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

EDITORIAL TEAM

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

PRIVACY IN THE DIGITAL ERA: LEGAL RESPONSES TO TECHNOLOGICAL DISRUPTIONS

AUTHORED BY - NAMRATA N WAGHMARE
& PRAJAKTA PIMPALSHINDE

Abstract:

The advent of the internet has revolutionized access to information, empowering individuals to explore new ideas, practices, and perspectives with unprecedented ease However, these technological advancements have also introduced significant privacy challenges. The pervasive mining of private information for unethical and illegal purposes has raised serious concerns regarding security breaches, identity theft, and unauthorized governmental surveillance.Moreover, the ethical implications of data practices employed by social media platforms have come under scrutiny, highlighting the tension between innovation and privacy protection. As human beings inherently value their privacy and seek to maintain control over personal information, the increasing vulnerability of private data posed by modern information technologyhas underscored the need for robust legal frameworks. This article explores the evolving legal landscape of privacy in India, examining the intersection of privacy rights with the rapid development of science and technology. It underscores the importance of balancing innovation with the protection of personal privacy, and the ongoing efforts to establish a robust legal framework that adequately addresses the challenges posed by the digital age.

Key words: Information, technology, security breach, identity theft, privacy rights.

Introduction:

Technology has had a profound impact on many aspects of our lives, mainly privacy. The growthof the internet and the widespread use of digital devices have made it simpler for individuals and organizations to share and access information[1]. However, this increased

[1] The Impacts of Technology on Privacy and Cybersecurity, Medium, available at https://fastfacts101.medium.com/the-impact-of-technology-on-privacy-and-cybersecurity-4d2037331311, last seen on 24/08/2024

 ISSN: 2582-6433

connectivity has also ledto new privacy and security concerns. In this article we'll see how technology has affected privacyrights, why it is important to protect the privacy and what are existing legal framework to combatthe issue and what other legal remedies could be introduced. One of the most significant effects oftechnology on privacy is the extensive collection, storage, and sharing of personal information online. As people increasingly use social media, online shopping, and other digital platforms, theywillingly share personal information like their name, address, phone number, and credit card details. Companies use this data for targeted advertising, data mining, and various other purposes.However, this same information can be exploited by hackers and malicious actors, leading to identity theft, fraud, or other crimes. The advancements in data analytics and machine learning have further increased these concerns. Organizations and individuals must take steps to secure their personal and sensitive information and be aware of the laws and regulations that govern privacy and cybersecurity.

At the core of this study the key question is how well do the current legal frameworks in India tackle the complex challenges presented by the fast-evolving field of digital privacy and data protection? This research seeks to comprehensively examine the existing legal frameworks, scrutinize their efficacy, and propose recommendations for potential enhancements[2]. Moreover, itaims to stimulate thoughtful discussions on shaping a more resilient framework for digital privacyand data protection in the country, considering the implications of The Digital Personal Data Protection Act, 2023. Policymakers can benefit from informed recommendations to enhance legislative frameworks, businesses can adapt strategies to ensure compliance with evolving regulations, and individuals can better understand and advocate for their digital rights. In navigating this research, the goal is not only to analyze the existing state of affairs but also to contribute proactively to the ongoing dialogue surrounding the challenges posed by the digital age.

Evolution of Privacy Concerns in the Digital Age

Emerging technologies, such as Artificial Intelligence (AI), have a profound impact on digital privacy. AI's advanced data processing and analysis capabilities can enhance service delivery andgenerate valuable insights. However, these same capabilities can also be used to scrutinize personaldata for profiling and decision-making without sufficient human oversight, potentially violating individual privacy without consent. Thus, AI represents both a significant opportunity

[2] Digital Privacy and Data Protection Laws in India, The Amikus Quriae, available at https://theamikusqriae.com/digital-privacy-and-data-protection-laws-in-india/, last seen on 21/08/2024

 ISSN: 2582-6433

and a potential threat to digital privacy, necessitating the development of strong privacy policies to regulate its use.

Similarly, data analytics—while powerful in providing insights into user behaviours and improving service personalization—can pose risks to privacy if not managed properly. Extensive data collection and analysis may infringe on individual privacy rights unless accompanied by practices such as data minimization and anonymization. Balancing the benefits of data analytics with privacy considerations is crucial[3].

As technology continues to evolve, individuals must remain informed about these changes and their privacy implications. This includes understanding the privacy policies of digital services, utilizing privacy tools and settings, and keeping systems updated to address any technical vulnerabilities.

The integration of Internet of Things (IoT) devices into everyday life introduces significant privacyconcerns. These devices collect, process, and transmit large amounts of potentially sensitive data, which can lead to privacy breaches if not properly secured. Users should be vigilant about the security settings and data management practices of their IoT devices.

Finally, advancements like facial recognition technology pose serious challenges to digital privacynorms. While offering potential benefits for security and access control, they raise concerns about the loss of anonymity in public spaces and the potential for misuse in surveillance. This highlightsthe urgent need for legal and ethical guidelines to regulate the use of such powerful technologies in a privacy-conscious era. Encryption plays a pivotal role in strengthening digital privacy. It involves encoding information such that only authorized parties can access it. By leveraging encryption technologies, users can ensure that even if their data is intercepted, it remains unreadable and thus, safe. Encryption is extensively used in protecting sensitive data transmissionand storage, including in email services, messaging apps, and cloud storage, thereby enhancing individual digital privacy.

[3] What is Digital Privacy and its Importance, IEEE Digital Privacy, available at https://digitalprivacy.ieee.org/publications/topics/what-is-digital-privacy-and-its-importance, last seen on 24/8/2024

 ISSN: 2582-6433

Technological Innovations and Their Impact on Privacy

(i) Internet

A major theme in the discussion of Internet privacy revolves around the use of cookies[4]. Cookiesare small pieces of data that web sites store on the user's computer, in order to enable personalization of the site. However, some cookies can be used to track the user across multiple web sites (tracking cookies), enabling for example advertisements for a product the user has recently viewed on a totally different site. Again, it is not always clear what the generated information is used for. Laws requiring user consent for the use of cookies are not always successful in terms of increasing the level of control, as the consent requests interfere with task flows, and the user may simply click away any requests for consent. Similarly, features of social network sites embedded in other sites (e.g. "like"-button) may allow the social network site to identify the sites visited by the user.

(ii) Cloud Computing

The rise of cloud computing has intensified privacy concerns. Previously, user data and programswere stored locally, limiting access to data and usage statistics by program vendors. With cloud computing, both data and programs are hosted online, creating uncertainty about how user- generated and system-generated data are utilized. Additionally, the global nature of cloud storagecomplicates the identification of applicable laws and the authorities that can access the data. Thisissue is especially pronounced with data collected by online services and apps, such as search engines and games, where it is often unclear which data is collected and how it is communicated.

Users frequently face limited choices, sometimes having no option but to use the application without full transparency on data handling**.**

(iii) Social Media

Social media platforms present unique privacy challenges. The issue extends beyond merely restricting access to information; it involves addressing the moral implications of encouraging users to share extensive personal data. Social networks often prompt users to provide more data toenhance their profiles and increase site value, creating a temptation to exchange personal information for service benefits. Users may be unaware of the full extent of data they are

[4] Palmer, D.E., 2005, "Pop-ups, cookies, and spam: toward a deeper analysis of the ethical significance of internet marketing practices", Journal of business ethics, 58(1–3): 271–280(2005).

 ISSN: 2582-6433

sharing,as seen with features like the "like" button. Simply limiting access to this information doesn't address the root problem; instead, efforts should focus on guiding user behaviour regarding data sharing.

One approach to reducing the temptation to share is implementing strict default privacy settings. While this can limit access for other users, it doesn't necessarily restrict the service provider's access. Such measures may also impact the functionality and benefits of social networking sites. An alternative is adopting an opt-in approach, where users must actively choose to share data or subscribe to services, potentially leading to more acceptable outcomes. However, the effectiveness of this approach depends significantly on how the options are presented to users[5].

(iv) Big Data

Users generate loads of data when online. This is not only data explicitly entered by the user, but also numerous statistics on user behaviour: sites visited, links clicked, search terms entered, etc. Data mining can be employed to extract patterns from such data, which can then be used to makedecisions about the user. These may only affect the online experience (advertisements shown), but,depending on which parties have access to the information, they may also impact the user in completely different contexts. In particular, big data may be used in profiling the user (Hildebrandt2008), creating patterns of typical combinations of user properties, which can then be used to predict interests and behaviour. An innocent application is "you may also like …", but, dependingon the available data, more sensitive derivations may be made, such as most probable religion or sexual preference. These derivations could then in turn lead to inequal treatment or discrimination.When a user can be assigned to a particular group, even only probabilistically, this may influencethe actions taken by others. For example, profiling could lead to refusal of insurance or a credit card, in which case profit is the main reason for discrimination. When such decisions are based onprofiling, it may be difficult to challenge them or even find out the explanations behind them. Profiling could also be used by organizations or possible future governments that have discrimination of particular groups on their political agenda, in order to [6]find their targets and denythem access to services, or worse.

[5] Steven Bellman, Eric J. Johnson, Gerald L. Lohse, Communications of the ACM, Volume 44, Number 2, The ACM Digital Library, Pages 25-27(2001)
[6] Privacy and Information Technology, Standford Encyclopedia of Philosophy, available at https://plato.stanford.edu/entries/it-privacy/#DevInfTec, last seen on 23/08/2024

 ISSN: 2582-6433

(v) Mobile Phones

As networked devices like smartphones become more common, they increasingly collect and transmit data through various sensors, such as GPS, movement sensors, and cameras. GPS sensorscan track precise locations, while even without GPS, approximate locations can be determined viawireless networks. This location data, linking the online and physical worlds, can pose privacy risks like stalking or burglary. Cameras on these devices can also capture private images, raising concerns about user awareness and control. While some devices indicate camera activation with alight, this can be manipulated by malicious software. Overall, the privacy implications of reconfigurable technology[7] hinge on users' awareness of how their data is managed and used.

(vi) The Internet of Things

Devices connected to the Internet extend beyond user-owned gadgets like smartphones to includea wide range of Internet of Things (IoT) devices. These include RFID chips in passports and publictransport systems, which can leak data such as nationality, and "dumb" RFIDs in products that could trace individuals. In homes, smart meters and connected appliances generate data on electricity use, water consumption, and environmental preferences, potentially enabling profilingand monitoring. As more household devices become interconnected, privacy concerns grow, particularly regarding data collection, user autonomy, and transparency. Users must be aware of features like microphones in connected devices and how their data is handled.

(vii) E-Government

Government and public administration have undergone radical transformations as a result of the availability of advanced IT systems as well. Examples of these changes are biometric passports, online e-government services, voting systems, a variety of online citizen participation tools and platforms or online access to recordings of sessions of parliament and government committee meetings. In elections, information technology impacts voter privacy throughout the voting process[8]. Secret ballot requirements aim to prevent vote buying and coercion, demanding that voters keep their choices private. While polling stations can enforce this privacy, mail-in and online voting are more vulnerable to breaches of confidentiality since privacy cannot be guaranteedtechnologically, and voters might be observed during the process.

[7] Dechesne, F., M. Warnier, & J. van den Hoven, Ethics and Information Technology, available at https://link.springer.com/article/10.1007/s10676-013-9326-1, last seen on 26/08/2024
[8] St´ephanie Delaune, Steve Kremer, Mark Ryan, Coercion-Resistance and Receipt-Freeness in Electronic Voting, 5,6(2008)

 ISSN: 2582-6433

Information technology influences how voters maintain this privacy and how authorities can verify it.

E-democracy initiatives could reshape privacy in politics. Additionally, online platforms and socialmedia can compromise privacy by enabling targeted misinformation and behavioural profiling, making it harder to protect preferences and increasing the risk of opinion manipulation.

(viii) Surveillance

Information technology enhances surveillance capabilities by improving traditional systems like CCTV with features such as facial recognition and integrating data from Internet-of-Things devices. This technology also powers "surveillance capitalism," where social media and online platforms collect extensive personal data, sometimes without clear consent, for purposes ranging from targeted advertising to potentially malicious activities like election interference.

In early April 2021, during the Kumbh Mela festival in Haridwar, India, AI-enabled cameras anddrones monitored pilgrims for mask-wearing and physical distancing as COVID-19 cases surged.While these technologies aimed to enhance safety, they also raised concerns about privacy and individual freedoms. In recent years, Indian police have increasingly used fingerprint and facial recognition technology (FRT) for surveillance in various public spaces, including during protestsagainst controversial laws. These technologies, often prone to high error rates and biases, have ledto privacy violations and wrongful arrests.

Digital surveillance in India extends beyond policing to broader datafication, where personal datais extensively collected and analysed by both the state and private entities. The proposed Social Registry Information System, intended to integrate with India’s Aadhaar biometric system, aims to track individuals' lives comprehensively, raising significant privacy concerns. This shift towardspervasive surveillance compromises privacy, a fundamental right linked to freedom of expressionand protection against discrimination.

In the context of India's expanding digital surveillance without a comprehensive data-protection law, the Supreme Court has recognized privacy as a fundamental right. However, the current surveillance regime reflects an emerging challenge. As the European Union

 ISSN: 2582-6433

considers regulations on surveillance technologies and data privacy, the need for robust protections in a rapidly evolvingdigital landscape becomes increasingly critical.

Legal Framework and Responses in India

Constitutional Framework

The Right to Privacy was not directly envisaged by the Constitution makers and as such does notfind a mention in Part III of the Constitution relating to Fundamental Rights. In the *MP Sharma vs Satish Chandra case*[9], the Supreme Court decided in favour of the practice of search and seizure when contrasted with privacy.

In 1975, the Indian Supreme Court's decision in *Gobind vs State of MP*[10] marked a significant moment for privacy rights, introducing the compelling state interest test from American law. Thistest requires that an individual's right to privacy may be overridden by a compelling state interest,which must be convincingly justified. Over time, the scope of privacy in India has broadened to include sensitive personal data, such as medical records and biometric information.

In 1997 in the matter of *PUCL vs Union of India*[11], commonly known as telephone tapping cases,the Supreme Court unequivocally held that individuals had a privacy interest in the content of theirtelephone communications.

The Indian Constitution does not explicitly guarantee the right to privacy. However, Indian courtshave interpreted Article 21—the right to life and liberty—to encompass a limited right to privacy.This interpretation was challenged in the 2015 case Justice *K.S. Puttaswamy vs. Union of India*[12].On August 24, 2017, the Supreme Court ruled that privacy is a fundamental right, integral to the right to life and personal liberty under the Constitution. The Court clarified that this right is not absolute and is subject to reasonable restrictions, similar to other fundamental rights.

[9] MP Sharma vs Satish Chandra,1954 SCR 1077
[10] Gobind vs State of MP, 1975 AIR 1378, 1975 SCR (3) 946
[11] PUCL vs Union of India, AIR 1997 SC 568 / (1997) 1 SSC
[12] Justice K.S. Puttaswamy vs. Union of India (2017) 10 SCC 1

 ISSN: 2582-6433

Existing Laws on Privacy

Presently, there is no specific legislation dealing with privacy and data protection. The protectionof privacy and data can be derived from various laws pertaining to information technology, intellectual property, crimes and contractual relations**.**

(i) Information Technology Act, 2000

In the absence of a specific law on privacy, this right is legally viewed under the Information Technology Act, 2000. The Act has some express provision guarding individuals against breach of privacy by corporate entities. The Act was amended in 2008 to insert Section 43 A which madethe Companies compromising sensitive personal data liable to pay compensation.

Exercising its powers under Section 43A of the IT Act, 2000, the Government framed eight rulesto protect privacy of an individual. These all relate to seeking permission by a company before accessing privacy data of individuals and fixing liabilities for violation of the same[13].

(ii) Credit Information Companies Regulation Act,2005("CICRA")

As per the CICRA, the credit information pertaining to individuals in India have to be collected asper privacy norms enunciated in the CICRA regulation. Entities collecting the data and maintaining the same have been made liable for any possible leak or alteration of this data. Basedon Fair Credit Reporting Act and Graham Leach Bliley Act, the CICRA has created a strict framework for information pertaining to credit and finances of the individuals and companies in India. The Regulations under CICRA which provide for strict data privacy principles have recentlybeen notified by the Reserve Bank of India.

***(iii) Intellectual Property Laws*:**

The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offence. Section 63B of the Indian Copyright Act provides that any person who knowingly makes use on a computer of an infringing copy of computer program shall be punishable.

It is pertinent to mention here that the Indian courts recognise copyright in databases. It has

[13] Prabhash K Dutta, Right to Privacy: 5 bills yet no law, how Parliament has dealt with personal data protection, India Today, http://indiatoday.intoday.in/story/right-to-privacy-fundamental-right-parliament/1/1032794.html last seen on 29/08/2024

 ISSN: 2582-6433

been held that compilation of list of clients/customers developed by a person by devoting time, money,labour and skill amounts to "literary work" wherein the author has a copyright under the CopyrightAct. As such if any infringement occurs with respect to data bases, the outsourcing parent entity may have recourse under the Copyright Act also.

(iv) Digital Personal Data Protection Act (DPDP Act), 2023

The law came into effect August 11, 2023 and covers personal data collected in digital format, or collected by other means and later digitized. The law is intended to protect personal information for citizens in the world's most populous country, and increase accountability for organizations that handle a lot of such data, including those with online operations and that run mobile apps.

Supreme Court Key conclusions from the judgment in *Justice K.S.Puttaswamy (Retd) vs Union of India*:

1. Life and personal liberty are inalienable rights central to human dignity and the Indian Constitution.
2. The recognition of the right to privacy is not a constitutional amendment but a judicial interpretation.
3. Privacy includes personal intimacies, family life, marriage, procreation, sexual orientation,and the right to be left alone.
4. Personal lifestyle choices are integral to privacy.
5. Privacy is inherent to individuals, even in public spaces.
6. Constitutional interpretation must adapt to technological advancements and societal changes.
7. Privacy is not absolute and must be balanced against permissible legal restrictions.
8. Privacy has both negative (protection from state intrusion) and positive (state protection ofprivacy) aspects.
9. Privacy is a fundamental right protecting individual autonomy from state and non-state interference.
10. The home environment must safeguard family, marriage, procreation, and sexual orientationas key elements of dignity.
11. Privacy is crucial in a diverse nation and must be upheld as a fundamental right.
12. Privacy rights are fundamental and not subject to majority opinion.
13. Privacy is an inherent fundamental right under Part III of the Constitution, subject to

 ISSN: 2582-6433

reasonable restrictions.

Judicial Pronouncements by Supreme Court on Privacy[14]

In the following seven cases, the Supreme Court had upheld the Right to Privacy:

1964	***KHARAK SINGH VS STATE OFUP & OTHERS (1963 AIR SC 1295)***	**SURVEILLANCE INTRUDES INTO PRIVACY:** This case is among the most cited cases in India when it comes to privacy. Here, a majority of a six-judge bench held that unlawfulintrusion into the home violates personal liberty.
1997	***PUCL VS UNION OF INDIA (AIR1997 SC 568)***	**TELEPHONE TAPPING INVADES PRIVACY:** A division bench held that a telephone conversation is an exercise in freedom of expression, and that telephone tapping is an invasion of privacy.
1998	***MR X VS HOSPITAL Z (1998 (8)SCC 296)***	**PRIVACY ISN'T ABSOLUTE:** The case concerned revealing the HIV status of a patient by a doctor. A division bench held the right to privacyisn't absolute. A doctor may disclose a patient's HIV status to the partner.
2008	***HINSA VIRODHAK SANGH VS MIRZAPUR MOTI KURESH JAMAT (AIR 2008 SC 1892)***	**CHOICE OF FOOD PERSONAL:** A division bench upheld the closure of slaughterhouses in Ahmedabad during the Jain Paryushan festival.It also observed that what one eats is part of one‟s right to privacy.

[14] Privacy and The Supreme Court, The Times of India, August 25, 2017

 ISSN: 2582-6433

2009	***JAMIRUDDIN AHMED VS STATE OF WEST BENGAL(CRIMINAL APPEAL NO. 1535 OF 2008)***	**RAID WITHOUT REASON NOT OKAY:** A division bench ruled that search/seizure without recording valid reasons violates the right to privacy
2011	***RAM JETHMALANI & OTHERSVS UNION*** **OF INDIA (2011) 8 SCC 1**	**CAN'T REVEAL BANK DETAILS WITHOUT VALID GROUNDS:** Popularly known as the "Black Money Case", here the Supreme Court held that revealing an individual"s bank account details without establishing grounds toaccuse them of wrongdoing violates their rightto privacy
2012	***SUPREME COURT TAKES SUOMOTU NOTICE OF THE RAMLILA MAIDAN INCIDENT***	**RIGHT TO SLEEP IS PART OF RIGHT TO PRIVACY:** The Supreme Court took *suo motu* cognizance of the crackdown on sleeping anti-corruption protesters camping at Ramlila Maidan led by Baba Ramdev. Identifying Rightto Sleep as an aspect of the Right to Dignity and Privacy, the court refused to permit "illegitimate intrusion into a person"s privacy as right to privacy is implicit in the right to lifeand liberty"

Role of Ministry of Electronics and Information Technology[15]

"The Cyber Law & Data Governance Division, operating under the Ministry of Electronics and Information Technology (MeitY), assumes a pivotal role in shaping India's digital landscape. Sincethe inception of the Information Technology Act in 2000, this division has been at the forefront, fostering electronic transactions, providing legal validation for e-commerce, facilitating e- governance, preventing computer-based crimes, and implementing robust security measures.

A notable recent addition to the division's initiatives is the Digital Personal Data Protection Act of 2023, a landmark legislation that adeptly balances individual privacy rights with the

[15] Cyber Law and Data Governance, Ministry of Electronics and Information Technology, available at https://www.meity.gov.in/cyber-security, last seen on 27/08/2024

 ISSN: 2582-6433

imperative to process digital personal data for lawful purposes. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 further showcase the division's commitment to regulating social media intermediaries, online gaming, and safeguarding digital citizens. The establishment of a Grievance Appellate Committee reflects the division's dedication to resolving social media grievances where grievance officers couldn't provide relief to the social media users in India.

Moreover, the division actively pioneers frameworks for data governance and protection, crucial for establishing an open, safe, trusted, accountable, and adaptable cyberspace. Acknowledging data protection as a fundamental right for Indian citizens, the division formulates policies to safeguard these rights. Furthermore, the division delves into the legal implications of cutting-edgetechnologies such as IoT, Blockchain, and Artificial Intelligence, while also addressing aspects of Competition Law, Company Law, Copyright Act, and Intellectual Property Rights (IPR) protection within the domain of information technology. In essence, the division operates as a guardian of digital rights, ensuring a secure cyberspace that is indispensable for the nation's digitaleconomy growth."

Role of Justice Sri Krishna committee in Data Protection Laws[16]

In the year 2017, the government of India, through its Ministry of Electronics and Information Technology, appointed a committee of ten members under the chairmanship of Justice B.R. Krishna (a retired Supreme Court judge). This committee was supposed to submit a detailed reporton the introduction of the data privacy law in India. The committee finally submitted its report onthe data protection framework on July 27, 2018.

- The committee recommended a clear distinction between sensitive personal data and critical personal data and separate provisions for the collection and processing of differentkinds of data. It was suggested that the term 'personal data' is any kind of data that allowsidentification of an individual, whether directly or indirectly. However, sensitive personaldata is in relation to more intimate matters such as caste, religion and sexual orientation ofa person. It was also made clear that the critical personal data should be processed in the centres that are located within the country only.

[16] Adv. Komal Arora, Data protection and data privacy laws in India, iPleaders, available at https://blog.ipleaders.in/data-protection-laws-in-india-2/#Role_of_Justice_Sri_Krishna_committee_in_data_protection_laws, last seen on 26/08/2024

 ISSN: 2582-6433

- The reports suggested that there is a fiduciary relationship between the service provider and individuals whose data is collected. So, the service provider is always under an obligation to deal with the personal data of the individuals in a fair and transparent manner and also to give the individual notice of data collection at various points. Also, the service provider would be bound by the 'purpose limitation principle', which states that personal data should be collected only for limited, explicit and specified purposes.
- The law was suggested not to have any retrospective effect and would be enforced forthe future, but only in a structured manner.
- The committee strongly suggested that the processing of personal data should have clear, specific and lawful purposes alone. The data should be processed only when it'sconsented to by the individual. This consent may, at any time, be withdrawn by the individual.
- A special mention was made in regard to the data on children. It said there needed to bestricter provisions for protection of their data.
- It was also pointed out that there may be four situations in which non-consensual processing of data may be allowed. These are:

1. When the processing is relevant for the state in order to do its welfare functions.
2. When it's required to comply with the law or legal orders within India.
3. When the processing is necessitated by the need to act upon it promptly.
4. in the scenario of employment contracts as well.

- The committee also put forth the idea that all organisations and firms that collect personal data should mandatorily appoint data protection officers. These officers would go on to become the main point of contact for the users who face any grievance in theirdata collection by the concerned company.
- The committee also made a key recommendation of imposing higher penalties rangingfrom 2-4% of the company's worldwide turnover or fines between Rs. 5 crore and Rs.15 crore, whichever is higher.
- Another highlight of the committee's report was that the data protection law enacted would have jurisdiction over the processing of personal data when that data has been used, stored, disclosed, or collected anywhere in India; it doesn't matter where the datais actually processed.

 ISSN: 2582-6433

- The report also suggested the setting up of a data protection authority that would be an independent regulatory body responsible for the enforcement and implementation of the data privacy law. This body would be responsible for conducting research and spreadingawareness on the issues as well. Any decision rendered by this authority could be appealed against and heard by an appellate body.
- It was also stated by the committee that there are certain rights of an individual, such asthe right to access their data, to correct it, withdraw their consent, right to object to thedata processing, right to be forgotten, etc.
- As per the report of the committee, there would be amendments needed in laws such asthe Information Technology Act, 2000; the Census Act, 1948; the Aadhar Act, 2016, Right to Information Act, 2005.

After receiving the recommendations of the committee and a draft privacy law bill, the bill remained in limbo. Its first draft was made public in July 2018 and then revised again in December2019. The Bill was then referred to a joint parliamentary committee for its report, which submittedits report two years later, that is, in December 2021. Later, the government decided to withdraw the bill as there were too many proposed changes to be incorporated. Later in November 2022, theMinistry of Electronics and Information Technology released a draft bill for public consultations. Finally, in August 2023, the government introduced the Digital Personal Data Protection Bill, 2022. After much consultation and amendment, the Digital Personal Data Protection Bill of 2023was finally passed and it received the President's assent after six years.

Digital Personal Data Protection Act, 2023

An Act provides for the processing of digital personal data in a manner that recognizes both the rights of the individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

1. The Act protects digital personal data (that is, the data by which a person may be identified) byproviding for the following:
    a. The obligations of Data Fiduciaries (that is, persons, companies and government entities who process data) for data processing (that is, collection, storage or any other operation on personal data);
    b. The rights and duties of Data Principals (that is, the person to whom the data

 ISSN: 2582-6433

relates);and

c. Financial penalties for breach of rights, duties and obligations.

The Act also seeks to achieve the following:

a. Introduce data protection law with minimum disruption while ensuring necessary changein the way Data Fiduciaries process data;
b. Enhance the Ease of Living and the Ease of Doing Business; and
c. Enable India's digital economy and its innovation ecosystem.2.The Act is based on the following seven principles:
a. The principle of consented, lawful and transparent use of personal data;
b. The principle of purpose limitation (use of personal data only for the purpose specified atthe time of obtaining consent of the Data Principal);
c. The principle of data minimisation (collection of only as much personal data as is necessaryto serve the specified purpose);
d. The principle of data accuracy (ensuring data is correct and updated);
e. The principle of storage limitation (storing data only till it is needed for the specifiedpurpose);
f. The principle of reasonable security safeguards; and
g. The principle of accountability (through adjudication of data breaches and breaches of theprovisions of the Bill and imposition of penalties for the breaches).

2. The Act has few other innovative features:
The Bill is concise and SARAL, that is, Simple, Accessible, Rational &Actionable Law asit—
    a. Uses plain language;
    b. Contains illustrations that make the meaning clear;
    c. contains no provisos ("Provided that…"); and
    d. Has minimal cross-referencing.

4. By using the word "she" instead of "he", for the first time it acknowledges women inParliamentary law-making.

5. The Bill provides for following rights to the individuals:
    a. The right to access information about personal data processed;

 ISSN: 2582-6433

b. The right to correction and erasure of data;
c. The right to grievance redressal; and
d. The right to nominate a person to exercise rights in case of death or incapacity.

For enforcing his/her rights, an affected Data Principal may approach the Data Fiduciary in the first instance. In case he/she is not satisfied, he/she can complain against the Data Fiduciary to theData Protection Board in a hassle-free manner.

6. The Act provides for following obligations on the data fiduciary:
    a. To have security safeguards to prevent personal data breach;
    b. To intimate personal data breaches to the affected Data Principal and the DataProtection Board;
    c. To erase personal data when it is no longer needed for the specified purpose;
    d. To erase personal data upon withdrawal of consent;
    e. To have in place grievance redressal system and an officer to respond to queries from Data Principals; and
    f. To fulfill certain additional obligations in respect of Data Fiduciaries notified as Significant Data Fiduciaries, such as appointing a data auditor and conducting periodic Data Protection Impact Assessment to ensure higher degree of data protection.

7. The Act safeguards the personal data of children also.
    a. The Bill allows a Data Fiduciary to process the personal data of children only withparental consent.
    b. The Bill does not permit processing which is detrimental to well-being of childrenor involves their tracking, behavioural monitoring or targeted advertising.

8. The exemptions provided in the Bill are as follows:
    a. For notified agencies, in the interest of security, sovereignty, public order, etc.;
    b. For research, archiving or statistical purposes;
    c. For startups or other notified categories of Data Fiduciaries;
    d. To enforce legal rights and claims;

 ISSN: 2582-6433

e. To perform judicial or regulatory functions;
f. To prevent, detect, investigate or prosecute offences;
g. To process in India personal data of non-residents under foreign contract;
h. For approved merger, demerger etc.; and
i. To locate defaulters and their financial assets etc.

Conclusion

The DPDP Act, the result of over five years of debate and negotiation, represents the beginning of formal personal data protection regulation. How effectively personal data privacy is safeguarded will depend on the regulatory developments and institutional frameworks established in the coming years. While the new law lays the essential groundwork, it alone is insufficient to ensure real data privacy.

It is uncertain whether earlier drafts of the bill would have provided significantly better privacy protection. However, the evolution of the law's content reflects a shift in the government's approach to privacy. The current version of the law, by imposing lower compliance costs on Indianbusinesses compared to earlier drafts, is a positive development.

In general, the law is both modest and practical, which is a good thing. Nevertheless, its practicalitysometimes comes at the expense of privacy interests. The significant discretionary authority granted to the central government means that the effectiveness of privacy protection will largely depend on the government's dedication to upholding it.

References

1. The Impacts of Technology on Privacy and Cybersecurity, Medium, available at https://fastfacts101.medium.com/the-impact-of-technology-on-privacy-and-cybersecurity-4d2037331311, last seen on 24/08/2024
2. Digital Privacy and Data Protection Laws in India, The Amikus Quriae, available at https://theamikusqriae.com/digital-privacy-and-data-protection-laws-in-india/, last seen on 21/08/2024
3. What is Digital Privacy and its Importance, IEEE Digital Privacy, available at https://digitalprivacy.ieee.org/publications/topics/what-is-digital-privacy-and-its-importance, last seen on 24/8/2024

 ISSN: 2582-6433

4. Palmer, D.E., 2005, "Pop-ups, cookies, and spam: toward a deeper analysis of the ethical significance of internet marketing practices", Journal of business ethics, 58(1–3): 271– 280(2005).
5. Steven Bellman, Eric J. Johnson, Gerald L. Lohse, Communications of the ACM, Volume44, Number 2, The ACM Digital Library, Pages 25-27(2001)
6. Privacy and Information Technology, Standford Encyclopedia of Philosophy, available at https://plato.stanford.edu/entries/it-privacy/#DevInfTec, last seen on 23/08/2024
7. Dechesne, F., M. Warnier, & J. van den Hoven, Ethics and Information Technology, available at https://link.springer.com/article/10.1007/s10676-013-9326-1, last seen on 26/08/2024
8. St´ephanie Delaune, Steve Kremer, Mark Ryan, Coercion-Resistance and Receipt-Freeness in Electronic Voting, 5,6(2008)
9. Prabhash K Dutta, Right to Privacy: 5 bills yet no law, how Parliament has dealt with personal data protection, India Today, http://indiatoday.intoday.in/story/right-to-privacy-fundamental-right-parliament/1/1032794.html last seen on 29/08/2024
10. Cyber Law and Data Governance, Ministry of Electronics and Information Technology, available at https://www.meity.gov.in/cyber-security, last seen on 27/08/2024
11. Adv. Komal Arora, Data protection and data privacy laws in India, iPleaders, available at https://blog.ipleaders.in/data-protection-laws-in-india-2/#Role_of_Justice_Sri_Krishna_committee_in_data_protection_laws, last seen on26/08/2024
12. Farsana, Right to Privacy : Indian Context, Rader's Blog, https://timesofindia.indiatimes.com/readersblog/the-daily-roam/right-to-privacy-an- indian-context-55047/
13. The Impact of Technology on Privacy and Cybersecurity, Fast Facts 101, available athttps://fastfacts101.medium.com/, last seen on 25/08/2024