CANONSPHERE LAW REVIEW

ISSN: 3107-460X (Online)

CANONSPHERE LAW REVIEW

Volume 1 Issue 4

October to December, 2025

@ 2025 CANONSPHERE LAW REVIEW.
All rights reserved.

TABLE OF CONTENT

S.No	Contents	Page No
1.	Abstract	3
2.	Introduction	4
3.	Historical overview	4
4.	Legal framework and other regulations	6
5.	The paradigm shift: from privacy to data privacy	7
6.	Challenges and emerging concerns	8
7.	Conclusion	9
8.	References	10

CANONSPHERE LAW REVIEW

From Right to Privacy to Data privacy: A paradigm Shift

This short article is written by Dr. Pranjya Paramita Panda, Asst.Professor,Rourkela Law College, M.S. Law University, coauthored by Anusmita Mahanta, a 4th Sem. LL.M. student from P.G. Dept. of Law, Sambalpur University.

Abstract

Digital privacy poses a new challenge in the technology-driven world. The right to Privacy, which is practised under Article 21 of our Constitution, is affirmed as a fundamental right and includes the protection of personal data or privacy of data. But now in this digital world, the major concern is for the security of data. Due to the proliferation of technology and the huge collection and storage of data, people are more aware of the risks and vulnerabilities related to their information and personal data. On one hand, the Right to privacy is a fundamental right, while on the other hand, data protection is a legal framework in this digital Era. Due to growth in digital technologies, it is very challenging nowadays to protect personal Data or Data Privacy, which ultimately leads towards a comprehensive law to regulate the same. And subsequently, in August 2023, the landmark legislation named the DPDP Act,2023, for data protection in India and handling digital data. Strict implementation of the Act will make this paradigm shift from right to privacy to personal data protection very safe and protected. Because nowadays privacy is not just about isolation, but it also refers to empowerment.

Keywords: Fundamental Rights, Privacy, Challenges, Data Protection, Technology

CANONSPHERE LAW REVIEW

Introduction

The most important and core aspect of human life is human dignity and autonomy, which is protected through privacy and prevents external sources from unnecessary intervention. This is also treated as a fundamental need for an individual in society. Traditionally, this privacy right was associated with physical and mental autonomy for protecting people from unwanted disclosure of personal matters. But with the advancement of time, the scope and nature of privacy have gone through an immense transition.

A significant statement by Justice Louis D. Brandeis from the judgment of the U.S. Supreme Court case of Olmstead v. United States, 277 U.S. 438 (1928), where he argued against warrantless wiretapping and stated privacy as a basic right. In that case, he also called it 'the right to be let alone', which was the initiation of privacy laws[1]. In this time, privacy is not limited to physical boundaries, but it is deeply intertwined with the protection of personal data, its use and control over it.

Here, data privacy has emerged as a new edge of individual rights which shows the untouchable reality associated with every possible use of personal information for profit. The transformation is demanding the transforming rules and policies for securing its meaningful rights in this progressive century. The landmark judgement of the Supreme Court, K.S. Puttuswamy(Retd.) vs Union of India,2017, the evolution was well established, where the nine-judge bench declared privacy as a fundamental right[2]. This case clarified that to safeguard the digital trials, which are broad and associated with the world, rather than just focusing on personal privacy.

Historical Overview-

The majority of worldwide democratic views is the foundation of privacy policies. While Warren and Brandeis defined privacy as the right to be let alone in their 1890 Harvard Law Review article, thinkers such as John Stuart Mill highlighted the value of individual autonomy[3]. That idea was to defend against all the sources, like the public, government, and media, for the dignity of personal life.

---

[1] *Olmstead V. United States, 277 U.S. 438 (1928); "The right to be let alone, the most comprehensive of rights and the right most valued by civilized men",* 2024.
[2] *K.S. Puttaswamy (Retd.) V. Union of India,* MANU/SC/1044/2017,AIR-2017, J.S. Khehar, C.J.I., Jasti Chelameswar et. al.
[3] Warren & Brandeis,The Right to Privacy, Vol.-4,p-5, 1890.

CANONSPHERE LAW REVIEW

Despite having similar philosophical foundations, data protection evolved with a different focus. In reaction to computerised data storage, Germany and Sweden passed the first data protection regulations in the 1970s, which is where it all began. Data protection is not just about 'being left alone', but also about giving people control over how their personal data is used[4]. Informational self-determination is emphasised in data protection jurisprudence. The German Federal Constitutional Court first stated this idea in the 1983 Census Act Case, acknowledging that personal data control is necessary for the unrestricted development of an individual's personality. Thus, privacy protection laws protected individuals against unfriendly encroachment, and the data protection laws were responsible for the interaction between people, government, and corporations for better outcomes.

The field of privacy law has historically dealt with topics including illegal searches, wiretapping, and spying. It addressed infractions after they happened and was mostly reactive and reparative. These data protection laws could take necessary action against the corporation in order to maintain security, transparency, consent and accountability.

An example of a standard international law is the General Data Protection Regulation (GDPR) of the EU, which establishes international standards for individual rights like express consent, data transfer, and the right to be forgotten[5]. India's Digital Personal Data Protection Act, 2023,[6] and California's California Consumer Privacy Act (CCPA) both set remarkable developments.

Privacy Rights Jurisprudence is based on human rights and constitutional law, which is confirmed by a number of judgments that the right is implicitly included in the right to life & liberty.

While data protection jurisprudence is managerial and prescriptive, dictating how information must be handled in a digital society, privacy jurisprudence is defensive and protective. There has been a substantial philosophical and legal shift from the traditional right to privacy to the contemporary idea of data protection. The DPDP Act,2023 was shaped by Justice B.N. Krishna Committee (2017-2018), which established the groundwork for data privacy in India by suggesting measures such as users' rights, accountability, consent and a regulating body.[7]

CANONSPHERE LAW REVIEW

[4] The Bundesdatenschutzgesetz (BDSG), 1978.
[5] *General Data Protection Regulation (GDPR)*, 2018.
[6] *Digital Personal Data Protection Act,2023.*
[7] *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*,2019.

Technical Transformation & Rise of Data Privacy-

Addressing cybercrime and legitimising digital transactions & data protection, the IT Act,2000, laid the base of electronic records, digital signatures & e-commerce. Sections like 43A hold the companies accountable for the failure to protect the sensitive data of users and compensate them, also in sec. 72 and 72A give penalties for breach of confidentiality and punishment for breach of a legitimate contract. The increasing productivity through growing artificial intelligence (AI) and big data has cost the users' data and faced algorithmic bias and targeted advertisements.[8]

There are two major pronouncements of courts in are Puttaswamy case,2017, where the Supreme Court established the foundation of India's Digital Personal Data Protection Act, 2023, by including it in Article-21[9]. Another was an American case of Carpenter vs U.S., 2018, where the court highlighted the necessity of digital privacy.[10]

Legal frameworks & other regulations-

a) Indian Context-

The first legal recognition of informational privacy was provided by the Information Technology Act of 2000, specifically Section 43A deals with compensation for failure to secure data, and 72A speaks about penalties for unlawful disclosure. After that, India's first data protection law, the Digital Personal Data Protection Act of 2023, establishes rights associated with consent-based processing, the authority to modify and remove personal data, and the obligations vested in data fiduciaries.

Relevant to this, some sector-specific rules like the RBI directive (2018), which mandated payment data location[11].

b) International context-

The General Data Protection Regulation (GDPR, 2018) from the European Union is an extraterritorial framework with a strict penalty system, which shows the significance of data protection in every possible way. In the United States, they don't

[8] *Information Technology Act,2000*, section- 43A, 72 & 72A.
[9] India Const. ,art.21, amended by One hundred and fifty amendment Act,2021.
[10] *CARPENTER V. UNITED STATES*, 2018, Vol-585, U.S.Report,p.296,Chief Justice John G.and Roberts, Jr. et al.
[11] *RBI*,2018, Notification for Storage of Payment System Data,(issued on 2019).

CANONSPHERE LAW REVIEW

have any specific law but have some sectoral laws, like in the health sector HIPAA[12] and COPPA for children's data privacy[13]. The California Consumer Privacy Act (CCPA), 2018[14] is a state-level legislation towards comprehensive consumer privacy rights. Here, India adopts a centralised approach, while the U.S. sets a state-based approach along with the specific segregated sectors.

The Paradigm Shift: From Privacy to Data Privacy-

The practice of privacy was often recognised as the right to be alone from the times. But with the advancement of the digital age, the idea of privacy has gradually changed [15]. This shift majorly depends on the following three principles such as Consent, Transparency and Accountability. Because every individual must have meaningful control over how their data is collected and used, the regulators must also require informed consent before processing such personal data.

In the case of transparency, the corporations and governments must disclose how they gathered, stored, and shared the data. Without it, an individual cannot exercise her/his autonomy over their virtual identities.

In this kind of privacy, the data fiduciaries, state agencies or private entities must be held responsible for any mishappening as misuse, breaches, or unauthorised disclosures of data. In India follows the Digital Personal Data Protection Act, 2023, follows or imposing duties on data fiduciaries and creates a regulatory oversight body[16].

In brief, the changes indicate a shift from personal isolation to the governance of mass digital information. It directly points out that the privacy of data is in need of collective responsibility from every individual and other entities through these principles.

CANONSPHERE LAW REVIEW

[12] Health Insurance Portability and Accountability Act of 1996.
Health Information Privacy, U.S. Department of Health & Human Service,2024.
[13] *Children's Online Privacy Protection Rule (COPPA), 1998*, (Retrieved on Sep.24,2025, 11.00 AM),https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

[14] California Consumer privacy Act,2018.
[15] Khushi Chopra & Surya Pratap Kasaudhan, *From Constitutional Rights to Data Protection: Art.21 and Comparative perspectives on privacy, M.A.*2024.(Retrieved on Sep.24,2025,3.30 PM),https://articles.manupatra.com/article-details/From-Constitutional-Rights-to-Data-Protection-Article-21-and-Comparative-Perspectives-on-Privacy

[16] Comes & Ferrer, Big Data Privacy : Challenges to Privacy Principles and Models,2015.

Challenges & Emerging Concerns-

This transition from privacy to data privacy has achieved undoubted improvements in the field of digital creativity and innovation, but it has also created some complicated issues. Some serious concerns as:

Cybersecurity Threats and Data Breach, which occur on a large scale all over the world. Here, the sensitive data got exposed and is being misused. For example, in the Aadhar data breach case of 2018, people of India raised questions about the safety of biometric and demographic information of over a billion citizens[17]. Another example is the U.S. Equifax breach case, U.S.,2017, [18] compromised the 147 million people's financial data.

State Power and Surveillance is the government's desire for security, for which it frequently uses technology for surveillance. In 2021, the Pegasus spyware incident revealed that even encrypted communication can be intercepted, which was a global debate between states' authority and people's right to privacy[19].

The companies' exploitation of Data is a major challenge where they monetise the user data through various ways. Cases like the Facebook scandal give scenarios of how personal data harvesting could be misused and affect common people's lives directly for political manipulation.

The Cross-Border Data Flows across the jurisdictions with different standards of protection, creating conflicts in execution.

Through all the above challenges and incidents that were threatening the human rights and the soul of democracy, the requirement must be more than a legal framework.

Possible Measures:

When the regulatory frameworks are made for digital privacy, they depend on various factors like the government, corporations, and every individual. And these factors were used as some measure to ensure the basic applicability of this framework and its effective implementation.

[17] Notice from Unique Identification Authority of India (UIDAI) , Data breach case,2018.

[18] Caitlin Kenny, The equifax Data Breach & the Resulting legal Resource. *Brooklyn Journal of Corporate, Finance & Commercial Law,*2018. (Retrieved on- Sep.22,2025,9:25 PM),https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1288&context=bjcfcl

[19] The Hindu, SC lists the Pegasus case for hearing on April 22, The H.B., 2025.

CANOPY SPHERE LAW REVIEW

For Individuals, improving digital literacy to help users comprehend permission. The use of VPNs, encryption apps and two-factor authentication-like technologies gives more protection to personal privacy. Simply reading the privacy policies and app permissions to exercise informed consent will make a change in an individual's perspective.

For Corporations, the incorporation of privacy protections into the design of every product or service is important. Identify the risks before processing significant amounts of sensitive data by performing Data Protection Impact Assessments (DPIAs). For getting the maximum benefit, establish an open grievance procedure and designate Data Protection Officers (DPOs) to ensure accountability as required by the GDPR and DPDP Act, 2023, in India[20].

For the Government, they have independent data protection authorities to monitor and supervise compliance and legal sanctions. The promotion of cross-border cooperation in data security in light of the increasing flow of data across borders, while seeking to balance national security needs with the fundamental rights of citizens to privacy.

Example- The international system GDPR imposes a 72-hour breach notification requirement. In this advanced age, these organisations turn it into more fulfilling and reliable.

Conclusion-

A significant shift from traditional privacy to data privacy illustrates a significant transition in concept and defence of rights. This shift recognises privacy as crucial for democracy, dignity, and global trust. Where the former idea of right to privacy has now broadened into the intricate field of informational autonomy, where private information is now the new currency of power. As a result of the development of digitalisation, the safeguarding of digital identities has become more important than physical space. Legal milestones like India's Puttuswamy case, DPDP Act of 2023 and the international concerns like the EU's GDPR of 2018 reflect the recent privacy norms. They were also evolving with the needs of citizens & trying to make it a collective responsibility.

[20] Cristina Tikkinen Piri ,et al., EU General Data Protection regulation: Changes & implication for personal data collecting Companies , 2017,(Retrieved on-Sep.25,2025, 7.30pm).https://oulurepo.oulu.fi/bitstream/handle/10024/22667/nbnfi-fe201802203509.pdf?sequence=1

CA IONSPHERE LAW REVIEW

References

- (2018, Jan 4). UIDAI. Retrieved Sep 26, 2025, from https://uidai.gov.in/images/news/Press_note08012018.pdf
- (2021, June). The Federal Ministry of Justice and Consumer Protection and the Federal Office of Justice. Retrieved Sep 20, 2025, from https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf
- California Privacy Protection Agency. (n.d.). *California Consumer Privacy Act,2018*. CCPA.gov. Retrieved Sep 24, 2025, from https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf
- *CARPENTER v. UNITED STATES*. (2018, Jun 22). LII. Retrieved Sep 21, 2025, from https://www.law.cornell.edu/supremecourt/text/16-402
- *Children's Online Privacy Protection Rule (COPPA), 1998*. (n.d.). Federal Trade Commission of the U.S. Retrieved Sep 24, 2025, from https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.
- Chopra, K., & Kasaudhan, S. P. (2024, Jul 2). *From Constitutional Rights to Data Protection: Art 21 and Comparative perspectives on privacy*. Manupatra Articles. Retrieved Sep 24, 2025, from https://articles.manupatra.com/article-details/From-Constitutional-Rights-to-Data-Protection-Article-21-and-Comparative-Perspectives-on-Privacy
- Comes, J. S., & Ferrer, J. D. (n.d.). Big Data Privacy: Challenges to Privacy Principles and Models. *Springer*, (Google Scholar). 10.1007/s41019-051-0001-x
- *Digital Personal Data Protection Act,2023*. (n.d.).
- *Digital Personal Data Protection Act,2023*. (2023, Aug 11). Meity.gov. Retrieved Sep 23, 2025, from

CAMONSPHERE LAW REVIEW

https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

- *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*. (n.d.). PRSIndia. Retrieved Sep 24, 2025, from https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf
- *General Data Protection Regulation*. (2018). Retrieved Sep 22, 2025, from https://gdpr-info.eu/
- *Health Information Privacy*. (2024). HHS.gov. Retrieved Sep 25, 2025, from https://www.hhs.gov/hipaa/index.html
- The Hindu Bureau. (2025, Mar 7). SC lists the Pegasus case for hearing on April 22. *The Hindu*.
- India. (2023). *Constitutional Law of India: The Constitution of India: as amended by The Constitution (One Hundred and Fifth Amendment) Act, 2021 (w.e.f. 15-9-2021, vide S.O. 4063 (E) dt. 15-9-2021) with list of Constitutional Amendments - a ready reckoner : alongwith:* . Law & Justice Publishing Company.
- *Information Technology Act,2000*. (2000, Oct 17). Ministry of Electronics and Information Technology. Retrieved Sep 22, 2025, from https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- *The Information Technology Act,2000*. (2000, Oct 17). Retrieved Sep 23, 2025, from https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf
- Kenny, C. (2018, Jan 10). The Equifax Data Breach & the Resulting Legal Resource. *Brooklyn Journal of Corporate, Finance & Commercial Law*, *13*(1). https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1288&context=bjcfcl

CAMONSPHERE LAW REVIEW

- *K.S. Puttaswamy (Retd.) v. Union of India, 2017*. (2017, Aug 24). Retrieved Sep 25, 2025, from https://www.manupatracademy.com/legalpost/manu-sc-1044-2017
- *Olmstead v. United States, 277 U.S. 438 (1928)*. (2024, October 1). The Library of Congress(gov). Retrieved Sep 25, 2025, from https://tile.loc.gov/storage-services/service/ll/usrep/usrep277/usrep277438/usrep277438.pdf
- Piri, C. T., Rohunen, A., & Markkula, J. (2017). EU General Data Protection Regulation: Changes & implications for personal Data Collecting companies. *Computer law and Security review- Journal 2017*. https://oulurepo.oulu.fi/bitstream/handle/10024/22667/nbnfi-fe201802203509.pdf?sequence=1
- *Reserve Bank of India*. (2019, June 26). Reserve Bank of India. Retrieved September 30, 2025, from https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995
- *Right to Information Act,2005, Sec 8(1)(j)*. (n.d.). CIC gov. https://cic.gov.in/sites/default/files/RTI-Act_English.pdf
- Warren, S. D. (1890, Dec 15). The Right to Privacy. *4*. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

CANONSPHERE LAW REVIEW