INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN:2582-6433

DISCLAIMER

 ISSN:2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN:2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN:2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN:2582-6433

PROTECTION OF PRIVACY IN THE IT AGE AND THE CHALLENGES BEFORE INDIAN LAW: AN ANALYSIS

AUTHORED BY: JUNAK GOSWAMI

ABSTRACT

Protecting privacy has become one of the most important concerns facing both the government and individuals in the present digital era. A growing amount of personal data is being gathered and kept in this modern age.

In India, the rise of digital platforms and the country's drive towards digitization has only intensified concerns about the protection of personal information and data privacy. The article will explore the dynamic landscape of privacy protection in the IT age and the legal challenges India faces in ensuring the safety of personal data.

Several provisions of the IT Act, 2000 are pivotal in this case and are especially relevant as cybercrimes become more sophisticated which I'll explore in my paper.

Even while these regulations seem promising, there are still a number of issues that need to be resolved, several of which I will discuss in more detail. These issues include the possible conflicts between privacy and security as well as the effectiveness of the laws' enforcement.

Furthermore, the IT Act is not the only piece of legislation in India that protects privacy.

The DPDP Act, 2023 is also a significant step in the Indian Data Protection landscape and privacy framework. This recently enacted regulation imposes strict obligations on data fiduciaries, such as securing the informed consent of individuals before processing their data and guaranteeing the legitimate and safe processing of personal data. Additionally, the Act grants certain rights to individuals, such as the capacity to access, amend, or remove personal data.

 ISSN:2582-6433

Additionally, the tension between national security and individual privacy is an ongoing debate in India's legal discourse. Laws that allow for Govt. surveillance and interception of data for security reasons have raised concerns about overreach and the potential for misuse, bringing the fine balance between personal privacy and state interests into sharp focus.

To what extent can the state advance national interests while respecting individualism and privacy? This is a regulation that bears separate, detailed consideration.

To sum up, despite the remarkable advancement in privacy laws in compliance with modern means of communication and data exchange; there are still gargantuan lacunae to bridge.

Key Words: Privacy, Surveillance, Digital Personal Data, Data Protection.

LIST OF ABBREVIATIONS

IT	Information Technology
NIG	National Intelligence Grid
CMS	Central Monitoring System
Anr	Another
SC	Supreme Court
PUCL	People's Union for Civil Liberties
UOI	Union of India
IAMAI	Internet and Mobile Association of India
RBI	Reserve Bank of India
Govt.	Government
i.e.	Id est/ That is
Pvt.	Private
M/S	Messrs
DPDP	Digital Personal Data Protection

 ISSN:2582-6433

JPC	Joint Parliamentary Committee
CFI	Consolidated Fund of India
GDPR	General Data Protection Regulation
EU	European Union
Art.	Article
Ibid	Ibidem/In the same place

I. INTRODUCTION

In this 21st century, the gradual evolution of technology has brought significant concern about the protection of our privacy. The concern has been extended to how our data is collected, stored, and utilized. Personal information has become a valuable commodity in our daily lives and to the data fiduciaries as well. This information ranges from user preferences and online activity to extremely private biometric data that can result in financial fraud, identity theft, or illegal spying if improperly handled.

In this IT age, there is a high risk of data leaks and privacy violations. Concerns regarding data breaches, unauthorized sharing, and exploitation are especially heightened by the everyday generation of enormous data sets.

As per Statista report, globally more than 22 billion data records were exposed in 2022 alone because of data breaches.[1] Hence, the necessity of strong mechanisms to protect personal data in the digital flooring.

India has emerged as one of the world's largest digital economies, with over 1.2 billion mobile phone internet users as of 2023.[2]

Nonetheless, the growing number of internet users on mobile devices may encounter privacy concerns in the digital realm due to their data or information. The massive growth of mobile

[1] Statista, 'Global Number of Data Breaches 2005-2023' (Statista) https://www.statista.com/statistics/1459417/data-breaches-worldwide/ [accessed 28 November 2024].
[2] Statista, 'Number of Mobile Internet Users in India 2015-2023' (Statista) https://www.statista.com/statistics/558610/number-of-mobile-internet-user-in-india/ [accessed 28 November 2024].

 ISSN:2582-6433

applications, e-commerce, and online banking have all put citizens' data at continuous risk. Despite recognition through global instruments[3] and Indian legislation, the absence of a comprehensive legal framework leaves privacy vulnerable to exploitation. So a comprehensive robust legal framework is needed to fight against this issue.

II. THE TERM 'PRIVACY' AND THE SCOPE

The term 'Privacy' is used in the context of personal information. Privacy is not connected with that information which is public in nature.

Privacy is an individual's ability to control his/her personal information. For example: Who can/cannot know that thing, Who can/cannot see, Who is involved in sharing, Who can/cannot process, all these things are in an individual's control and he/she will control it.
Personal information[4] can be age, blood group, bank account, data, etc.

In addition to that Privacy is the dimension of liberty and it has a direct connection with the Right to Life and Personal Liberty[5] as well as Freedom of Speech and Expression[6]. So that the privacy will be protected under the constitution of India. If the privacy is not protected it will make a detrimental impact on his/her personal liberty. Now in terms of cyberspace, Privacy is under threat and it is difficult to violate or identify the privacy violation of an individual. Because, when we are online or when we are using all social media platforms, we are sharing our data and so that the data are vulnerable.

A) UNDERSTANDING THE CONCEPT OF PRIVACY IN THE DIGITAL ERA

The issues regarding privacy exist in physical space, but they have become more problematic in digital space.

The privacy and data of ours under threat in the digital era. For example, even Govts. are involved in the surveillance of personal data, and from the standpoint of data privacy, it has

[3] United Nations, 'UN Entities Issue Joint Statement on Data Protection and Privacy' (UN) https://www.un.org/en/delegate/un-entities-issue-joint-statement-data-protection-and-privacy [accessed 28 November 2024].
[4] Information Technology Act 2000, s 2(1)(v).
[5] Constitution of India, art 21.
[6] ibid art 19(1)(a).

 ISSN:2582-6433

grown to be a significant worry.[7]

The Indian Govt. now has the most up-to-date and modern tools to monitor its inhabitants at multiple levels through a variety of agencies following decades of the IT revolution. Different agencies and departments have been established and empowered by the Govt. for surveillance and gathering of data of its citizens including the NIG, CMS, etc. Reading about the many Govt. departments and agencies that carry out surveillance tasks or are somehow involved in the broader process is essential if we want to comprehend the systems and methods of surveillance in India.[8]

Despite the landmark Puttaswamy case law's judgment[9] establishing privacy as a fundamental right, it doesn't have any appropriate data protection regulation.

In its ruling in Ritesh Sinha v. State of Uttar Pradesh and Anr. in 2019, the SC ruled that, despite being a fundamental right, the right to privacy is not an absolute one.[10] The same limitations apply to it as to other fundamental rights. The Puttaswamy ruling was thus supported by this ruling. In a clear and unequivocal ruling, the three-judge panel—which included Justice Deepak Gupta, Justice Sanjay Khanna, and former Chief Justice Ranjan Gogoi—held that "the right to privacy is not absolute and must bow down to compelling public interest."[11]
In the Shreya Singhal case[12], the SC of India struck down Section 66A of the IT Act, 2000, for being unconstitutional and violative of free speech and expression. It also addressed concerns regarding privacy and data interception by authorities. Through this, it highlights the dangers of vague laws enabling state surveillance in the digital age.[13]

In the PUCL vs. UOI, the SC of India held that telephone tapping by the Govt., without proper safeguards, violates the individual's fundamental right to privacy.[14]

---

[7] Businessline, 'Government Surveillance at Alarming Levels' (Businessline, 2019) https://www.thehindubusinessline.com/info-tech/government-surveillance-at-alarming-levels/article28138407.ece [accessed 25 November 2024].
[8] Legal Services India, 'Surveillance in India and its Legalities' (Legal Services India, 2020) http://www.legalservicesindia.com/article/2162/Surveillance-in-India-and-its-Legalities.html [accessed 25 November 2024].
[9] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.
[10] *Ritesh Sinha v State of Uttar Pradesh and Anr* (2019) 8 SCC 1.
[11] ibid
[12] *Shreya Singhal v Union of India* (2015) 5 SCC 1.
[13] ibid
[14] *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.

 ISSN:2582-6433

Last but not least, in the IAMAI vs. RBI case, the apex court struck down the RBI's circular banning of cryptocurrency transactions, noting concerns about data protection and individual privacy in digital financial systems, and bringing attention to privacy challenges in financial technology.[15]

Hence, it is notable that the problem is that privacy has become more vulnerable in the case of the digital era. So, one might be thinking of the information or data of his/her in private and control over it but the reality is different. If any data fiduciary particularly Govt. wants to take or get any information about someone they can easily get it. For example, although WhatsApp claims that the messages are encrypted, WhatsApp itself can read the messages and can pass the messages to the Govt. if they want.

III. THE ROLE OF THE IT ACT, 2000 IN PROTECTING THE DATA IN THE DIGITAL AGE

There are number of provisions which talk about Privacy.

If we look at section 66(E) of this Act[16] the term Privacy has been used. But, this section is not about data protection.

The essence of this section is if someone is capturing the image of the private area of any person without her/his consent i.e. will be considered as an offense.[17]

In Kalandi Charan Lenka vs. State of Odisha, the accused allegedly: Created a fake Facebook account in the victim's name and uploaded morphed obscene photographs of the victim, portraying her in a sexually explicit manner. Then disseminated these images online with the intent to harm her dignity and reputation. So, here the accused was charged under Section 66E along with the other relevant provisions.[18]

Although the accused has been charged under section 66E of this Act, there were no such

[15] *Internet and Mobile Association of India v Reserve Bank of India* (2020) 10 SCC 274.
[16] Information Technology Act 2000, s 66(E).
[17] ibid
[18] *Kalandi Charan Lenka v State of Odisha* (2017) SCC Online Ori 650.

 ISSN:2582-6433

judgments pronounced related to data protection regulations.

When an individual shares information with another person with trust and expects not to disclose the information i.e. is called confidentiality. Confidentiality is the extension of Privacy.

When confidentiality and privacy breaches there will be a penalty under this Act.[19]

But, in this section of this Act, the penalty has been imposed only on the authorities under the Act if they got punished over certain information or data because they are supposed to perform certain functions. So in pursuance of their official duty, if they get certain information, they will have the responsibility not to disclose that information to someone else.[20] Thus, the scope of the section 72 is very limited.

Now in section 72A of this Act[21] is also relevant because it talks about confidentiality and privacy as well. So here the responsibility has been imposed not to disclose information in breach of the lawful contract. For example, if an individual's laptop or mobile phone gets damaged so that he/she goes to the repairing centre to repair it. Now here the shopkeeper impliedly comes under the contract to fix the device only and not to store or disclose any information or data inside the device. But, if the particular shopkeeper breaches this contract he/she will be liable under this section.[22]

In the case Google India Pvt. Ltd. vs. M/S Visakha Industries, the issue was about the alleged defamatory content posted on a Google Groups platform hosted by Google LLC. The plaintiff claimed that such content caused harm to the company's reputation. While Section 72A is not explicitly discussed in the judgment, its principles align with the overarching themes of intermediary accountability and user protection. It serves as a complementary provision ensuring that entities managing platforms or user data adhere to strict confidentiality and ethical standards, thus preventing reputational harm or misuse of sensitive information.[23]
However, the scope of the section 72A is also limited in nature. It does not lay down any

[19] Information Technology Act 2000, s 72.
[20] ibid
[21] Information Technology Act 2000, s 72(A).
[22] ibid
[23] *Google India Pvt Ltd v Visakha Industries* (2020) 11 SCC 96.

 ISSN:2582-6433

regulations or talk about data protection in general.

Apart from this, section 43(a) of this Act[24] has been inserted to deal with data protection. However, this section was not sufficient and comprehensive enough because of some shortcomings such as under this section the responsibility has been imposed on the part of body corporate only means any company which is engaged in commercial or professional activities and if they are unable to protect the data in that case they will be liable to pay compensation. This section is a very narrow one and hasn't covered the companies which are not involved in any commercial or professional activities.

Apart from that, in the contemporary world personal data is under threat mainly because of the Govt. agents, and Govt. is significantly responsible. But, we can see under section 43(a) it does not apply to Govt. agencies.

Moreover, in this section, the body corporate will be responsible for sensitive personal data which has been categorized.[25] But, haven't covered all the personal data.
That is why section 43(a) has been omitted by the DPDP Act, 2023.[26]

IV. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

In the Puttaswamy case law when the question arises of the constitutionality of the Aadhar Act[27] in 2017 then immediately after that, the Govt. of India constituted a committee named 'The Committee of Experts on Data Protection Framework for India' which is popularly known as The B.M. Krishna Committee. Because the SC of India needs recommendations that India should enact a strong law on data protection. The mandate of this committee was to examine the data protection regime in India and draft legislation regarding data protection. The B.M. Krishna Committee gave its report in the year of 2018 which was titled as 'Protecting Privacy Empowering Indians A Free and Fare Digital Economy'.[28] Along with the report The B.M. Krishna Committee also provided a draft bill known as the Personal Data Protection Bill in the

[24] Information Technology Act 2000, s 43(a).
[25] ibid
[26] Digital Personal Data Protection Act 2023, s 44(2)(a).
[27] Puttaswamy (n 1).
[28] B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 2018) https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf [accessed 25 November 2024].

 ISSN:2582-6433

year of 2018. On the basis of that draft bill of the year 2018, the Govt. of India came up with a bill known as the Personal Data Protection Bill 2019. When the Bill was introduced, it was criticized for several terms. Because of that reason, the Bill was sent to the JPC. Then the JPC suggested more than 90 amendments to the Bill of 2019.

Keeping all these things in mind, the Govt. of India basically once again brought a bill in the year of 2022. But, in the month of December of the same year, the Bill of 2022 was withdrawn by the Govt. After that in the year of 2023 the Govt. came up with a Bill which is known as the Digital Personal Data Protection Bill of 2023 and that Bill became the Act in the same year.

If we observe the short title of the DPDP Act, this Act wants to ensure the protection of Digital Personal Data. And from the long title of this Act, it lays down the rules regarding the processing of digital personal data and by doing so it wants to recognize the rights of an individual to protect their digital personal data.

Here, Personal Data has been defined in this Act where it interprets any individual's Signature, Name, Age, Biometric, Bank account, Aadhar number, PAN card, etc. which are identifiable.[29]

So eventually, this DPDP Act is not about the public data rather it is about the personal data by which an individual can be identified.

On the other hand, Digital Personal Data means personal data in digital form.[30]

Thus, this Act is not about either the private data or any other data such as public data which is available in digital form.

Eventually, this Act is all about how DPDP can be processed. Processing means collection, recording, organisation, combination, structuring, storage, adaptation, retrieval, use.[31]
Under this Act, if the digital personal data has been processed in India, in that case, this Act will be applicable.[32] And, if the digital personal data has been processed outside of India, in that case also this Act will be applicable but only on the condition that the processing must

[29] Digital Personal Data Protection Act 2023, s 2(t).
[30] ibid s 2(n).
[31] ibid s 2(x).
[32] ibid s 3(a).

 ISSN:2582-6433

have been done in connection with the any activity related to the offering of the goods or services to data principals within the territory of India.[33]

The most important thing about this Act is the consent of the data principal. Without the consent, the data cannot be processed. The consent shall be free, informed, unconditional, and unambiguous with a clear affirmative action, and also the consent shall be obtained by an agreement.[34]

Apart from the consent, the data can be processed under a lawful purpose for certain legitimate use.[35] So here we can see that consent is not so much important. The interpretation of legitimate use i.e. things has been provided under section 7 of this Act.[36] That is why the sections 5 and 6 of this Act are not relevant.

The data principal has the right to withdraw her/his consent.[37] Moreover, he/she has the right to access, correct, and erase the personal data.

Under this Act, every Data Fiduciary should have a grievance officer and similarly, every consent manager also have a grievance officer. If the Data Principal has a grievance against the Data Fiduciary or against the consent manager in both cases data principal has the right to file a complain to that grievance officer of the data fiduciary as well as the consent manager.[38]

A) CHALLENGES AND LIMITATIONS OF THE DPDP ACT

In this legislation the central Govt. has enormous power to exempt any data fiduciary including startups from the purview of this particular Act.[39]

So the problem here is the central Govt. can exempt any data fiduciary as the central Govt. has excessive power in this. Because of that reason, all the sections will not be applicable including sections 5, 8, 3, 7, 10, and 11 with regard to those data fiduciaries which the central govt has exempted.

[33] ibid s 3(b).
[34] ibid s 6(1).
[35] ibid s 4.
[36] ibid s 7.
[37] ibid s 6(7).
[38] ibid s 13.
[39] ibid s 17(3).

 ISSN:2582-6433

The another problem with this DPDP Act is that it does not discuss about Data Localization. Because, if we look at the history behind this Act, there was a demand in India to enact a data protection law, which should ensure data localization means any data fiduciary under this Act is not bound to store data in its server located in India and they can store the data even outside India as well.

Additionally, the penalties which have been imposed under the DPDP Act will be deposited to the CFI.[40] But, what the victim or the data principal will get? Neither the victim nor the data principal will get anything or any monetary compensation.

Last but not least, this Act doesn't talk about the Right to be forgotten. For example, if an individual by mistake gives any information to any data fiduciary which he/she forgot of that thing then the privacy of that data principal may be violated. There is another relevant example is if Mr. X involved in theft but at the end of the day Mr. X did not do anything. But, on the internet news items remained there. So Mr. X will have the right that the detrimental item should be deleted from the internet news.

Even in the B.M. Srikrishna Committee report, it has been emphasized that India is going to enact a law that the law should incorporate the concept of the right to be forgotten but that is missing in the DPDP Act of 2023.

V. SUGGESTIONS AND MOVING FORWARD

India's approach to cross-border data transfers is more lenient, which might pose challenges for securing personal data internationally.

But if we see the GDPR's cross-border data transfer policy which ensures that European citizens' data is protected, even when processed outside the EU.[41] Moreover, GDPR has clear rules for data breaches, and mandatory reporting within 72 hours sets a high standard for responsiveness.[42]

[40] ibid s 34.
[41] European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* [2016] OJ L119/1, arts 3, 44–46.
[42] ibid arts 33–34.

 ISSN:2582-6433

India should follow the policy of the EU's GDPR. Additionally, data localization should be implemented immediately. It is understandable that the digital personal data will be taken by the govt. or any other data fiduciary based on the lawful or legitimate principle but it also should be ensured that the data shouldn't be misused.

Digital data protection is vital as the digital footprint of every citizen is increasing day by day. When the violation of privacy occurs, the victim should get appropriate compensation. That is why it is high time to set an amendment in section 34 of the DPDP Act, 2023.

However, to have an independent and fair approach in a democracy (like India), the powers to exempt data fiduciaries should be given to an independent regulator rather than the central government. Such a body should work in a transparent manner and reliance on exemptions should be based on predetermined, objective criteria reflecting public interest and data protection principles. Judicial or parliamentary scrutiny of all exemption decisions is necessary to guarantee accountability and guard against abuse. This will guarantee a balance between justice and regulation.

If nothing else, we should make sure that this right to be forgotten is incorporated into the law so that it is feasible to ask for the removal of a person's personal information when it is no longer accurate, relevant, or required. By protecting privacy, this right helps prevent the harm that inaccurate or dangerous information could do. This clause will ensure that data principals have stringent privacy rights and bring the Act into accordance with international data protection standards and the recommendations of the B.M. Srikrishna Committee.