design files, customer databases, legal contracts, patents, and proprietary information exemplify intellectual property. Sensitive and classified information, typically pertaining to military or political matters, encompassing confidential documents, agreements, and meeting records. Confidentiality and information security Personal information of individuals should not be easily accessible to third parties due to concerns of data security and privacy.[12]

A significant amount of control over such data should reside with each individual. Measures exist to avert the unlawful utilization of personal data on the internet and other electronic platforms. Security procedures are established to safeguard personal data, encompassing administrative, technical, and physical aspects. Privacy and data security are inseparable. Personal information on individuals can be located in directories, websites, educational institutions, financial institutions, and surveys. This encompasses elements such as names, residences, telephone numbers, occupations, familial relations, and preferences. Dissemination of this information may result in unsolicited commercial calls and other violations of privacy. The Information Technology (Amendment) Act of 2008 delineates the essential tenets of data protection and privacy while instituting criminal and civil liabilities for legal violations.

Kharak Singh V State of UP

Kharak Singh was acquitted from a dacoity inquiry due to insufficient evidence; yet, the U.P. Police created a "history sheet" against him in accordance with Chapter 20 of the U.P. Police Regulations. These constraints facilitated the monitoring of individuals who were either recognized for committing recurrent offenses or suspected of being at risk of doing so. The police adhered to Regulation 236 of the U.P. Police Regulations during the surveillance operation. This surveillance included covert trips to the petitioner's residence, frequent interrogations, nocturnal home visits, and monitoring and confirming his location. The petitioner asserts that Chapter 20 of the U.P. Authorities

[12] Stephen J. Balla, 'Administrative Procedures and Political Control of the Bureaucracy' (2012) 92 *American Political Science Review* 663, 670.

Regulations questions the legality of such monitoring by authorities. The central issue is whether the controversial concept of "surveillance" in Chapter 20 of the U.P. Police Regulations violates the fundamental rights enshrined in Part III of the Constitution. Contentions The petitioner claimed that every provision of Regulation 236 infringed upon his constitutional rights to "personal liberty" (Article 21) and "to move freely throughout the territory of India" (Article 19(1)(d)). He claimed that psychological inhibitions and a deficiency of "free movement" could arise from stalking. The Respondent-State contended that the Regulations were lawful as they did not infringe upon any fundamental rights. [13] They argued that the Regulations could be deemed "reasonable restrictions" on the pertinent rights, as they were established "in the interest of the general public and public order" and facilitated the police in performing their duties effectively, despite encroaching upon fundamental rights. Selection The Court promptly concluded that the Regulations were executive in nature rather than legislative, as they lacked any statutory foundation, whether delegated or otherwise. Moreover, the Regulations did not satisfy the stipulations of Articles 19(2)-(6) and did not constitute law as defined by Article 21's "procedure established by law," as they were only departmental guidelines aimed at instructing police officers. If the Court determines that the Regulations violate basic rights, the Respondent would forfeit the ability to invoke "reasonable restrictions," which is applicable only to properly enacted "law." The Court assessed the legality of each provision of Regulation 236. The Court determined that a psychological impediment to action is not safeguarded by Article 19(1)(d), and that clause (a)—permitting covert picketing of suspects' residences—and clauses (c), (d), and (e)—designed to monitor habitual offenders—did not physically obstruct the suspects' movement. According to the language in Article 21, the suspect's "personal liberty" was similarly safeguarded. The Court considered whether clause (b), which allowed history-sheeters to visit residents' homes nightly, infringed upon Articles 19(1)(d) or 21. The Court determined there was no breach, as Article 19(1)(d) exclusively addressed unrestricted physical movement, not psychological confinement. In interpreting Article 21, the Court examined both United States Supreme Court precedents and the historical context of the term "personal liberty." The court upheld its prior decision that, per Article 21 of the United States Constitution, "life" encompasses not only the right to the continuation of a person's biological existence but also the right to retain all of one's bodily organs, including limbs, as stipulated in the Fifth and Fourteenth Amendments.

[13] Brent Snook, Joseph Eastwood, Paul Gendreau, Claire Goggin & Richard M. Cullen, 'Taking Stock of Criminal Profiling: A Narrative Review and Meta-Analysis' (2007) 34 *Criminal Justice & Behavior* 437, 455

This was achieved by referencing Justice Field's ruling in Munn v. Illinois ((1877) 94 U.S. 113). Justice Frankfurter articulated in Wolf v. Colorado ((1949) 338 U.S. 25) that "the concept of ordered liberty" inherently encompasses "the security of one's privacy against arbitrary intrusion by the police," which is "fundamental to a free society." Furthermore, it claimed that the Indian Constitution lacks a provision analogous to the Fourth Amendment of the US Constitution, which protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In addressing notions of individual liberty, the Court used the English common law adage "every man's house is his castle." [14]Upon examining the interrelation of the "liberties" in Articles 19(1) and 21, the Court concluded that whereas Article 19(1) addressed specific freedoms, Article 21 employed the term "personal liberty" to encompass all of them. The phrase "personal liberty" aims to advance the fundamental objective of safeguarding individual dignity, as stated in the Preamble to the Constitution.

The Court declared Clause (b) of Regulation 236(b), which permitted domiciliary visits, unconstitutional for contravening Article 21, as previously elucidated. The remaining sections of Chapter 20 of the U.P. Police Regulations were affirmed based on the rationale that "the right to privacy is not an enshrined right within our Constitution" and that an individual's personal space may only be intruded upon to ascertain their whereabouts. The minority's opinion states, "Although our Constitution does not explicitly recognize a right to privacy as a fundamental right, this right is a crucial component of personal liberty." Referencing Justice Frankfurter's decision in Wolf v. Colorado, it asserted that "nothing is more detrimental to a man’s physical happiness and health than a calculated interference with his privacy." This illustrates the significance of safeguarding individuals' privacy from governmental intrusion without a warrant. It was determined that "personal liberty" included the lack of both direct and indirect constraints on mobility to an adequate extent. The minority determined that Regulation 236(b) was null and unlawful since it continuously contradicted Articles 19(1)(d) and 21.

Moreover, they indicated that all subclauses of Regulation 236 were intended to fulfill the same objective, rendering any effort to divide the monitoring process into distinct outcomes futile. The court determined that Regulation 236 infringed against the First Amendment's right to free speech by obstructing individuals from expressing their genuine and personal viewpoints.

[14] Brian Gorlick, ‘Human Rights and Refugees: Enhancing Protection through International Human Rights Law’ (2000) 69 *Nordic Journal of International Law* 117, 126.

K S Puttaswami Case

On August 24, 2017, a nine-judge bench of the Indian Supreme Court unanimously upheld the right to privacy for all persons as enshrined in the Indian Constitution, as evidenced in the case of Justice K.S. Puttaswamy vs. Union of India. Despite a unanimous finding, there were six distinct decisions that concurred. Justice Chandrachud authored the ruling in conjunction with Justices Khehar, Abdul Nazeer, and R.K. Agarwal. The remaining five justices expressed their dissent in individual concurring opinions. The many perspectives and privacy concerns articulated in the Bench's concurring opinions are apparent.[15]

The judgments delivered by judges Bobde, Chelameshwar, and Chandrachud. The three rulings M.P. Sharma vs. Satish Chandra, Kharak Singh vs. State of U.P., and Govind vs. State of Maharashtra—intellectually affirm India's right to privacy. The M.P. Sharma verdict does not determine whether the constitution guarantees the right to privacy. Although Kharak Singh asserts that "life" under Article 21 does not equate to mere "animal existence," this assertion is undermined by the ruling that deemed the regulation permitting domiciliary visits unconstitutional due to privacy concerns, despite the absence of explicit mention of the term, indicating that privacy was not constitutionally safeguarded. We dismiss the two assertions that the Indian Constitution fails to ensure people' right to privacy, as they are mutually exclusive. The fundamental values of freedom and dignity encompass an individual's intrinsic right to autonomy. The listing of many liberties in Article 19 does not diminish the breadth and intricacy of Article 21. Some fundamental rights are intrinsic to human nature; this underpins privacy, which stems from an individual's capacity to govern his own identity. Similar to other rights in Part III of the Constitution, privacy cannot be violated without prior consideration of legitimate state interests and adherence to the legal standards of due process and procedure. To prevent similar legal issues related to infringing upon individuals' rights to life and personal freedom, the state must uphold their right to privacy.

Human life and individual liberty are inalienable, signifying that they do not derive from the constitution or the state but exist autonomously from both. In the absence of legitimate legal justification, no reputable nation would contemplate the occupation of another's territory. The ruling in ADM Jabalpur v. S.S. Shukla, which indicated that the aforementioned rights could be relinquished during an emergency, has been reversed. The right in question is inherently linked to the freedoms outlined in Part III and is derived from the principles of dignity and liberty in the Preamble; thus, the judiciary's recognition of the constitutional protection of a private right does not equate to an encroachment on legislative

[15] Cheng-Yun Tsang, 'From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of FinTech' (2019) *University of Illinois Journal of Law, Technology & Policy* 355, 360.

authority. Concerning sexual orientation, marriage, domestic matters, intimate relationships, and the significance of family life, the fundamental concept of privacy acknowledges that individuals possess authority over crucial aspects of their lives and the maintenance of their autonomy. To maintain its relevance for both the present and future, the Constitution necessitates amendments. Due to the prevalence of both state and non-state entities that regulate social existence and impact individual freedom, the courts must interpret the notion of personal liberty in this era of information technology that governs nearly all aspects of our lives. All individuals, irrespective of their social status or financial capacity, are entitled to the personal space and autonomy that privacy provides. The esteemed Chelameshwar P. The survival of humanity relies on a limited set of fundamental rights enshrined in the Constitution, which also serves to avert governmental abuse of power.[16]

Thus, these rights are acknowledged as essential to their liberty and cannot be revoked. Liberty is the autonomy to act according to one's desires, however privacy is crucial for the actualization of such autonomy. M.P. Sharma cannot be regarded as an expert on the issue of constitutional protection of the right to privacy due to the inaccuracy of that assertion. The right to privacy is founded on individual choice, a secure sanctuary, and the opportunity for quiet reflection to rejuvenate. All fundamental components of an individual's autonomy are encapsulated in the liberties provided under Part III. Unjustified governmental intervention jeopardizes fundamental liberties and human rights in contemporary democracies. Government encroachment on personal liberties, particularly privacy, constitutes a breach of essential rights. Privacy, akin to other fundamental rights, is subject to limitations. It is essential to differentiate among several categories of privacy interests to address them effectively. The courts shall be regulated by the principles of equitable, rational, and just law as stipulated in Article 21. The application of the most sophisticated research methods, driven by significant state interest, is required. Equity Bobde vs All individuals possess inherent moral interests that are protected by natural rights. Certain moral ideals, such as individual liberty and intrinsic value, are generally acknowledged and endorsed. Their right to privacy is intrinsic and inalienable because of the nature of their intimate relationship. Regardless of whether it is derived from common law or statutory law, it must be recognized as a fundamental right and safeguarded by the constitution.

The fundamental and statutory right to privacy is, in essence, inalienable. No alterations have occurred between the two formats. Common law protections extend to individuals, whereas fundamental rights are invoked in response to state

[16] David Wallace & Mark Visger, 'Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community' (2018) 6 *Journal of Law & Cyber Warfare* 3, 5.

actions. The essential element of privacy is the freedom to be solitary and unbothered by external entities. Rest constitutes an essential human right. The concepts of privacy and liberty are closely interconnected, and safeguarding one's privacy is often crucial for the complete enjoyment of one's liberties. Part III comprehensively addresses privacy, as it underpins the rights it safeguards. It is a constitutionally guaranteed fundamental right that cannot be revoked. The examination of the state's plenary powers is contingent upon the acknowledgment of the right to privacy as a fundamental right. No evidence supports the assertion that an individual's right to privacy is absolute and inviolable. Although the liberties enshrined in the Constitution do not extend to specific individuals or groups, individuals nonetheless possess the right to privacy. Consequently, negative liberty, defined as the capacity to abstain from action, encompasses the right to privacy. All human liberties are inherently connected to the right to privacy, as specifically stated in Part III and safeguarded under Article 21.[17]

It appears that enjoyment is limited by its infringement and is distributed over all sections of Part III. Consequently, in addition to being rational, equitable, and just under Article 21, a state action that infringes upon a right must also satisfy the stipulations of the relevant Article.

Civil Liability and Criminal Liability

With the increasing digitalization of personal data, data privacy has gained prominence in India's legal landscape. Civil and criminal liabilities in data privacy arise primarily under the **Digital Personal Data Protection Act, 2023 (DPDP Act)**, the **Information Technology Act, 2000 (IT Act)**, and other relevant laws.

1. Civil Liability on Data Privacy

Civil liability typically involves compensation, penalties, or damages imposed for violating data privacy norms. The key provisions include:

A. Digital Personal Data Protection Act, 2023

- **Section 33**: Imposes financial penalties for failure to protect personal data.
- **Section 34**: A Data Principal (individual whose data is processed) can seek grievance redressal if their rights are violated.
- **Adjudicatory Mechanism**: The Data Protection Board of India (DPBI) handles complaints and can impose civil penalties.

B. Information Technology Act, 2000

- **Section 43A**: Compensation for failure to protect sensitive personal data by a body corporate.

[17] Dhiraj R. Duraiswami, 'Privacy and Data Protection in India' (2017) 6 *Journal of Law & Cyber Warfare* 166, 168.

    - Companies must follow "reasonable security practices"; failure results in liability for damages to affected individuals.
- **Section 72A**: Unauthorized disclosure of personal information leads to civil and criminal penalties.

C. Contractual Liability

If a party violates a data protection clause in a contract (e.g., failing to maintain confidentiality), they can be sued for breach of contract under the **Indian Contract Act, 1872**.

2. Criminal Liability on Data Privacy

Criminal liability arises when data breaches involve fraud, identity theft, hacking, or intentional misuse of data.

A. Information Technology Act, 2000

- **Section 66**: Hacking with dishonest or fraudulent intent—punishable with imprisonment up to **3 years** and/or a fine.
- **Section 66C**: Identity theft—unauthorized use of someone's personal identity credentials can lead to imprisonment of **up to 3 years** and a fine of **₹1 lakh**.
- **Section 66D**: Punishment for cheating using impersonation via electronic means—punishable with **up to 3 years** in prison and a fine.
- **Section 67**: Publishing obscene or offensive content—punishable with **up to 5 years** of imprisonment.
- **Section 72**: Unauthorized access or disclosure of personal information by government officials—**up to 2 years** of imprisonment or a fine of **₹1 lakh**.

B. Indian Penal Code (IPC), 1860

- **Section 419**: Punishment for cheating by impersonation (including digital impersonation)—**up to 3 years** of imprisonment.
- **Section 420**: Cheating and dishonestly inducing delivery of property (including data theft)—**up to 7 years** of imprisonment.

Conclusion

The Indian legislature enacted a contemporary, comprehensible rule delineating the principles of data security architecture following extensive deliberation. Regrettably, the law's brevity and universal applicability constitute certain deficiencies. The Act remains vague due to the postponement of various problems until later changes, suggesting that further work is required. The Indian lawmaker must be held accountable for his reluctance to address the issues raised by this regulation, especially those related to transparency and personal freedom, which are fundamentally limited to processing based on individual consent.

Likewise, the presence of merely two legal foundations results in a significant deficiency of credibility. The system will stay static as long as the legal supervisory body is incapable of establishing soft law. The myriad exclusions to the rule that result in contradicting statutes and legal ambiguity represent the foremost critique of the DPDP. Concerns exist regarding unrestricted government monitoring due to the potential for extensive exclusion of public authorities. We must await the Indian government's approval of the law modifications before gaining further insight into the new data protection framework and the potential resolution of the aforementioned issues. Individuals below the age of 18 are classified as children, and data controllers are required to get verifiable consent from a parent or guardian before to processing their data. Targeted advertising constitutes an additional method via which monitoring children's internet activities is unlawful.

This ban applies to all data controllers, irrespective of whether a corporation explicitly handles kid data or has other signs of collecting and exploiting such data. Consequently, controllers lack plausible deniability if they do not deliberately target children; rather, they must operate under the assumption that they will likely gather and utilize data from minors unless they are unequivocally certain this will not occur. The Act lacks clarity on the procedures a data controller must follow to get "verifiable consent," suggesting that governmental bodies would likely formulate implementing regulations to offer guidance in the future.

The governing body may exclude certain data controllers from these additional responsibilities, contingent upon the type of controller or processor.
For instance, individuals under the age of 15 may necessitate parental consent if an Ed-Tech platform is intended to facilitate their education. However, a controller must demonstrate to the government that its processing techniques are significantly secure to obtain this exemption. The Digital Personal Data Protection Act, 2023 is a pivotal advancement in India's efforts to safeguard personal data amid the evolution of its digital economy. It offers a coherent framework that addresses the requirements of global data flow by integrating

business-friendly provisions with crucial privacy safeguards, rendering it more adaptable than its predecessors and other international regulations like the General Data Protection Regulation (GDPR).
The DPDP Act enables startups and smaller enterprises to save compliance expenses while enhancing data security by establishing adaptable protocols for international data transfers that address the unique issues faced by different data custodians. The criteria for verified parental consent and the rigorous rules for processing children's data demonstrate the government's commitment to protecting vulnerable populations.

The Digital Personal Data Protection Act establishes a secure and thriving digital environment by creating a comprehensive and progressive regulatory framework that adheres to global standards while addressing India's specific needs. After more than ten years of postponement, India is set to revise its data and IT legislation with several amendments. Undoubtedly, the transformation will enable India to emerge as one of the globe's foremost data-driven economies.

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618