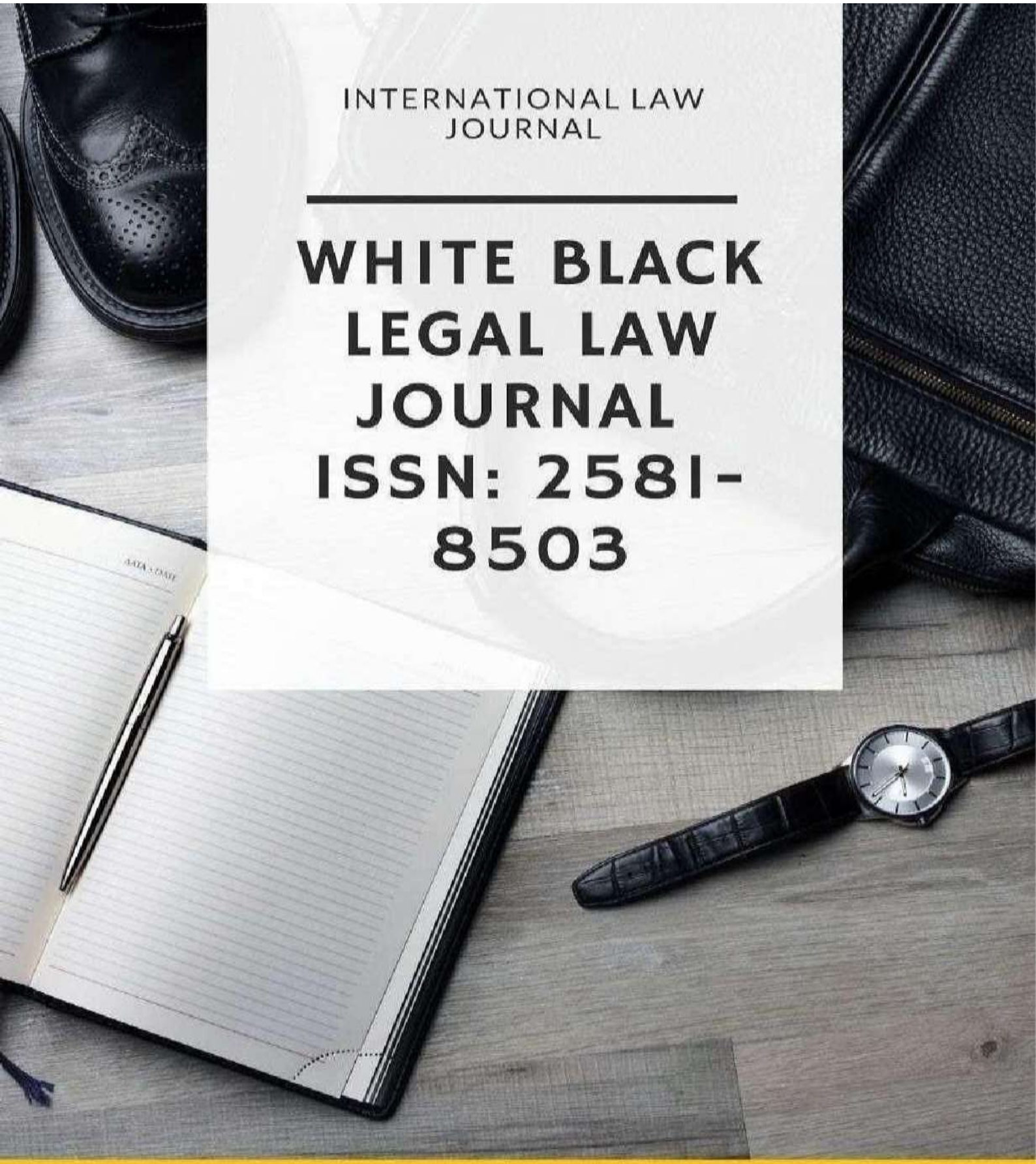

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

DATA PROTECTION AND PRIVACY: PRESENT SCENARIO AND LEGAL FRAMEWORK IN INDIA

AUTHORED BY - NIKITA BEGUM TALUKDAR

Abstract[1]

More people are utilizing digital platforms to fulfil a variety of needs, such as purchasing food, receiving health care, online shopping, e-banking, putting online food orders and even using social networking sites and instant messaging systems. Unfortunately, the number of personal data breaches from large digital service providers has increased drastically. Recent news has revealed how corporate powerhouses and prominent social networking sites make money by jeopardizing their customers' and users' data privacy. With the increased usage of data in this information era, protecting data privacy has become increasingly complex. People are ignorant toward the protection of data as a result they share their personal data with third parties, putting their privacy at risk. Personal data of citizens is left at the mercy of corporations and the government, despite the fact that it is deemed a fundamental right under Article 21 of the Indian Constitution. There is currently no data protection law in India, and one is urgently needed.

Author, through this paper aims to shed light on the evolution of right to privacy doctrine in India, analyse data breaches in recent times, the current legal framework on Data protection, discuss the features the Digital Personal Data Protection (DPDP) Act, 2023, Pegasus controversy and infringement of privacy and lastly the importance of data protection in India.

Keywords: Data protection, right to privacy, data protection bill, Pegasus controversy, Facebook data breach

[1] Nikita Begum Talukdar, Assistant Professor Senior Scale, University of petroleum and Energy Studies, Dehradun, Uttarakhand.

1. Introduction

"Data is the new oil," as the saying goes. Data has surpassed oil as the most valuable commodity in the twenty-first century. The Internet has given rise to completely new markets: those that acquire, store, and process personal data, whether directly or as a fundamental component of their business strategy. India is well on its way to becoming a digital economy, with about 450 million Internet users and a growth rate of 7-8 percent, and a significant market for foreign companies.[2] While the transformation to a digital age is underway, personal data processing has already become mainstream. The fact of today's digital environment is that practically every single activity that a person does in includes some type of data transaction. While data can be useful, the uncontrolled and indiscriminate use of data, particularly personal data, has generated concerns about an individual's privacy and autonomy. The term "Digital privacy" refers to a broad variety of concerns and topics. It may be defined as an individual's online privacy rights in relation to their data, as well as online infringement of those rights. Because of the ever-changing nature of the online space, privacy problems and challenges are constantly changing. This was also the subject of the Supreme Court's historic decision, which established the right to privacy as a fundamental right. It therefore becomes necessary to protect the data of the individual.

The Indian government has formed a Committee of Experts to look at different data protection concerns in India and proposed a Digital Personal Data Protection (DPDP) Act, 2023**.** The objectives is to "ensure the expansion of the digital economy while keeping individuals' personal data secure and secured."[3]

2. Right to privacy: Origin, Evolution and present position

2.1 Origin:

Individuals' right to privacy goes hand in hand with their freedom to control their own personalities. Its origins may be traced back to the idea that a human person has some natural or inherent rights. Since natural rights are inextricably linked to human personality, they are unalienable. To find out the origin of the privacy doctrine, we need to analyse it how the famous jurists have considered and

[2] Ministry of Electronics an IT, "Data Protection in India" February, 2018, *available* at https://www.digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf. (Last visited on 4/2/2022)
[3] Ibid.

defined privacy.

Aristotle, the Greek philosopher, distinguished between the public realm of political affairs (which he called the polis) and the private realm of human life (which he called the psyche) (termed oikos). This dichotomy may provide an early recognition of "a confidential zone on behalf of the citizen".[4] The division between the public and private realms established by Aristotle was a basis to limit governmental authority to public domain only. Private activities, on the other hand, should be kept for "private reflection, familial relationships, and self-determination."[5] The evolution of the notion of privacy has followed the public – private distinction to some extent.

William Blackstone discussed this issue when categorizing wrongs into private and public wrongs. Private wrongs are infringements of specific rights affecting individuals, and thus fall under the category of civil injuries. Public wrongs, according to him, "are defined as violations of general and public rights that harm the whole community and are referred to as crimes and misdemeanors".

John Stuart Mill, in his essay 'On Liberty,' (1859), "expressed the necessity to preserve a zone where the citizen's liberty is unfettered by the state's control. Mill proposed that the tyranny of the majority may be restrained by the recognition of civil rights such as the individual right to privacy, free speech, assembly", and "struggle between liberty and authority."[6]

According to J.S Mill:

"The only part of the conduct of any one, for which he is amenable to society, is that which concerns others. In the part, which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign."[7]

Samuel D Warren and Louis Brandeis discussed the evolution of the law to include the right to life as "a recognition of man's spiritual nature, his feelings, and his intellect."[8] The right to life had "come

[4] Michael C. James, "A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe, Vol. 29 Issue 2, *Connecticut Journal of International Law*, 261, (2014)
[5] *Id.* at 261.
[6] John Stuart Mill, *On Liberty* 13 (Batoche Books, 1859)
[7] *Id.* at 06.
[8] Warren and Brandeis, "The Right to Privacy", *Harvard Law Review* Vol.4, No. 5, 193 (1890)

to mean the right to enjoy life – the right to be let alone" when legal rights were expanded. Thus, the right "to be left alone" was an expression of "an inviolate personality," a core of freedom and liberty from which the human being had to be safeguarded. The emergence of photography was the technology that provided rationale for the need to protect an individual's privacy.

In today's globalized world driven by the internet and information technology, Warren and Brandeis' ringing insights on the influence of technology are nevertheless relevant. The connotations and scope of privacy have changed as society have progressed. Though many contemporary accounts attribute the Warren and Brandeis article with establishing the modern notion of the "right to privacy," historical evidence suggests that **Thomas Cooley** used the phrase "the right to be left alone" in his Treatise on the Law of Torts.[9] Cooley remarked of personal immunity:

"The right of one's person may be regarded to be a right of complete immunity; the right to be alone."[10]

The fact that traditional social institutions are being replaced as a result of urbanization and economic progress cannot be avoided. The tranquilly of self-sufficient rural lives has been replaced by urban ghettos. Thus, the necessity to defend the privacy of the being is no less pressing, when progress and technological change continuously as it threatens to bring the person into public gaze and portend to submerge the individual into a seamless web of interconnected lives.

2.2 Origin and Evolution in India:

There has been a controversy "whether of right to privacy is a fundamental right under Article 21 of the Indian Constitution". There are decisions where right to privacy has been considered as a fundamental right, but smaller benches gave these decisions.[11] However, the decisions of Supreme court in the following cases which was decided by a larger bench held that, "the Indian Constitution does not specifically protect the right to privacy: *M P Sharma* v. *Satish Chandra, District Magistrate, Delhi*[12] (decided by eight judges) and in *Kharak Singh* v. *State of Uttar Pradesh*[13] (decided by a Bench of six judges)."

---

[9] Thomas Cooley, *Treatise on the Law of Torts*, 2nd edition, (1888).
[10] *Id.* at 29.
[11] *Gobind* v. *State of Madhya Pradesh* (1975) 2 SCC 148; *R. Rajagopal* v. *State of Tamil Nadu* 1994) 6 SCC 632; *People's Union for Civil Liberties* v. *Union of India* (1997) 1 SCC 301.
[12] (1954) SCR 1077
[13] 1964) 1 SCR 332

Before discussing the present position on the right to privacy controversy, let us discuss the earlier case laws.

It was clearly observed in the **M.P Sharma case** that, *"right to privacy cannot be read into the Indian Constitution in the absence of a clause like the Fourth Amendment to the US Constitution."* However, the judgement in M P Sharma did not address whether other provisions of the fundamental rights, such as the right to life and personal liberty under Article 21, safeguard a constitutional right to privacy. Significantly, the Court observed in *R M Malkani* v. *State of Maharashtra*[14], which followed the decision of Kharak Singh case, that :

"Article 21 was invoked by submitting that the privacy of the appellant's conversation was invaded. Article 21 contemplates procedure established by law with regard to deprivation of life or personal liberty. Courts will protect the telephone conversation of an innocent citizen against wrongful or high handed interference by tapping the conversation. **The protection is not for the guilty citizen against the efforts of the police** to vindicate the law and prevent corruption of public servants. It must not be understood that the Court will tolerate safeguards for the protection of the citizen to be imperiled by permitting the police to proceed by unlawful or irregular methods."[15]

The observations of the court in the case of *Gobind* v. *State of Madhya Pradesh*[16] is very important while discussing about the evolution of privacy doctrine in India. It was emphasized, that "individual autonomy and the dangers of individual privacy is eroded by new developments", which "will make it possible to be heard in the street what is whispered in the closet". The Court also expressed reservations about adopting a broad definition of privacy because the right to privacy "is not explicit in the Constitution." The judgement in *R. Rajagopal* v. *State of Tamil Nadu*[17] has also assumed some significance with respect to doctrine of privacy. It regarded privacy as "implicit in the right to life and personal liberty under Article 21." It was again, reiterated, in the case *People's Union for Civil Liberties* v. *Union of India*[18] that, "right to privacy is a part of Article 21. The Court stated that wiretapping infringes on privacy and, as a result, the right to life and personal liberty under Article 21 and the freedom of speech and expression under Article 19(1) (a) is also infringed."

---

[14] (1973) 1 SCC 471
[15] *Id.* at 476.
[16] (1975) 2 SCC 148.
[17] 1994) 6 SCC 632;
[18] 1997) 1 SCC 301.

Due to the above controversy it was necessary to decide on this matter by a larger bench as to "whether right to privacy is a fundamental right under Indian Constitution or not."

2.3 Present position:

In 2015, many petitions were filed in the Supreme Court, alleging that, Aadhaar violated people's right to privacy, informational self-determination, and physical integrity. The petitioners claimed that enrolling in Aadhaar was a step toward creating a "Totalitarian State" and an empty threat for personal data leaks. The government argued that informational privacy does not exist before compelling State interests, according to the court, and is not an absolute right.

In 2017, a nine judge constitutional bench headed by CJI Justice Khehar, was formed to decide the matter "whether right to privacy is a fundamental right under Indian Constitution or not?" In this landmark judgement of *K.S. Puttaswamy (Retd)* v. *Union of India*,[19] the Court unanimously concluded that the right to privacy is a constitutionally protected right.

Thus, the court in this case overruled M.P Sharma case and over-ruled the decision of Kharak Singh to the extent that, "it holds that the right to privacy is not protected by the Constitution." It held that: "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."

1.3 Data privacy

The idea of privacy, has taken on a new meaning as a result of the digital revolution. With the passage of time, people's perceptions of privacy have transformed. Privacy is frequently weighed against ideals, such as societal security and safety. There is no empirical data on how individuals perceive privacy. Privacy, in general, refers "to the right to be left alone as well as the freedom from interruption or interference." Information privacy refers to the right to have some control over how your personal data is collected and utilized. The most straightforward approach to comprehend the concept of data privacy is to see it as the protection of private individuals' data while they use digital media. However, when people discuss digital privacy, they typically discuss it in terms of how it relates to Internet usage. The greater a user's social media sharing, the less privacy they have.

[19] (2017) 10 SCC 1.

Data may be divided into two categories: public data and personal data. Public data is information that is available to the general public, such as court documents, records of birth and death, and basic corporation information. Private data is personal to a person or organisation and cannot be freely transferred by anyone without the individual's permission. Financial information, family information, browsing information, tastes, psychological features, places, conduct, photos and similar information are all included. It might be a mix of these characteristics or even conclusions based on the enhanced data.

2.4 Data Breaches in India in recent times:

Cyberattacks and data breaches raged on while the pandemic kept people inclined to their gadgets. According to a survey by consultancy firm Accenture, the average number of Cyber attacks per company has increased by 31% since 2020. Furthermore, successful breaches to companies through the supply chain increased from 44% to 61%. In addition, according to the Indian Computer Emergency Response Team (CERT-In) "over six lakh cyber security incidents occurred in India in the first six months of 2021."[20] Since 2004, CERT-In has operated as the nodal agency for addressing to computer security breaches whenever such breaches occur.

In 2021, High Court of Delhi, has ordered the Centre to respond to a petition questioning the CERT-In inactivity, in the wake of allegations of purported cyber security infringements and data leaks on digital platforms including: Big Basket, Domino's, MobiKwik, Air India, Facebook and Cowin vaccination website.

Let us examine the breaches that happened in these companies in the year 2021.

- According to reports, "there was data breach affecting approximately 20 million Big Basket customers, which is currently being sold on the dark web. There are 100 million MobiKwik users' data and 3.5 million KYC data for sale on the dark web."[21]

[2020]Aditya Saroha, "Explained-What kept cybersecurity busy in 2021?", *The Hindu*, November 21, 2021, *available* at https://www.thehindu.com/sci-tech/technology/explained-what-kept-cybersecurity-busy-in-2021/article37995271.ece. (Last visited on 2/2/2022)

[21] Nivedita, "HC seeks Centre's response to petition on cyber security breaches", *The Hindu*, August 16, 2021, *available* at https://www.thehindu.com/news/national/delhi-high-court-seeks-centres-stand-on-plea-concerning-data-leaks-at-air-india-bigbasket-dominos-mobikwik/article35937434.ece. (Last visited on 2/2/2022)

- "Around 180 million order details and one million credit card details of Domino's consumers have been compromised," according to reports. The data breach includes customer names, email addresses, phone numbers, delivery addresses, and payment information.[22]
- There was also a data breach at Air India, which exposed the personal information of nearly 4.5 million worldwide passengers. Passengers' personal details have all been leaked.[23]
- The most recent Facebook data breach occurred in April 2021, when 533 million Facebook users' personal information was made public on an online hacking forum. This data, which contained names, phone numbers, and other details, was first scraped in 2019 using Facebook's contact importer. Facebook has come under scrutiny from the European Union for infringing the General Data Protection Regulation as a result of this and other instances. For these data privacy breaches, the Irish Data Protection Commission proposed a penalty of up to 36 million euros in October 2021.[24]
- Hackers also attacked the Cowin app, a vaccination portal, in order to steal personal information. They created bogus Cowin applications, posing as the official portal for reserving covid vaccination times or enrolling for the vaccination, and distributed them via viral communications. "The SMS contains a link that downloads and instals the malicious programme on Android-based smartphones, which then distributes to victims' contacts through SMS.[25]

2.4.1 Pegasus controversy and infringement of data privacy

NSO Group, an Israeli surveillance company, created Pegasus, a spyware that allows spies to hack into phones. The situation was brought to light in 2019 when WhatsApp filed a case against the company in a US court. Amnesty International, along with 13 media outlets from around the world, produced a report in July 2021 detailing how the malware was used to snoop on hundreds of people, including Indians. While the NSO says that its spyware is solely marketed to governments, none of the countries have confirmed this.[26]

---

[22] *Id.*
[23] *Id.*
[24] Aaron Holmes, "533 million Facebook users' phone numbers and personal data have been leaked online", *Business Insider India,* November 21, 2021, *available* at https://www.businessinsider.in/tech/news/533-million-facebook-users-phone-numbers-and-personal-data-have-been-leaked-online/articleshow/81889315.cms. ((Last visited on 2/2/2022)
[25]Aditya Saroha, "Explained- What kept cybersecurity busy in 2021?", *The Hindu,* July 21, 2021, *available* at https://www.thehindu.com/sci-tech/technology/explained-what-kept-cybersecurity-busy-in-2021/article37995271.ece. (Last visited on 2/2/2022)
[26] Special correspondent, "Pegasus surveillance", *The Hindu,* July 21, 2021, *available* at https://www.thehindu.com/topic/pegasus-surveillance/. (Last visited on 2/2/2022)

This spyware was a threat to the privacy that, once installed it may send the target's contacts, calendar events, phone conversations, and messages sent through messaging applications such as WhatsApp and Telegram to the spyware controller. By turning on the phone's camera or microphone, it may also convert it into a surveillance device. Several politicians, lawyers, journalists and activists in India were targeted and their data has been leaked by this software.[27] According to The Wire, "which undertook the research with foreign partners, Indian ministers, government officials, and opposition leaders are among those whose phones may have been hacked by the spyware".[28]

The organization which created Pegasus, claims to have 60 clients in around forty countries, though the names of these clients have not been disclosed. India, and the United Arab Emirates are among its top ten clients.[29] So, as per the reports, the government of India has used the spyware Pegasus to snoop on its own citizens.

The order by a Bench led by India's Chief Justice, N.V. Ramana, is notable for stands out for asserting two clear principles: that "surveillance, or even the knowledge of being spied on, affects how individuals exercise their rights, necessitating the Court's interference and that there is no blanket prohibition on judicial review simply because the threat of national security is raised." The Court found the government's failure to throw any light on an issue involving suspected infringement of citizens' rights to be unacceptable, and stated that national security grounds cannot be utilized by the government to "get a free pass." The Supreme court through this order, on October 27, 2021, also constituted an independent expert technical committee to investigate the claims, to be led by Justice R.V. Ravindra,, a former apex court judge.[30]

The Supreme Court's decision in this matter is an effective step to safeguard citizens from illegal surveillance. It also observed in its ruling that, "the privacy of the individuals are sacred and should

---

[27] I *Id.*

[28] Special correspondent, "Pegasus spyware used to 'snoop' on Indian journalists, activists", *The Hindu,* July 21, 2021, *available at* https://www.thehindu.com/news/national/pegasus-spyware-used-to-snoop-on-indian-journalists-activists/article35399573.ece. (Last visited on 2/2/2022)

[29] P.J George, "Explained-Pegasus and the laws on surveillance in India", *The Hindu,* July 25, 2021, *available at* https://www.thehindu.com/news/national/explained-pegasus-and-the-laws-on-surveillance-in-india/article35516430.ece. (Last visited on 2/2/2022)

[30] Ashok, "A credible probe: On Supreme Court verdict on Pegasus row", *The Hindu,* October 28, 2021, *available at* https://www.thehindu.com/opinion/editorial/a-credible-probe-the-hindu-editorial-on-supreme-court-verdict-on-pegasus-row/article37200571.ece. ((Last visited on 2/2/2022)

be fully respected and government's right to pry into people's sacred private space in the name of national security is not absolute."

3. Need of Data Protection Law in India:

While data can be useful, the uncontrolled and arbitrary use of data, particularly personal data, has prompted concerns about an individual's privacy and autonomy. This was also the subject of the Supreme Court's landmark decision, which recognized the right to privacy. In essence, a comprehensive legislative framework for data protection will keep citizens' personal data safe and secure thereby providing a strong foundation for data-driven innovation and entrepreneurship in India. A data protection legislation has the ability to provide effective legal remedies, give teeth to the fundamental right, and create impediments for data fiduciaries to unlawfully gather personal data. Since they do not form a "state" within the sense of Article 12, the Indian constitution does not now offer writ remedies against entirely private organisations. This means that, in every case where a purely private body infringes on a citizen's right to privacy, Indian law provides only limited recourse, such as section 43A of the IT Act, 2000 read with the IT Rules, 2011.

The need of Data protection Law is essential because the current provisions related to data protection and privacy have several limitations, mentioned below:

- The primary objective of IT Act is not protection of data protection.
- The provisions of the IT Act on Data Protection have a very limited scope and application.
- The IT Act's provisions do not name any specific government authority that would oversee data protection in India.
- Except for Section 72A, the IT Act has no consequences for data breaches.
- The IT Rules only apply to information that is created and sent electronically.
- Government or the state are not covered under the IT Rules and they only apply to body corporates when a contract is not in existence, which means they may be easily avoided by getting into a contract.

4. Laws protecting data privacy in India:

Presently, India does not have any comprehensive data protection legislation in place. The Information Technology Act of 2000 ("the IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("the IT Rules") are India's legislative framework for data security and privacy. The Information Technology Act (2000) was amended by the parliament to add Sections 43A and 72A, which provide a right to compensation for disclosing personal information

There is no national regulatory authority in India for the protection of personal data. The Ministry of Electronics and Information Technology is in charge of enforcing the IT Act as well as providing regulations and other clarifications. The Personal data Protection Bill (PDP Bill) proposes the establishment of an Indian Data Protection Authority, which will be responsible for safeguarding data principals' rights, preventing exploitation of personal data, and enforcing compliance with the new legislation. India has not yet passed the data protection bill.

4.1 The Laws at present in India for Data Protection are as follows:

As per Section 43A of the IT Act, "it imposes a liability on a body corporate (including a firm, sole proprietorship, or other association of individuals engaged in commercial or professional activities) that possesses, deals, or handles any sensitive personal data or information in a computer resource, which it owns, controls, or operates. It has to pay damages to the person affected if there is any wrongful loss or wrongful gain to any such person, because of the negligence in implementing and maintaining reasonable security practices and procedures to protect the information of the person affected."[31]

As per Section 43 of IT Act: It states that "anyone who gains secure access to a computer system without the permission of the system's owner, or extracts and downloads any information, or steals and destroys any information, or follows anyone to slither and destroy any source code from the

[31] The Information Technology Act, 2000 (Act 21 of 2000), s. 43: "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected."

computer, will be held liable for damages. A person shall be responsible to pay compensation to the individual who has been harmed, the amount of one crore rupees."

Section 66 E of IT Act: Under this section, anybody who willfully captures a photograph and distributes it without the permission of the person, infringing on the individual's privacy, will be punishable with a sentence of up to three years in jail or a fine of up to two lakh rupees, or both.

Section 72 of IT Act: "If a person with authorization to access and secure any information, book, record, document, or electronic file discloses such data without permission, shall be sentenced to two years in jail or a fine of up to one lakh rupees, or both".

Section 72 A of the IT Act states that, "any person (including an intermediary) who has secured access to any material containing personal information about another person while providing services under the terms of a lawful contract, with the intent of causing or knowing that he is likely to cause wrongful loss or gain, discloses such material to any other person without the consent of the person concerned, or in breach of a lawful contract, shall be punished with 3 years imprisonment or fine(up to 5 lakh rupees) or both."32

Under Section 43A of the IT Act, the central government issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) **IT Rules**. The Rules imposes additional duties on Indian commercial and corporate enterprises pertaining to the acquisition and disclosure of sensitive personal data or information, which are similar to the GDPR and the Data Protection Directive.

Under the IT Rules, individuals have the right to their personal information, and any corporate entity

[32] The Information Technology Act, 2000 (Act 21 of 2000), s 72 A: "¨Punishment for disclosure of information in breach of lawful contract. –Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both".

must establish privacy policy. It also gives people the right to access and correct their information, and it makes it compulsory for the corporations to acquire consent before disclosing sensitive personal information, with the exception of law enforcement, where consent can be withdrawn.

4.2 The Digital Personal Data Protection (DPDP) Act, 2023

Since the SC ruling in 2017, India has been working on enacting a comprehensive data privacy law. Retd. Justice B N Srikrishna, headed a committee that was formed to prepare a data protection act. Based on the committee's recommendations, the Government proposed the Personal Data Protection Bill 2019. A legislative committee examined this version and released its findings in December 2021.5. However, the government retracted this bill and released a new draft, the Digital Personal Data Protection Bill, 2022, for public comment in November 2022. This draft differed significantly from the other versions. The Digital Personal Data Protection (DPDP) Act, 2023.is the second and fourth versions of the measure that have been introduced in Parliament.

The processing of digital personal data that is gathered online or offline and then converted to digital form inside the borders of India is subject to the Digital Personal Data Protection (DPDP) Act, 2023. If it entails offering products or services to the data principals inside India's borders, it also applies to the processing of digital personal data outside of that country.

A. Key Features of the DPDP Act 2023:

1. Significant data fiduciary

The DPDP Act emphasizes the function of a significant data fiduciary (SDF), which is determined by the government based on the amount and sensitivity of processed personal data as well as the related risk. Specifically, this calls for the appointment of an independent data auditor, a data protection impact assessment (DPIA), and a data protection officer (DPO) with headquarters in India.

2. Consent

With the individual's consent, personal data may only be processed for legitimate purposes. For some acceptable purposes, such an individual's voluntary data sharing or the State's processing of applications for benefits, licenses, permits, and services, consent might not be necessary.[33]

[33] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) S. 4.

3. **Data fiduciaries**[34]

Data fiduciaries will be responsible for ensuring data accuracy, data security, and data deletion after intended use.[35]

4. **Rights of an Individual**

a) **Informational right:** People will be entitled to more information about how their data is used, and the data fiduciary will provide this information in an easily comprehensible manner.[36]

b) **The right to file a grievance:** People will have the ability to file a grievance with a data fiduciary through easily accessible channels.[37]

c) **Right to rectification and deletion**: People are entitled to have their erroneous or incomplete data corrected and to have their data erased if it is no longer needed for processing.[38]

d) **Right to nominate**: In the event of death or incapacity, individuals may designate any other person to exercise these rights.[39]

5. **Penalties**

The penalty clause in the DPDP Act is another noteworthy aspect. Data fiduciaries who violate the laws face fines of up to INR 250 crore. Among them are: Breach of the data principal's obligation to observe up to INR 10,000. Up to INR200 crore may be lost if the data protection board and the impacted data principals are not notified of a breach involving personal data. Breach of an additional responsibility up to INR 200 crore with regard to children.[40]

[34] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) S. 2 (i) "Data Fiduciary" means "any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."
[35] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) S. 4.
[36] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) S. 11
[37] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) S. 13
[38] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) S. 12
[39] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) S. 14
[40] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) S. 33, The Schedule.

6. Exemptions

For certain reasons, such as maintaining public order, state security, or deterring crime, the central government may waive the Act's obligations for government entities.[41]

7. Data Protection Board of India

The Data Protection Board of India will be established by the central government. The Board's primary responsibilities are to: (i) oversee compliance and levy fines; (ii) instruct data fiduciaries on what steps to take in the event of a data breach; and (iii) hear complaints from individuals who may have been impacted. Members of the board may be reappointed after their initial two-year term.[42]

B. Issues and challenges of the Act

Infringement of Privacy:

- Data collection, processing, and retention beyond what is necessary may result from exemptions to the State's right to handle data on the basis of things like national security. The fundamental right to privacy might be violated by this. The State may collect, process, and retain more data than is necessary if it is granted exemptions. This might not be appropriate and might go against the privacy right. The Act gives the Central government the authority to waive any or all of the requirements pertaining to processing carried out by government agencies in order to achieve objectives including maintaining public order and state security. Except for data security, none of the duties and rights of data fiduciaries and data principals will apply in specific situations, such as when processing is necessary for the avoidance, detection, and prosecution of offences.
- The Act does not mandate that government organisations destroy personal information once the processing goal has been satisfied. Under the aforementioned exclusions, a government agency may gather information about a citizen in order to compile a 360-degree profile for monitoring purposes on the grounds of national security. It might use information kept on file by several government departments for this.

[41] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) S. 17.
[42] The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) Ss. 18-26.

Right to data portability and the right to be forgotten not provided:

- **Right to Data Portability:** Under this legal protection, data principals are permitted to take their data in a commonly-used, machine-readable format from data fiduciaries and utilize it for their own purposes. The data principal has more control over their data as a result. It might make data movement between data fiduciaries easier. One worry has been that it would divulge the data fiduciary's trade secrets. The Srikrishna Committee (2018) had advised that the right should be guaranteed to the extent that it is possible to give the information without disclosing such trade secrets. Trade secrets cannot be used as an excuse to deny right-to-right data portability; instead, it can only be refused on the basis of technical viability, according to the Joint Parliamentary Committee.[43]
- **Right to be Forgotten:** This pertains to people's ability to restrict the amount of personal information that is disclosed online. According to the Srikrishna Committee (2018), the concept of the right to be forgotten aims to impose memory constraints on an otherwise boundless digital realm. The Committee did point out that this right could need to be balanced against other rights and interests, though.[44]The exercise of this right may infringe upon the freedom of expression and the right to knowledge for another person. The degree of sensitivity of the personal information that needs to be restricted, the public interest in the personal information, and the significance of the data principal in public life are some of the elements that may determine its applicability.

5. Conclusion

A data protection law has the potential to provide a clear legal basis for our entitlements reasonably expected to arise from the fundamental right to privacy, defining what is permissible and what is not, clarifying the scope of our fundamental right to privacy, and describing what data fiduciaries who collect our personal data can and cannot do with it. A 'fundamental' right to privacy does not particularly outline entitlements that necessarily accrue until it is decided. In the absence of a data protection statute, courts have adopted differing opinions on the scope of fundamental aspects of privacy, such as the right to be forgotten. Since there is no data protection legislation in place, it is

[43] A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 2018.
[44] *Ibid.*

hard to tell what rights we have, rendering the fundamental right practically useless.

The kind and volume of personal data that is gathered, stored, processed, retained, and disposed of in India means that the act is anticipated to have an effect on most organisational areas, including legal, IT, human resources, sales and marketing, procurement, finance, and information security. Therefore, in light of the DPDP Act, 2023, organisations in these and allied areas need to create a robust programme for implementing data privacy and protection.

Undoubtedly, in India's digital society, privacy is a developing and increasingly becoming a crucial topic. As companies collect more data from and about online users, and as the government seeks greater access and surveillance capabilities, it is critical that India prioritizes privacy and implements strong safeguards to protect the privacy of both Indians and foreigners whose data resides in India temporarily or permanently. The passage of comprehensive privacy legislation that recognizes privacy as a basic right is the first step in this direction. The Group of Experts on Privacy Report and the government's consideration of a proposed privacy bill are all positive moves.