Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Privacy in the Digital Age: A Legal Study

Elly Lalrinsangi[a] Adv. (Dr.) Vidya Selvamony[b]

[a]CMR University School of Legal Studies, Bengaluru, India [a]Faculty, CMR University School of Legal Studies, Bengaluru, India

Received 30 April 2025; *Accepted* 30 May 2025; *Published* 04 June 2025

The advancement of digital media has profoundly transformed the landscape of communication, expression, and information dissemination. Although these innovations have fostered greater democratic participation, enhanced access to information, and strengthened freedom of speech, they have simultaneously posed serious challenges to the constitutionally guaranteed right to privacy. This research paper critically examines the evolving relationship between digital media and the right to privacy within the Indian constitutional framework. The study explores how digital platforms, while promoting open dialogue, often become arenas for surveillance, unauthorised data collection, cyberbullying, and the widespread sharing of sensitive personal information. It provides a comprehensive analysis of existing legal provisions, judicial pronouncements, and regulatory mechanisms that govern this complex intersection. Emphasis is placed on the emerging jurisprudence surrounding data protection, informational autonomy, and digital rights. Through this inquiry, the article highlights key gaps in the current legal architecture and underscores the urgent need for a balanced legal approach. It advocates for a nuanced regulatory framework that ensures the protection of individual privacy without unduly restricting the freedom and independence of the digital media ecosystem.

Keywords: *privacy, digital media, freedom of expression, data protection, legal framework.*

INTRODUCTION

The concept of digital privacy refers to an individual's right and ability to control how their data is collected, used, and disseminated in the virtual environment. It reflects the desire to engage with the digital world, be it browsing, communicating, shopping, or socialising, without the constant fear of unauthorised access, surveillance, or exploitation of personal information. In the traditional sense, privacy was associated with physical spaces and tangible interactions; however, with the widespread adoption of digital technologies, the boundaries of privacy have undergone significant evolution. Today, the internet, social media, cloud storage, mobile applications, and artificial intelligence tools are all capable of recording and analysing user data, often without explicit consent or knowledge.

As technology has become more pervasive and sophisticated, the collection and use of personal data have grown exponentially, rendering the once straightforward concept of privacy into a multifaceted legal and ethical concern. From cookies and metadata to biometric identifiers and behavioural analytics, individuals constantly leave behind a digital footprint that can be used to profile, track, and even manipulate them. The digital self, created through one's online searches, posts, clicks, and transactions, has become an extension of the physical self, equally deserving of constitutional and legal protection.

In this transformed environment, privacy is no longer limited to the confidentiality of communication or the sanctity of personal space. It now encompasses a wide range of issues, including data protection, consent, informational autonomy, cyber surveillance, and digital identity. The growing reliance on online platforms for essential services such as banking, healthcare, education, and governance further complicates the privacy landscape. Users are often compelled to share sensitive data in exchange for access, without fully understanding the implications or risks involved.

In the Indian context, where digital literacy is still developing and regulatory mechanisms are in an emerging stage, the challenges to digital privacy are even more pronounced. The absence of a comprehensive data protection law, instances of government surveillance, data leaks, and corporate misuse of information have raised serious concerns about the safeguarding of individual rights in the digital age. Therefore, it becomes imperative to explore and redefine the contours of privacy in the context of rapid technological change,

ensuring that the legal system remains strong, responsive, and aligned with the fundamental rights guaranteed under the Constitution.

WHAT IS PRIVACY?

The concept of privacy differs from one society to another, influenced by the dominant political system in each; the political structure is important in shaping the patterns of privacy and surveillance enforced by the State. The classification of modern society can range from a democratic system to a totalitarian system. An analysis of privacy across different societies provides a clear insight into how the political framework shapes the concept of privacy. In countries that favor totalitarian governance, there is significant monitoring by the state. The government is likewise very concealed regarding its operations, as evident in China and Russia. These States reject the notion of individualism and prioritise the interests of the State over those of individuals. Unlike totalitarian regimes, democratic nations are more inclined to follow the individualistic theory, which emphasises the rights and freedoms of the individual. As a result, surveillance, secretly listening to or recording conversations, and gathering personal information from citizens with sophisticated technological devices have become prevalent in these societies.[1]

Several theorists incorporate the concept of control when defining privacy, with Charles Fried being the most prominent. In his writings, he defined 'Privacy' as 'the control we possess regarding information about ourselves.' Charles Fried was worried about the rising number of stealthy encroachments by advanced technology into areas that were previously untouched and the escalating demands for personal data by government and private organisations. He described that the idea of privacy necessitates a feeling of authority and control over elements of one's surroundings. This authority may be granted through a legal title for oversight.[2]

Arthur Miller, in his book 'The Assault on Privacy', informs that a 'Dossier Society' fostered by computers poses a danger to personal privacy, which is needed in a democracy. Arthur asserts that defining privacy is challenging since it is frustratingly unclear and fleeting as a

[1] Margaret Mead and Elena Calas, 'Child-Training Ideas in a Post-Revolutionary Context: Soviet Russia' in Margaret Mead and Martha Wolfenstein (eds), *Childhood in Contemporary Cultures* (University of Chicago Press 1955) 179, 190–91

[2] Charles Fried, 'Privacy' (1968) 77(3) Yale Law Journal 475, 482–483

principle, serving different meanings for different people. He concurs with the perspective that a key component in defining the right to privacy is the person's capacity to manage the dissemination of information about themselves.[3] In this age of technology and sophisticated monitoring methods, it is essential to uphold human dignity.

As stated by Prof. P.K. Tripathi, the core of privacy is rooted in the concept of exclusion.[4] While the right to privacy may appear as a single right, it encompasses a variety of ideas expressed by various individuals over time. Thus, it is contextual in essence. Privacy is simply the act of keeping others away from personal affairs, so the crux of privacy is exclusion.

As evident from the definitions, it is obvious that academics and legal experts do not share the same opinion on the definition of privacy, even so, the concept of the right to privacy can be summarized in this way- every person has an essential requirement for personal space where they can feel assured of no intrusion from others and the concept of privacy differs based on cultures, traditions, societies and countries.[5]

UNDERSTANDING PRIVACY IN THE DIGITAL AGE

Privacy involves more than merely concealing personal matters from the public; it encompasses the right and autonomy of individuals to determine which aspects of their personal information may be shared and who may access it. As everyday activities and private lives become increasingly integrated with digital technologies, understanding and protecting personal details has become more vital than ever. Comprehending privacy in the digital era also involves acknowledging its economic worth. Personal data is an important resource for numerous companies as it enables them to serve their clients more efficiently. Nevertheless, the improper and unchecked utilisation of this information may result in numerous issues for individuals, such as identity theft, financial deception, and pervasive monitoring. The government collects data for various reasons, commonly tied to matters like national security and preventing crime. In the digital age, privacy entails being aware of how government authorities collect, use, and manage personal data. Yet, in the absence of

[3] Arthur R Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press 1971)
[4] Prof. P. K. Tripathi, 'Kesavananda Bharati vs. State of Kerala: Who Wins' (1974) 1 SCC J-3
[5] Soli J Sorabjee, *The Laws of Press Censorship in India* (2nd edn, N M Tripathi 1976) 144

adequate oversight and regulation, this type of collection may result in a violation of civil liberties.

DEFINITION AND SCOPE OF DIGITAL MEDIA

Digital media encompasses any device or medium that utilises digital signals to transfer content. Digital media, in contrast to conventional media like printed books or artwork, allows individuals the freedom to reach their preferred digital content anytime and anywhere they want. Instances of digital media in everyday life could include text, audio, video, graphics, video games, podcasts, and touchscreen kiosks.[6] The word 'digital' includes anything involving numerical digits, while 'media' denotes a way of conveying information; therefore, digital media refers to content that is conveyed through electronic devices or digital screens. In essence, it refers to any type of media that depends on an electronic device for its production, distribution, observation, and storage.[7] The dictionary meaning of digital media is that it is a type of media that can be stored, modified, and accessed through digital technology.[8] There can be different types of digital media depending on the format- audio, video, image, text, content type, e-books, blogs/articles, social media, advertising, art, gaming, and digital reality.

ROLE OF DIGITAL MEDIA IN MODERN COMMUNICATION

The function of digital media in modern communication is important, but at the same time complex. Digital media has transformed how people communicate with one another; services like WhatsApp, Zoom, and Facebook Messenger enable people to communicate across geographical limits, instantly improving both personal and professional exchanges. For example, social networking platforms enabled by digital media played a crucial role during emergencies like the COVID-19 pandemic. At a time when physical distancing was necessary, these platforms became the primary channels through which people stayed connected, shared information, and maintained social relationships.

---

[6] 'What Is The Future of Digital Media? What Are Types of Digital Media??' (*builtin*) <https://builtin.com/media-gaming> accessed 22 April 2025

[7] Christy Walters, 'Guide to Digital Media in Marketing' (*Copy Press*, 27 April 2022) <https://www.copypress.com/blog/digital-media-definition-and-examples/> accessed 22 April 2025

[8] 'Digital Media' (*Merriam-Webster*) <https://www.merriam-webster.com/dictionary/digital%20media> accessed 22 April 2025

Digital media has made the circulation of information more accessible to everyone. Traditionally, the distribution of information was largely controlled by journalists and mainstream broadcasters. However, the rise of digital platforms has significantly altered this by enabling anyone with internet access to produce and share content. This shift has empowered marginalised communities, giving them a platform to voice their concerns and has provided grassroots movements with greater visibility and influence on both national and global stages. Movements like #BlackLivesMatter and #MeToo gained momentum via social media, demonstrating the influence of digital platforms in shaping socio-political discussions.

Digital media has changed political communication. Politicians and public officials now utilise social media platforms to connect directly with constituents, circumventing conventional media outlets. This open communication encourages transparency and promptness, but also brings up worries regarding the dissemination of false information and the decline of journalistic standards. Digital media has emerged as a transformative force in contemporary communication. Its ability to facilitate real-time interaction, ensure widespread access to information, and encourage civic engagement has made it an indispensable component of modern society. However, to fully leverage its capabilities, it is essential to tackle the issues related to misinformation, data privacy, and the digital gap. As digital media keeps advancing, a harmonious strategy that encourages innovation while protecting personal rights and maintaining social unity is crucial.

INTERSECTION OF DIGITAL MEDIA AND INDIVIDUAL PRIVACY

The rapid expansion of digital media has greatly affected individual privacy, altering how personal data is gathered, distributed, and managed. Accordingly, the intersection of digital media and privacy has emerged as an urgent issue for legal experts, policymakers, and technology users.

Digital media platforms operate by continuously gathering user information such as location, online behaviour, individual tastes, and interaction styles. This information is frequently collected by algorithms that aim at customising user experiences for better advertisements. On the other hand, these practices pose considerable privacy issues, especially when data is gathered without informed consent or utilised for purposes that exceed user expectations.

The intersection of digital media and personal privacy constitutes one of the most complicated challenges of the digital age. Although digital platforms provide substantial advantages in terms of connectivity and access to information, they also present notable risks to personal privacy.

PRIVACY CHALLENGES POSED BY DIGITAL MEDIA

Many challenges confront people when it comes to preserving privacy in digital media. The prevalent and frequently concealed data collection techniques employed online, hinder individuals from knowing what data are gathered and its subsequent usage, trying to manage the transmission of personal data throughout the extensive reach of the internet is an overwhelming challenge and many people do not possess the required information and resources to effectively handle their online privacy.

The emergence of smart city technologies represents a significant technological development that may pose potential risks to digital privacy; these technologies seek to enhance the quality of life by integrating digitalisation and data analysis into urban management, leading to the vast accumulation of personal data. Improper use of this data may result in individuals facing unjust surveillance, targeted advertising, and potential discrimination. The extensive development of digital media has resulted in the acceptance of surveillance by government entities and private companies.

Social media sites and search engines consistently monitor user activity, while governments employ digital monitoring for security and law enforcement objectives. This has significantly diminished online anonymity, subjecting individuals to constant observation. Users frequently consent to terms without grasping their consequences because of complicated legal terms and the need to use services. This situation weakens personal autonomy and emphasises the necessity for more accessible and significant consent processes in digital media contexts. Although privacy policies and consent forms are widely used, the effectiveness of consent as a safeguard for personal data has increasingly been called into question. Social media sites motivate users to willingly disclose personal details, frequently merging the boundaries between public and private realms. The practice of self-disclosure, fuelled by likes, shares, and algorithmic exposure, complicates the conventional concept of privacy.

Tech firms exert considerable power over digital privacy standards via their platform configurations, data practices, and reactions to state requests. As private companies hold extensive user data, concerns emerge regarding accountability, transparency, and the equilibrium between business interests and user rights. Corporate behaviours, including shadow profiling and unclear data-sharing contracts, intensify privacy worries.

EVOLUTION OF RIGHT TO PRIVACY IN INDIA'S LEGAL FRAMEWORK

In the historic ruling of Justice K.S. Puttaswamy (Retd) v Union of India[9], a nine-judge panel of the Supreme Court of India unanimously upheld the fundamental right to privacy as a core component of the right to life and personal liberty under Article 21[10] of the Constitution. The judgment overturned previous rulings in MP Sharma v Satish Chandra[11] and Kharak Singh v State of Uttar Pradesh[12] to the degree that they rejected the recognition of a constitutional right to privacy.

Justice D.Y. Chandrachud, in a statement on behalf of four judges, underlined that privacy is not a limited, singular right but rather a wide and multifaceted idea that safeguards dignity and autonomy. He noted that privacy encompasses the ability to make decisions regarding marriage, procreation, contraception, sexual orientation, and personal data.

LAW RELATING TO DIGITAL MEDIA IN INDIA

The IT Rules 2021[13] are the sole legislation in India that explicitly governs the digital media sector; there are numerous other legal provisions in the current framework that also address this topic. Therefore, it is appropriate to first address the IT Act (main provisions of IT Rules 2021) and other pertinent provisions therein, before discussing the IT Rules 2021. These laws and regulations are detailed as follows:

[9] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1
[10] Constitution of India 1950, art 21
[11] *M.P. Sharma v Satish Chandra* (1954) SCR 1077
[12] *Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295
[13] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

Information and Technology Act 2000 -

Under Chapter XI of the IT Act 2000, Sections 65[14], 66[15], 66A[16], 66C[17], 66D[18], 66E[19], 66F[20], 67[21], 67A[22], and 67B[23] specify penalties for computer-related crimes that can also be performed via digital media. These offenses include altering computer source code, committing computer-related crimes defined in Section 43[24], sending offensive messages via communication services, identity theft, impersonation fraud by utilizing computer resources, privacy violations, cyber terrorism and distributing or transmitting obscene materials electronically, along with materials featuring sexually explicit acts and those depicting children in sexually explicit acts, respectively.

Section 43A[25] requires that corporate entities that 'own, manage or process' any 'sensitive personal information' to adopt and uphold 'adequate security measures'; if they do not, they will be responsible for compensating individuals harmed by any negligence linked to this omission. This section contains three important things:[26]

1. Only the specifically defined 'body corporates' involved in 'commercial or professional activities' are the focus of this section. Therefore, this section completely omits government agencies and non-profit organisations.[27]
2. 'Sensitive personal data or information' refers to any details that the Central Government may label as such, at its discretion.[28]

[14] Information Technology Act 2000, s 65
[15] Information Technology Act 2000, s 66
[16] Information Technology Act 2000, s 66A
[17] Information Technology Act 2000, s 66C
[18] Information Technology Act 2000, s 66D
[19] Information Technology Act 2000, s 66E
[20] Information Technology Act 2000, s 66F
[21] Information Technology Act 2000, s 67
[22] Information Technology Act 2000, s 67A
[23] Information Technology Act 2000, s 67B
[24] Information Technology Act 2000, s 43
[25] Information Technology Act 2000, s 43A
[26] Prashant Iyengar, 'Privacy in India: Country Report - October 2011' (2013) SSRN <http://dx.doi.org/10.2139/ssrn.2302978> accessed 22 April 2025
[27] Information Technology Act 2000, s 43A expl (i)
[28] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, r 3

3. The section mandates that body corporates adhere to 'reasonable security practices,' which are limited to measures specified in either an agreement between the parties, any existing laws, or as outlined by the Central Government.[29]

Section 69[30] empowers the Central or a State Government to issue direction for the interception, monitoring or decryption of any information via any computer resource to safeguard the sovereignty or integrity of India, defence of India, maintain State security, uphold friendly relations with foreign nations, preserve public order, prevent incitement to commit any cognizable offence and assist in the investigation of any offence. Section 69A[31] gives power to the Central Government to issue directions to restrict public access to any information using any computer resource for similar reasons, and Section 69B empowers the Central Government to issue directives allowing any agency to oversee and gather traffic data or information via any computer resource for cybersecurity.[32]

Cases under the Act -

Shreya Singhal v Union of India:[33] The issue was regarding the constitutionality of Section 66A,[34] which criminalised sending offensive messages through communication services. The Supreme Court struck down Section 66A as unconstitutional for violating freedom of speech and expression under Article 19(1)(a)[35]. The Court held the provision vague, overbroad, and prone to misuse. It remains a landmark decision for digital free speech, emphasising the need for clarity in laws affecting expression.

Kamlesh Vaswani v Union of India:[36] The petitioner sought a complete ban on online pornography in India, citing moral and social concerns. The Court did not pass a blanket ban; it directed the government to block specific child pornography websites and improve cybercrime monitoring. It highlighted tensions between morality, free speech, and technological enforcement under the IT Act.

[29] Information Technology Act 2000, s 43A, Explanation (ii).
[30] Information Technology Act 2000, s 69
[31] Information Technology Act 2000, s 69A
[32] Information Technology Act 2000, s 69B
[33] *Shreya Singhal v Union of India* (2015) 5 SCC 1
[34] Information Technology Act 2000, s 66A
[35] Constitution of India 1950, art 19(1)(a)
[36] *Kamlesh Vaswani v Union of India* WP (C) No 177/2013

State of Tamil Nadu v Suhas Katti:[37] Suhas Katti was accused of posting obscene, defamatory messages about a woman in a Yahoo chat group and creating a fake email account in her name. The accused was convicted and sentenced to two years' imprisonment with a fine. First conviction under the IT Act, 2000, and a milestone case in cyberstalking and harassment, showing the Act's applicability in protecting personal dignity.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 -

This Act was enacted under Section 43A[38] to regulate the handling of sensitive personal data and ensure reasonable security practices for protecting user privacy. IT Rules, 2011[39] aim to safeguard personal data by mandating informed consent for its collection, restricting unauthorised disclosure, and enforcing security measures. Through these provisions, the regulatory framework seeks to prevent data misuse, protect individual privacy, and mitigate the growing threats posed by cyberattacks and digital vulnerabilities. Even so, the absence of solid enforcement mechanisms and the introduction of the Personal Data Protection Bill[40] have underscored the necessity for more stringent data protection regulations in India.

Karmanya Singh Sareen v Union of India:[41] It is a case related to the challenge of WhatsApp's updated privacy policy that allowed sharing user data with Facebook, allegedly violating user consent and the 2011 IT Rules. Petitioners argued that WhatsApp's data-sharing practice violated Rule 5[42], which mandates informed consent for data disclosure. Though the Delhi High Court allowed the policy change with conditions, the Supreme Court transferred the matter to the Constitution Bench in light of the broader privacy debate under the Puttaswamy case. It raised serious questions about consent, third-party data sharing, and the enforceability of privacy rules in India.

[37] *State of Tamil Nadu v Suhas Katti* Case No 4680/2004
[38] Information Technology Act 2000, s 43A
[39] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, pt II s 3(i)
[40] Personal Data Protection Bill 2019, s 4
[41] *Karmanya Singh Sareen v Union of India* (2017) 10 SCC 1
[42] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, r 5 pt II s 3(i)

Dhruval B. Shah v State of Gujarat[43]: The issue is regarding the disclosure of private information on a matrimonial website without valid consent. The petitioner contended that revealing his sensitive personal data violated Rules 3 and 5 of the 2011 Rules[44] (especially regarding lawful purpose and consent). The Court acknowledged the relevance of the 2011 Rules and stressed that consent must be free, informed, and specific. It recognised that matrimonial and user-generated platforms must follow the IT Rules in managing sensitive personal information.

Unique Identification Authority of India (UIDAI) v Central Bureau of Investigation (CBI):[45] The CBI sought access to Aadhaar data during a criminal investigation. UIDAI objected, citing privacy and the 2011 Rules. UIDAI argued that disclosure of biometric information without proper authorisation violates Rule 6[46], which limits data disclosure without prior consent. The Court ruled in favour of UIDAI, reinforcing that data protection rules override general investigative access unless due process is followed. It affirmed the applicability of the 2011 Rules to state agencies, not just private entities, thereby protecting informational privacy.

The Personal Data Protection Bill 2019 -

The Personal Data Protection Bill, 2019,[47] was presented in Lok Sabha by the then Minister of Electronics and Information Technology in December 2019. The Bill aims to ensure the safeguarding of individuals' data and sets up a Data Protection Authority for this purpose. The Bill was retracted in 2022 following criticisms and was substituted with the Digital Personal Data Protection Act 2023.[48] The DPDP Act 2023[49] updates the structure yet diminishes personal rights relative to the PDP Bill 2019[50].

[43] *Dhruval B Shah v State of Gujarat* 2015 CriLJ 3107
[44] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, rs 3 and 5
[45] *UIDAI v Central Bureau of Investigation* WP (Crl) 2103/2012
[46] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, r 6
[47] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, r 3
[48] Digital Personal Data Protection Act 2023, s 2
[49] Digital Personal Data Protection Act 2023
[50] Personal Data Protection Bill 2019

Justice K.S. Puttaswamy (Retd.) v Union of India:[51] This landmark Supreme Court judgment declared the right to privacy as a fundamental right under Article 21 of the Indian Constitution. The judgment explicitly called for a comprehensive data protection law, which became the basis for the Justice B.N. Srikrishna Committee Report and the drafting of the PDP Bill, 2019. Although this case predates the formal introduction of the Bill, it is foundational to its drafting and constitutional justification.

Internet Freedom Foundation v Union of India[52]**:** The petition challenged the voluntary use of Aarogya Setu (a COVID-19 contact-tracing app), raising concerns over consent, data retention, and purpose limitation. The petition argued that the absence of a data protection law like the PDP Bill leaves users vulnerable to excessive data collection by the State without safeguards.

WhatsApp LLC v Union of India:[53] This case challenged the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, particularly the traceability requirement that allegedly undermined user privacy and end-to-end encryption. WhatsApp relied on the principles of the PDP Bill, such as data minimisation, consent, and purpose limitation, to argue that these rules violated user privacy. Although not under the PDP Bill itself, this case uses its proposed standards to assess the constitutionality and proportionality of government-imposed obligations on digital platforms.

Digital Personal Data Protection Act 2023 -

The DPDP Act 2023 has a considerable effect on digital media, especially concerning the methods of collecting, storing, processing, and sharing personal data by online platforms, news agencies, social media companies, and digital advertisers.[54]

The Act has a considerable effect on digital media, especially concerning the methods of collecting, storing, processing, and sharing personal data by online platforms, news agencies, social media companies, and digital advertisers. The Act consist of - it applies to personal data collected in digital form or digitised later[55], definition of personal data[56], consent and

[51] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1
[52] *Internet Freedom Foundation v Union of India* WP (C) No 3062/2020
[53] *WhatsApp LLC v Union of India* WP (C) No 313/2021
[54] Digital Personal Data Protection Act 2023
[55] Digital Personal Data Protection Act 2023, s 3
[56] Digital Personal Data Protection Act 2023, s 2

legitimate use[57], obligations of data fiduciaries[58], rights of data principals[59], cross-border data transfers[60], exemptions[61], penalties and enforcement.[62]

The Act strengthens data rights and consumer control over personal information and supports businesses while ensuring accountability in data handling. In the fast-changing digital environment, effective enforcement measures are crucial for maintaining privacy rights. As technology progresses faster than regulatory systems, government agencies, regulatory organisations, and international collaboration are essential in enforcing and guaranteeing adherence to privacy regulations.

USER AWARENESS AND BEHAVIOUR TOWARDS PRIVACY RISKS

An inconsistency in digital privacy arises when individuals express a strong desire to protect their personal information, yet willingly share sensitive data on online platforms. Research shows that while users are deeply concerned about the potential misuse of their data, their actions often reflect the loss of control; several factors contribute to this, including the vague and complex nature of privacy policies, users' habitual acceptance of intrusive interfaces, and the cognitive burden involved in managing privacy settings. For the sake of convenience and ease of use, many users tend to accept default options or disregard permission requests without fully understanding the implications.

Awareness of privacy risk among users differs greatly in various groups. Surveys reveal that although digital natives (like Gen Z) possess technological skills, they often do not fully grasp the complexities of data collection and monetisation. Older individuals may be more wary but often face challenges with the digital literacy necessary to utilise privacy tools. Factors such as educational background, socioeconomic status, and regional digital infrastructure also contribute to varying levels of privacy awareness. Initiatives aimed at enhancing awareness generally emphasise policy transparency, public education initiatives, and digital literacy education.

[57] Digital Personal Data Protection Act 2023, ss 4-5
[58] Digital Personal Data Protection Act 2023, ss 6-9
[59] Digital Personal Data Protection Act 2023, ss 11-14
[60] Digital Personal Data Protection Act 2023, s 16
[61] Digital Personal Data Protection Act 2023, s 17
[62] Digital Personal Data Protection Act 2023, ss 25-33

The design and architecture of digital platforms significantly impact user behaviour regarding privacy. Interface options, including default opt-ins and dark patterns, guide users to share their data even if they favour privacy; regular updates to privacy policies and settings generate confusion and fatigue. Behavioural economics indicates that decision-making in this area is frequently irrational, influenced more by convenience and instant rewards than by future privacy concerns.

ETHICAL CONCERNS IN DIGITAL MEDIA PRIVACY

Media organizations bear a unique ethical responsibility to honour privacy, particularly in their reporting methods and the sharing of content; there is an ethical duty to balance the freedom to share information with the responsibility to protect individual dignity Digital journalism frequently confuses public interest with nosiness, endangering individuals who are unexpectedly thrust into the spotlight.

Responsible journalistic practices involve anonymising information, securing informed consent before publication, and steering clear of sensationalist coverage that infringes on personal lives without a strong public justification. The ethical issues related to digital media privacy are complex and necessitate more than just adherence to laws; they call for a shift in digital governance focused on human dignity, autonomy, and fairness. With digital platforms increasingly influencing society, it is essential to incorporate ethical values into design, policy, and practice. It can be said that safeguarding privacy in the digital era is as much an ethical challenge as it is a technological or legal one.

CONCLUSION

The intersection of digital media rights and the right to privacy presents a multifaceted and continually evolving legal challenge, particularly within the Indian legal and socio-political framework. As digital platforms become more integral to personal communication, professional engagement, and public discourse, the scope for potential violations of privacy rights expands significantly. While digital media has undoubtedly enhanced democratic participation by enabling greater freedom of speech and access to information, it has also blurred the lines between public and private spheres. In such a scenario, safeguarding privacy becomes more difficult and more crucial.

Freedom of speech and expression enshrined under Article 19(1)(a)[63] of the Indian Constitution is a foundational pillar of democracy. However, its exercise must be tempered with a sense of responsibility, especially when it has the potential to intrude upon the private lives of individuals. The right to privacy is recognised as a fundamental right under Article 21[64] in the landmark judgment of Justice K.S. Puttaswamy v Union of India[65] affirms that individual autonomy and dignity must be preserved, even in the digital space. This judicial recognition underscores the urgent need for a legal approach that reconciles both rights without subordinating one to the other.

Despite these important judicial strides, India still lacks a comprehensive and enforceable data protection framework that can adequately address the complexities of digital privacy. Regulatory bodies often lack the autonomy, expertise, or authority to effectively enforce privacy norms against both state and private actors. Additionally, vague or outdated laws, combined with rapid technological advancements, create legal gaps that can be exploited to the detriment of individual rights.

This research concludes that a full-bodied, rights-based approach to data governance is imperative. India must prioritise the enactment and implementation of stringent data protection legislation that aligns with global standards while also being sensitive to the unique challenges of its diverse population. Besides, there is a need to evolve judicial and legislative principles that ensure a harmonious balance between the liberty of digital media and the protection of individual privacy. A democratic society governed by the rule of law cannot afford to privilege one right at the expense of another. Instead, a careful equilibrium must be established, one that fosters free expression while preserving the sanctity of personal privacy in an increasingly digitised world.

[63] Constitution of India 1950, art 19(1)(a)
[64] Constitution of India 1950, art 21
[65] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1