
DIGITAL AUTONOMY AND STATE SURVEILLANCE: A RIGHTS-BASED EVALUATION

Roshni. S & Sri Yalini. V, Advocates

ABSTRACT

The rapid growth of digital governance has amplified the tension between fundamental rights and state surveillance. Often, these rights, such as freedom of speech and expression, privacy, and the right to memory, are put to the test by the state's interest in security, governance, and administration. The paper critically analyses how the Indian legal system strikes a balance between liberty and state surveillance with the help of principles laid down in the landmark cases like *PUCL v. Union of India (1997)*, *Anuradha Bhasin v. Union of India (2020)*, and *Justice K.S. Puttaswamy v. Union of India (2017)*, and the constitutional framework laid down in Articles 19 and 21 of the Constitution of India. With a focus on the exceptions that allow for extensive state access to personal data, it evaluates the functioning of statutory mechanisms under the Digital Personal Data Protection Act, 2023, and the Information Technology Act, 2000. These statutes not only aid in processing the personal data of data subjects but also sanction punishments for persons violating their provisions. The emerging "right to be forgotten" in Indian jurisprudence and its interaction with other realms of rights like the right to freedom, privacy, and the right to live with dignity are examined by a comparative analysis between India, the European Union, and the United States. This helps to understand the global trends in protecting digital rights while upholding legitimate state interests. The doctrinal research also advocates for a rights-based approach for e-governance by utilising the principles of proportionality, transparency, and accountability. It concludes that, in the digital era, protecting privacy and digital memory is not a threat to national security, but rather essential for preserving human dignity, promoting public participation, and fostering confidence in governmental institutions.

Keywords: Privacy, Freedom, Surveillance, Digital Memory, Right to be Forgotten, Data Protection.

INTRODUCTION

“The Constitution does not permit the State to make an individual a subject of unregulated surveillance”

- Justice D.Y. Chandrachud

In the contemporary digital age, technology is rapidly becoming the medium for the interaction between the State and the individual. The State uses digital technologies for governance, security, welfare delivery, and law enforcement. Simultaneously, the same technologies allow for state surveillance on an unprecedented scale: data collection, monitoring of communications, and algorithmic analysis of digital behaviour. This changing landscape raises a fundamental constitutional question: how to preserve digital autonomy in the face of expanding powers of surveillance¹.

The constitutional provisions for safeguarding these rights under Articles 19 and 21 of the Indian Constitution form the basis for upholding the freedoms regarding speech and expression, privacy, personal liberty and life with dignity. Judicial decisions have continuously widened these provisions to react to challenges arising out of technology. Landmark decisions such as *Justice K.S. Puttaswamy v. Union of India*², and *Anuradha Bhasin v. Union of India*³ have held that any government action for surveillance, interception, and curbs on the internet must be justified from the aspect of reasonability and necessity under the constitutional framework. These judgments emphasise that national security and public order cannot be invoked as excuses to override fundamental rights. Statutes like *the Information Technology Act, 2000* and the *Digital Personal Data Protection Act, 2023* emerged creating a paradigm shift in the governance of personal data and digital surveillance. These regulations are to make provisions regarding the protection of personal data and regulation of data fiduciaries, but, in contrary, they have granted a huge exemption to the government and its agencies in the interests of sovereignty, security, and public order, raising concerns of executive overreach⁴.

One of the new and most controversial developments within digital rights jurisprudence is that

¹ U.N. Human Rights Council, ‘*The Right to Privacy in the Digital Age*’, U.N. Doc. A/HRC/27/37 (June 30, 2014).

² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

³ Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

⁴ Digital Personal Data Protection Act, No. 22 of 2023.

of the "right to be forgotten" through which individuals have claimed the right to be free from perpetual digital memory that might affect dignity, reputation, and autonomy. The comparative study that is borrowed from both the European Union and the USA offers a crucial understanding to jurisdictions such as India with diverse constitutional backgrounds on managing tensions within digital rights such as privacy, memory, and public interest⁵. The study undertakes a rights-based evaluation of State surveillance and digital governance in India. It delves into constitutional jurisprudence, legislative systems, and international comparative practices to determine whether existing provisions are sufficient in supporting individual liberty as well as accommodating national interests. It proposes that in supporting concepts such as proportionality, transparency, and accountability, ensuring digital privacy and memory is in no way conflictive with national issues but is, in fact, imperative in ensuring that democracy is maintained.

The research paper is doctrinal and descriptive in nature. It is written with the help of existing statutes, central and state regulations, scholarly articles written by eminent jurists, international conventions and landmark case laws pronounced by the Supreme Court and various High Courts in India. It evaluates the conflict between state governance and digital autonomy, and suggests a rights-based approach to resolve the same. This study consists of three Chapters. The First Chapter introduces the topic of Right to Freedom in digital environment and all the supplementary rights curtailed in this concept; the Second Chapter includes the Right of Privacy and Memory in handling personal data and the Final Chapter provides a Comparative Analysis of the Indian Data Laws with other country Data Regulations like the USA and European Union.

CHAPTER I: RIGHT TO FREEDOM IN DIGITAL ERA

The Right to Freedom is generally associated with speech, expression, movement, association, and occupation under Article 19 of the Constitution⁶ and has undergone a profound transformation in the digital age. As digital technologies increasingly mediate communication, commerce, governance, and social interaction, constitutional freedoms are now extended to virtual and online spaces, demanding renewed legal and normative interpretation.

⁵ Regulation (EU) 2016/679, *General Data Protection Regulation*, art. 17, 2016 O.J. (L 119) 1.

⁶ INDIA CONST. art. 19.

1.1 Right to Freedom of Speech and Expression

The above right is guaranteed under Article 19(1)(a) of the Indian Constitution that allows an individual to share his views, opinions, thoughts, creativity and ideas freely to the common public⁷. Since, India follows democratic form of government, freedom of speech and expression in the country is professed widely but subject to certain restrictions under Article 19(2). These restrictions are intended to safeguard the society and nation. For instance, speech or views that compromises public order, national security, or other people's reputations may be prohibited⁸. Additionally, the government has the authority to act against hate speech, defamation, and violent content. But these limitations ought to be acceptable, not oppressive. Judicial scrutiny plays a crucial role in determining whether such restrictions are proportionate and constitutionally permissible⁹.

In the digital context, people in India can speak, write, publish, and express opinions in any form — including newspapers, TV, social media, and other online platforms. This right also includes the freedom to receive and share information with others. It helps people participate in public debates, question the government, and discuss social issues freely¹⁰. However, the dispute arises when certain restrictions are placed by the government in order to preserve the national security and sovereignty.

1.1.1 Social Media Platforms

In India, social media has grown to be a significant communication channel. People share ideas, news, and opinions using apps like YouTube, Facebook, Instagram, and X (Twitter). The government places certain norms to regulate free speech and expression to ensure safety and fairness because millions of people use them on a daily basis. These platforms must be regulated. But, proper regulations are not given nor are the reasonable restrictions on the content, clearly defined. This shows the users of these platforms in a bad light which transforms into fake news or hate speech. On social media, hate speech and false information are major issues. Fabricated stories, and inaccurate information can confuse or frighten people. Posts targeting individuals based on their gender, caste, religion, or other identities are considered

⁷ INDIA CONST. art. 19, cl. 1(a).

⁸ INDIA CONST. art. 19, cl. 2.

⁹ Dr. Suja Nayar, 'Digital Era and Human Rights in India: An Analysis of Privacy, Surveillance, And Freedom of Expression', 11 (9) INTERNATIONAL EDUCATION AND RESEARCH JOURNAL (Sept, 2025).

¹⁰ *Id.*

hate speech. These kinds of content have the potential to shatter society, incite violence, and propagate rapidly over the internet¹¹. Thus, there is a need to regulate them to make sure they are safe and fair. Both the government and these platforms have obligations to safeguard users while upholding their right to free speech and expression.

1.1.2 The Test of Reasonableness

In addition to its beneficial applications, social media can be used for an array of digital crimes, including racial insults, defamation, invasion of privacy, and instigating criminal action. India does not support an unconditional right to free speech and expression. The Constitution permits 'reasonable restrictions' on the use of this right when they promote public order, security, sovereignty, morality, or decency¹². For example, Social media intermediaries such as Facebook, Instagram, TikTok, and X may remove information that is in violation of the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*¹³ when such information shared is against the sovereignty and integrity of India; affects friendly relation with foreign states, disrupts public order or morality. However, such practices and rules were amended after the landmark judgement in the case of *Shreya Singhal v. Union of India*¹⁴. The Court held *Section 66A of the Information Technology Act* as invalid and unconstitutional because terms like "grossly offensive," "menacing," "annoyance," and "inconvenience" were undefined, subjective, and overly broad. This vagueness gave excessive discretionary power to authorities and failed to distinguish between innocent speech, discussion, advocacy, and incitement. Thus, it was stated that these terms did not fall under the purview of 'reasonable restrictions' in Article 19(2). The Court also acknowledged that the vague and arbitrary nature of these provisions created a "chilling effect" on free speech, preventing people from legitimately expressing themselves digitally for fear of prosecution¹⁵. Thus, the test of reasonableness should be transparent, accountable and non-arbitrary.

¹¹ Dr. Suja Nayar, 'Digital Era and Human Rights in India: An Analysis of Privacy, Surveillance, And Freedom of Expression', supra note 9.

¹² MdNurul Momen, 'Threats to Free Expression in the Digital Age', RESEARCH GATE (July 2020).

¹³ Taniya, 'Freedom of Free Speech and Expressions in Digital Era', 6 (6) INDIAN JOURNAL OF LAW AND LEGAL RESEARCH, p. 4579-4589.

¹⁴ *Shreya Singhal v. Union of India*, (2013) 12 SCC 73

¹⁵ Aishwarya Agrawal, 'Shreya Singhal v. Union of India', LAW BHOOMI (April, 2025),

[https://lawbhoomi.com/shreya-singhal-v-union-of-india/#:~:text=Vagueness%20and%20Arbitrary%20Application:%20The,under%20Article%2019\(2\).](https://lawbhoomi.com/shreya-singhal-v-union-of-india/#:~:text=Vagueness%20and%20Arbitrary%20Application:%20The,under%20Article%2019(2).) (Last visited 11th Jan, 2026)

1.1.3 Internet Shutdowns

Internet shutdown refers to the temporary suspension of internet access in a certain region. They are frequently implemented in India during protests, or circumstances when the government is concerned about social media abuse or violence. Shutting down the internet has numerous adverse effects on people's everyday lives and fundamental rights, even when its primary objective is to uphold law and order. One of the countries with the greatest rates of internet outages worldwide is India. It has experienced more shutdowns than most other nations for a long time. In 2019, there was a shutdown in Jammu and Kashmir following the revocation of Article 370. In a similar vein, Iran blocked the internet in November 2019 during demonstrations against increases in fuel prices, hindering communication and recording abuses of human rights. In Ethiopia, shutdowns were implemented in response to the 2020 murder of a well-known singer in an effort to reduce violence and false information. These shutdowns are an example of how the Governments hinder movement to effect change and limit public voice through internet shutdowns¹⁶.

The economy is significantly impacted by shutdowns as well. Responding to these kinds of situations become slower and more challenging without the internet, jeopardizing lives. So, the Supreme Court of India, in the famous case of *Anuradha Bhasin v. Union of India*¹⁷ ruled that the freedom of speech and expression guaranteed by Article 19(1)(a) includes the right to utilise the internet too. It was held that such shutdowns can be temporary, proportional, and adequate. This decision reinstated the importance of fundamental rights and assessed the limitations of government's interference in restricting those rights.

1.2 Right to Freedom of Assembly and Association

The aforementioned rights are protected in India by Articles 19(1)(b) and 19(1)(c), respectively, and it encompasses virtual protests, groups, and movements under it. Online communities, digital movements, and virtual protests are the modern ways to form a collective association. Messaging platforms, forums, and social networks act as a medium to facilitate political mobilisation and civic engagement, thereby extending constitutional protection to digital assemblies. However, these rights face high risks from state surveillance, internet

¹⁶ Article 370: *India Supreme Court upholds repeal of Kashmir's special status*, (December, 2023), <https://www.bbc.com/news/world-asia-india-67634689> (Last visited 15th Jan, 2026)

¹⁷ *Anuradha Bhasin v. Union of India*, supra note 3.

shutdowns, and restrictive regulations such as the Information Technology Act, 2005 and IT Rules, 2021, sparking debates about balancing security with fundamental digital rights as courts uphold online expression while the government imposes restrictions¹⁸.

Digital media has made it possible for protesters to organize and communicate worldwide, and this has consequently led to a revolutionary approach in freedom of assembly. *Black Lives Matter* and *Arab Spring* movements are examples of how Facebook, Instagram, and Twitter are utilised as social networking sites that can help organise mass movements, create awareness, and enable protest participants to create recordings of injustices and share with a broader audience without going through the traditional media approach. These sites allow for boundary-less geography and enable diverse and inclusive environments for collaborations and expressions¹⁹. Nevertheless, social media sites commonly use algorithms with a tendency towards interesting and shocking information, which can add to animosity, hate speech, and misinformation with a disregard for other perspectives, opinions, and notions, possibly adding towards prejudice and censorship, and possibly bringing a shutdown for social movements. Therefore, better regulations and accountability are required for protecting digital rights and appropriately dealing with sensitive information as a part of national values and interests²⁰.

1.3 The Right to Freedom of Occupation, Trade and Commerce

Under Indian Constitution, Article 19(1)(g) grants all citizens of the country the right to practice any profession or to engage in any occupation, trade, or business. But this privilege is subject to certain limitations as outlined in Article 19(6). It does not include the right to engage in any illegal business, trade, occupation, or profession, or to hold a certain job or occupy a specific position of one's choice. The Government is empowered to impose such limitations that may affect the interest of the public²¹.

The expansion of the digital economy has produced new job and entrepreneurship opportunities, such as in e-commerce, software development, and the gig economy (freelancing). The rapid progress of digital technologies and infrastructure provide higher

¹⁸ R. Lalthasangzeli and Dr. Shobha Yadav, 'Challenges to Freedom of Press, Assembly, and Association in the Digital Age: A Comparative Study of Jurisdictions', 3 (1) THE ACADEMIC: INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH (JANUARY, 2025), p. 436-450.

¹⁹ Ben Scott, 'A Contemporary History of Digital Journalism', 6 (89) TELEVISION & NEW MEDIA (2005).

²⁰ Hans-W. Micklitz et al., 'Constitutional Challenges in the Algorithmic Society' (2021).

²¹ INDIA CONST. art. 19.

productivity, process automation, and better resource use, all of which contribute to economic growth. But, this steep growth also frequently outpaces regulatory frameworks, resulting in data breaches, misinformation and false news²².

Article 301 of the Constitution further ensures that trade and commerce would be freely conducted throughout India's territory to achieve national economic unity, but this is also subject to limitations imposed by the Government²³. As discussed above, 'reasonable restrictions' are placed by the State to curb information that are against the national security and safety. The enactment of India's *Digital Personal Data Protection Act, 2023* gives wide powers to the government in determining data transfer permissions. The Act allows cross-border data transfers, using a "blacklist" approach in which transfers are permitted to all countries unless the Indian government limits them to a particular "negative list," requiring Data Fiduciaries to store the backup of the data in India and follow the law's consent/processing rules even for overseas transfers, with the possibility of stricter rules on sensitive records and industry-specific localisation obligations²⁴. This due process raises concern about legal overreach, lack of transparency, and potential conflicts with international data transfer norms. It must be legal, necessary, temporary and proportionate. Therefore, it is vital for a robust and secure digital regulatory framework that serves the public interest and ensures national digital sovereignty.

1.4 The Chilling Effect in Digital Medium

When people restrict their speech, expression, or online behaviour out of fear of state surveillance, legal consequences, platform charges, or social protests, even when their actions are legal and protected by the Constitution, is known as the "chilling effect" in the digital medium. It includes:

- i. Fear of being banned or removed which discourages the users from voicing their ideas on social media.
- ii. Fear of legal action or monitoring due to which reporters and campaigners avoid

²² Rana Sourav Kumar, et. al., 'Data Localisation and its Impact on Cross-Border Digital Trade in India: Legal, Economic and Strategic Implications', 30(3) EDUCATIONAL ADMINISTRATION: THEORY AND PRACTICE (2024), p. 3326 -3333.

²³ INDIA CONST. art. 301.

²⁴ The Digital Personal Data Protection Act, supra note 4.

releasing their content online

- iii. Fear of their information/data/opinions being looked up, distributed, or interacted with online political content.

In India, the laws and regulations does not protect people against the illegal or excessive surveillance, allowing for the deployment of such monitoring without oversight or accountability. Data Surveillance technology for state surveillance (like Pegasus), vague regulations (IT Rules 2021), and misinformation are already being used to target journalists, activists, and human rights defenders in India, creating a climate of suppressed free speech and critical discourse, impacting journalism and dissent²⁵.

Data interception may be necessary for India's sovereignty and integrity, security, good relations with foreign states, maintaining public order, and preventing incitement to commit crimes. However, such activities must be authorised by the Central or State Government or an authorised authority on their behalf. During this process, there is lack of transparency which leads to arbitrary interpretation during surveillance. The government has the sole authority over monitoring activities, with no judicial or parliamentary scrutiny²⁶. In addition, the *IT Rules of 2021*, intended to increase accountability, are criticised as overly broad, granting wide powers to government entities and demand private information, leading to self-censorship among online platforms and its users. Even as Section 79 of the IT Act gives a safeguard, the requirement of “due diligence” in the *IT Rules, 2023* pressurizes these online intermediaries to overly restrict content to escape being held liable. In a case involving **Kunal Kamra v. Union of India**²⁷, a plea against the notification of IT Rules, 2023 in the Bombay High Court alleged that it caused a “chilling effect” on free speech as it discouraged expression out of fear of a retort by government agencies through a newly formed Fact Check Unit (FCU), which would deem the content to be untrue. Although the IT amendment standards may align with legitimate goals and proportionality *stricto sensu*, there is still a need for clarification on the suitability and necessity of such standards. This judgment highlights the importance of judicial review in

²⁵ *Growth of Digital Restrictions in India: Spotlight on Surveillance and Other Threats to Free Expression*, INTERNATIONAL CENTER FOR NON-PROFIT LAW (November, 2022), <https://www.icnl.org/wp-content/uploads/ICNL-Digital-Rights-Update-India-FINAL-12.2022.pdf> (Last visited 12th Jan, 2026).

²⁶ Chaitanya Ramachandran, “*PUCL v. Union of India Revisited: Why India’s Surveillance Law Must Be Revised for the Digital Age*”, 7(2) NUJS LAW REVIEW (2014), <http://nujslawreview.org/2016/12/04/pucl-v-union-of-india-revisited-why-indiassurveillance-law-must-be-revised-for-the-digital-age/> (Last visited 12th Jan, 2026).

²⁷ *Kunal Kamra v. Union of India*, 2024 BHC 1575

restraining arbitrary government intervention in data regulation on online platforms. The split verdict given out in this case has been explained on the interpretation of the ways in which an ambiguous law represses genuine ideas and criticisms, including an extension to the scope of the chilling effect from mere legal intimidation to social pressures, in the context of the online age. A law that protects the misuse of data and information technology should be created in India and other nations. This includes protecting civic freedoms for civil society and vulnerable communities²⁸.

CHAPTER 2: RIGHT TO PRIVACY, MEMORY, AND PERSONAL DATA

India is a developing country with a growing economy that is moving towards digitalisation.

Article 21 of the Constitution states, *'No person shall be deprived of his life or personal liberty except according to procedure established by law.'*²⁹ The rights under this Article include the right to life and personal liberty available to all - citizens and non-citizens. The scope of Article 21 in 1950, when the Constitution was established, was significantly smaller compared to the present time due to the interference of the judiciary. One such right that is brought to the spotlight in this chapter is the Right to Privacy and related rights.

2.1 Evolution of The Right to Privacy

Privacy can be stated as the absence of intrusion into one's personal space, or the right to be let alone. Before the introduction of the Right to Privacy under Article 21, Justice Ayyangar in ***Maneka Gandhi v Union of India***³⁰ held that *'right to privacy is not a guaranteed right under our constitution and therefore the attempt to ascertain the movement of an individual, which is merely a manner in which privacy is invaded, is not an infringement of a fundamental right guaranteed by Part III'*. Later, this stance was changed that the right to privacy is the right to be let alone³¹.

This right was further justified in the telephone tapping case, ***People's Union of Civil Liberties v. Union of India***,³² which struck down a provision under the Indian Telegraphs Act, 1995

²⁸ Ayush Kumar, 'Kunal Kamra v. Union of India: on Deciding whose Perspective to Push?', A BLOG ON SOCIETY FOR CONSTITUTIONAL LAW DISCUSSION, CHANAKYA LAW UNIVERSITY (2024), <https://www.tsclcd.com/kunal-kamra-case-analysis> (Last visited 15th Jan, 2026).

²⁹INDIA CONST, Art. 21.

³⁰Maneka Gandhi v Union of India AIR 1978 SC 597

³¹R.Rajagopal v. State of Tamil Nadu AIR 1995 SC 264

³²People's Union of Civil Liberties v. Union of India, AIR 1997 SC 568

through which the state could intrude or intercept calls for public emergencies and surveillance. The Court held that the "right to privacy" comprises the ability to have private phone conversations and that any tapping of a phone, unless done in accordance with a legal procedure, is a violation of Article 21. The Court further observed that current laws do not recognize a general right to privacy when reviewing the Second Press Commission report, which characterized phone tapping as a serious invasion of privacy and behind times under the Indian Telegraph Act, 1885. The report suggested restricting phone tapping to situations such as criminal investigations and national security³³.

Section 5(2) of the Telegraphs Act, which sets requirements for interception orders and requires a public emergency or public safety interest as prerequisites, were examined by the Court. India's sovereignty and integrity, state security, friendly foreign relations, public order, and preventing incitement to crime were the grounds on which the designated government officer must deem it necessary. The Court upheld the constitutionality of Section 5(2), but to prevent arbitrary actions and protect the right to privacy, it decided to set temporary guidelines in place. In this case, digital autonomy and the right to privacy were not granted as an absolute right but only with certain guidelines.

In *Ram Jethamalani v. Union of India*³⁴, it was stated that the Right to privacy also requires the state not to make public any personal information about an individual, which would violate his/her privacy. The right to privacy is the cornerstone of digital rights available to individuals worldwide. The personal data that we lodge into cyberspace is under the control of the state, and the state is liable for any loss of data or data leak. As the state takes measures to store, analyse, and process data, there is monopoly of power on the side of the state.

2.2 Right to Privacy as a Fundamental Right

The introduction of the Identity card called Aadhaar in 2011 by the Unique Identification Authority of India (UIDAI) helped establish and legitimise the concept of Right to Privacy. In 2015, Puttasamy, a former judge filed a case in the Supreme Court questioning the validity of the Aadhaar Act. In the said case, *K. S. Puttasamy v. Union of India*³⁵, the Aadhaar Act was contested due to its implementation of a standardised biometric identification card. The main

³³ Chaitanya Ramachandran, "PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Revised for the Digital Age", supra note 26.

³⁴ Ram Jethamalani v. Union of India, (2011) 8 SCC 137

³⁵ K S Puttasamy v. Union of India, supra note 2.

argument was that it was intended to be a compulsory ID card for everyone, and that only individuals with this card could access certain governmental benefits. The card was made compulsory for all the legal residents and is not proof of citizenship. However, the Aadhaar Act was upheld as constitutionally valid by the court as it satisfied the three-fold test- Legality, Need and Proportionality.³⁶ The Act was considered legal as it was passed by a competent authority i.e. the Parliament. There was a need for the said Identity card as it was meant to be used as a unique card and the Act complied with the principle of proportionality by being appropriately tailored to achieve the objective for which it was laid down.³⁷ The Aadhaar card is used by private entities for verification in the present day, without the consent, which clearly is an invasion of privacy. This demonstrates a social intrusion of the state into the personal data of individuals. The Government has also made it mandatory to link bank accounts and PAN cards to the Aadhaar card, leaving people with no choice but to apply for the card. This clearly shows a violation of the right to live with personal autonomy as well as the right to live a dignified life. The power imbalance between the state and citizens in this democratic country is portrayed in this case.

In 2021, a new form of attack was casted upon famous personalities in India. **Pegasus** was an Israeli spyware used to get access to information and was meant to be used to stop terrorism and crime. It was said that the spyware was used by 'state-sponsored attackers' and targeted social activists, leaders of opposition, as well as journalists. Pegasus is a powerful malware used for cyber espionage, allowing operators to read messages, emails, and retrieve all data without the owner's knowledge. It used a 'zero-link technology' in which the device would get corrupted without clicking on links. This has widely raised serious concerns about privacy and abuse of power. The owner, NSO Groups, stated that it sold Pegasus only to Governments and Security Agencies.³⁸ The attack triggered a public backlash because the state had taken and leaked personal sensitive data of some high-profile personalities including Rahul Gandhi, Siddaramaiah and many others.³⁹ The state is said to have played a major role in the spread of

³⁶*Aadhar Authentication By Private Entities From Data Privacy Perspective*; <https://ssrana.in/articles/aadhaar-authentication-by-private-entities-from-data-privacy-perspective/> (last visited 28 Dec,2025)

³⁷*Constitutionality Of Aadhaar Act*, <https://www.scobserver.in/cases/puttaswamy-v-union-of-india-constitutionality-of-aadhaar-act-case-background/> (last visited 02 Jan,2026)

³⁸*India targeted high-profile journalists with pegasus spyware* <https://www.aljazeera.com/news/2023/12/28/india-targeted-high-profile-journalists-with-pegasus-spyware-amnesty> (last visited 04 Jan,2026)

³⁹*Rahul Gandhi: Pegasus A Tool To Silence People*; <https://timesofindia.indiatimes.com/india/rahul-gandhi-pegasus-a-tool-to-silence-people/articleshow/85065103.cmsl> (last visited 04 Jan,2026)

Pegasus, as they could get access to the personal data of A-listers.

2.3 The Emergence of Right to Memory

The Right to privacy also includes the right to memory, also known as the ‘right to be forgotten’ (RTBF). This right falls under the right to live with dignity and with personal liberty. Data subjects are the owners of their personal, sensitive information, and they must have rights on the storage and deletion of the said data.

The existence of the RTBF was brought into question in the case of *Dharamraj Bhanushankar Dave vs. State of Gujarat*⁴⁰. The petitioner, who was acquitted of the offense, prayed that the court should restrain the respondents from disclosing the matter, as it would harm him. The Gujarat High Court accepted the new RTBF but said it was not absolute. In the matter of *Jorawar Singh Mundy vs. Union of India*⁴¹, the Delhi High Court acknowledged the right to be forgotten and also recognized the right of the person to request the de-indexing of judgments from public sites⁴². From the above matters, it could be ascertained that right to memory also includes the right to move on from reputational harm.

Moreover, the Supreme Court of India upheld that the right to be forgotten is included in Article 21, in the significant case of *K.S. Puttaswamy v. Union of India*⁴³, which had also established the right to privacy. Additionally, the right is non-absolute, and the data cannot be utilised for fulfilling any legal obligation, enforcing legal assertions, exercising the right to freedom of speech and expression, fulfilling a duty in the public interest or in terms of health, or for statistical, historical, and scientific use.⁴⁴ In *Vysakh K.G. v Union of India*⁴⁵, the Kerala High Court stated that the right to be forgotten cannot prevail over the principles of open justice and larger public interest, and declined to overstep judicial boundaries and infringe on the powers of the legislature.

From the above case laws, it can be ascertained that the court has not been rigid with the

⁴⁰Dharamraj Bhanushankar Dave vs. State of Gujarat; SCA No. 1854 of 2015

⁴¹Zorawar Singh Mundy Vs. Union of India and Ors ; W.P.(C) 3918 of 2021

⁴²*The Right To Be Forgotten: Path Towards Efficacious Realization Of Data Protection*, <https://nualslawjournal.com/2023/08/29/the-right-to-be-forgotten-path-towards-efficacious-realization-of-data-protection/> (last visited 04 Jan,2026)

⁴³K S Puttaswamy v. Union of India , supra note 2.

⁴⁴*Right To Be Forgotten And Digital Memory: Preserving The Past While Protecting Privacy*, <https://blog.primelegal.in/right-to-be-forgotten-and-digital-memory-preserving-the-past-while-protecting-privacy/> (last visited 06 Jan,2026)

⁴⁵Vysakh K.G. v Union of India,2022 SCC OnLine Ker 7337

implementation of the right to memory, even if the data subjects are the owners of the data. The Government or the judiciary has a final say on the erasure or retention of data. The right to let alone can never be stated as an absolute right. However, RTBF must have greater precedence over the state's access to personal data as well as the economic interests of the third-party sites.⁴⁶ The precedence or ownership of data by the state can be clearly seen as a power move. This is the reason why people are hesitant to be involved with the government, their institutions, e-governance sites, and are still not registered with the UIDAI. So, there must be proper implementation, and the arbitrariness in executing the said laws must be removed to boost confidence in the Government among the people to protect their data.

CHAPTER 3: COMPARATIVE ANALYSIS ON THE LEGAL FRAMEWORK

3.1 Indian Legal Framework Governing the Right to Privacy and Memory

The *Puttaswamy* judgment laid down the right to privacy and memory in the Indian legal system under Article 21 of the Constitution, making it a fundamental right. India lacks clear and complete laws on data privacy. The law that governs electronic media and sensitive data is the *Information Technology Act of 2000*. As per this Act, no personal/sensitive data may be collected for any purpose unless an entity authorized by law has authorized to collect data for a specific reason provided in writing. The collection of personal sensitive information requires informing the individual whose data will be collected about its collection, including what the information is, its purpose, and to whom the information will be given for processing and storage⁴⁷.

According to *Section 43A of the IT Act*, organisations that hold sensitive personal data and do not maintain proper security to protect this data may have to pay damages if someone suffers a wrongful loss or gain. Eventhough there exists a law, it cannot be ascertained from where and by whom the data has been leaked. RTBF is not directly included in the IT Rules, 2021.⁴⁸ However, it does outline steps for filing complaints with a Grievance Officer to remove content that reveals personal information about the complainant from the internet without the

⁴⁶*Balancing Privacy And Public Interest: The Evolving Jurisprudence Of The Right To Be Forgotten In India*, <https://chambers.com/legal-trends/the-right-to-be-forgotten-in-indian-law>(last visited 08 Jan,2026)

⁴⁷*Laws Regarding Right To Privacy Of Personal Data In India*, <https://ijirl.com/wp-content/uploads/2023/08/LAWS-REGARDING-RIGHT-TO-PRIVACY-OF-PERSONAL-DATA-IN-INDIA.pdf>, (last visited 10 Jan,2026)

⁴⁸The Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules, 2021, *supra* note 13.

complainant's consent.

The privacy right has been enormously compromised because of the State's ability to infringe on an individual's private domain by virtue of Section 69 of the Act. The intrusion into the private sphere of one's personal life by the state authorities to listen, review, and decrypt private messages (i.e., email, Instant Messenger, etc.) for a wide variety of reasons, like national security, public order' provides access to a person's activities. The ability of authorities to conduct surveillance without prior judicial review and accountability provides disproportionate amounts of power to the executive while leaving individuals unaware that their privacy has been violated.

The government, through the *Srikrishna Committee* in 2017 set up data protection standards which paved the way for the *Personal Data Protection Bill, 2019* and later the *Digital Personal Data Protection (DPDP) Act, 2023*. This was passed for the sole reason of processing personal data in India. The law states that personal data is allowed to be handled only with the express and unambiguous consent of the relevant person unless there are other legitimate reasons for processing their data. Such consent must include all five elements that make it valid; these elements are “free, specific, informed, unconditional, and unambiguous”⁴⁹

Once a purpose has been fulfilled or if someone has withdrawn their authorization to access/use their information, all data must be deleted to avoid keeping it for an indefinite time frame. The Data Processor will be required to promptly cease using the data and destroy all records of that data as soon as possible. This helps prevent unauthorised access/overaccumulation of data beyond what is needed. As outlined in the Act, there are certain exemptions for the Government in terms of keeping data due to issues concerning National Security and Public Order. However, the exemptions do raise concerns over the degree of surveillance being generated on individuals, and over continued retention of individuals' data by public authorities beyond what is necessary.

It should be noted that the Act alters the meaning of Digital Memory, whereby it will be viewed as information held in trust by the individual for their individual data rather than as property owned by either the Government or a Private Entity. All this sounds good on paper and as per

⁴⁹*Right To Privacy And Data Protection Act: An Analytical Study*, <https://ijirl.com/wp-content/uploads/2025/01/RIGHT-TO-PRIVACY-AND-DATA-PROTECTION-ACT-AN-ANALYTICAL-STUDY.pdf>(last visited 13 Jan,2026)

the law, but in actual practice, it doesn't function as the law states. The data that we give to the government is used by third parties. For example, FASTag, operated by NHAI, is compulsory for vehicles, but nowadays, even shopping malls use it to deduct their parking fees. WhatsApp is an application that is end-to-end encrypted in India. Although this is the case, as per section 69 of the IT Act, the Government can get hold of our encrypted files as well. This is just one of numerous instances that underscore the reality that absolute privacy is more aspirational than achievable. There have been talks that the personal data of people is sold on the dark web for money. This blatantly shows the negligence and carelessness with which the state handles the personal data of citizens.

3.2 International Framework on the Protection of Personal Data

The right to privacy is recognized under the *Universal Declaration of Human Rights (UDHR)*, *International Covenant on Civil and Political Rights (ICCPR)*, *Health Insurance Portability and Accountability Act (HIPAA)*, *General Data Protection Regulation (GDPR)*.

Although the right to privacy is not expressly stated in the UDHR, it is Article 12, which reads: "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation."⁵⁰ The ICCPR, and the UNCRC adopted the same language.⁵¹ The right of the data subject to request the de-referencing of their old personal data was established in 2014 in the significant judgment of *Google Spain in the CJEU landmark case*⁵², which was incorporated in India. Consequently, RTBF has been said to be included in the title of Article 17, GDPR⁵³, while it is not defined or regulated in the provision.⁵⁴ The GDPR, when read alongside *Articles 7, 8 and 52 of the Charter of Fundamental Rights of the EU*, allows for interference with the privacy of individuals; however, that interference can only be allowed when it is strictly necessary and proportionate to the legitimate purpose. As per the GDPR, data must be collected and stored only for a specific amount of time for a particular purpose. Once the purpose for which it was secured is fulfilled, the data subject can request the removal of the personal data. But the right

⁵⁰Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/810 (Dec. 10, 1948),

⁵¹Universal Declaration of Human Rights art. 12, G.A. Res. 217 A (III), U.N. Doc. A/810 (Dec. 10, 1948).

⁵² Google Spain SL v Agencia Española de Protección de Datos (2014) 3 WLR 659

⁵³General Data Protection Regulation GDPR, <https://gdpr-info.eu/>

⁵⁴*The Right To Be Forgotten In Data Protection Law And Two Western Cultures Of Privacy*, <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/right-to-be-forgotten-in-data-protection-law-and-two-western-cultures-of-privacy/31D2EDDE753A64F40FAFBF4B76CEA89C>, (last visited 20 Jan,2026)

of the data subject in this regard is qualified and not absolute.

Under the US laws, there is no general right to be forgotten recognised at the federal level, and privacy is governed through a sector-specific approach. Laws such as HIPAA, COPPA, provide limited safeguards in specific contexts, but they do not offer individuals a general right to erase personal data. Surveillance and access to data by the State are largely regulated through national security legislation, including the *Foreign Intelligence Surveillance Act* and the *USA PATRIOT Act*. The State of New York became the first to introduce a draft '*Right to Protection Bill*' in its State Assembly, which was titled "*An act to amend the civil Rights law and the civil practice law and rules, in relation to creating the 'Right to be forgotten' act*"⁵⁵

Data protection regimes throughout the world provide specific approaches to handling personal data through the use of techniques such as encryption, pseudonymisation, , data masking, and anonymisation. Under the DPDP Act, the emphasis has been placed on minimisation of data, limitation of purposes, and protection by appropriate security safeguards, while also treating data masked, pseudonymised, or encrypted even if anonymised. All three of these methods help reduce the possible misuse, profiling, and surveillance risks to the individual

While the GDPR emphasizes privacy as the primary basis for State interference with its citizens, U.S. law is built on a balance between the right to privacy and national security, primarily through secret governance. Nevertheless, Indian laws continue to maintain broad executive surveillance powers, which have highlighted the necessity for strong legal and judicial protections for privacy rights under the Constitution, although, there needs to be a balance between people's rights and state surveillance. In order to prevent the arbitrary application of laws, the State must create specific statutory provisions to protect rights of people; provide limits on how personal data will be used; create independent review mechanisms for requests; and establish limits for erasure/retention of data under the Right to Be Forgotten. Moreover, there needs to be proper implementation of the laws, and a rights-based approach must be warranted.

CONCLUSION

While there are many new legal and technological safeguards for protecting the freedom and

⁵⁵*Right To Be Forgotten*, <https://articles.manupatra.com/article-details/Right-to-be-forgotten> (last visited Jan 21, 2026)

privacy of individuals' personal data, the effectiveness relies upon how well they are executed and implemented in practice. This gap between what is recognised by law and what is actually enforced, is especially large in the area of the State's access to personal data in India. Without adequate safeguards, such as reasonable restrictions placed under the Constitution, the ability for individuals to access or delete their data, the power of the Government will diminish the ability of an individual to control their own life and reduce their dignity to bureaucratic procedures. Therefore, it is important to strike a balance between excessive freedom that leads to online abuse, data breaches, misinformation, and oppressive regimes that doesn't allow an individual to freely express his / her own views, opinions and ideas on digital platforms. A constitutional democracy must ensure that any access to an individual's data by a state is both necessary and proportionate to the individual's circumstances, and that any liability of the state for accessing or holding the data of an individual is addressed, so that the rights associated with freedom, privacy and memory remain as enforceable rights rather than merely being a part of the Constitution.