

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

DIGITAL PRIVACY AND THE RIGHT TO PRIVACY IN INDIA- A SOCIO- LEGAL RESEARCH

AUTHORED BY - ASWATHY VISWANATHAN
Sree Narayana Law College, Poothotta, Ernakulam, Kerala

ABSTRACT

The rapid expansion of digital technology has fundamentally transformed the relationship between individuals, the State, private corporations, and personal information. In India, digital platforms, smartphones, biometric identification systems, online banking, electronic health records, social media, artificial intelligence, and e-governance have become integral to everyday life. These developments have created significant opportunities for economic growth, social interaction, public administration, and access to essential services, but they have simultaneously generated serious concerns regarding privacy, surveillance, profiling, data breaches, identity theft, behavioral manipulation, and unauthorized processing of personal information. The constitutional recognition of privacy as a fundamental right by the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India* marked a decisive transformation in Indian constitutional jurisprudence. The judgment established that privacy is intrinsic to life, liberty, dignity, autonomy, and individual identity under Article 21 and is also connected with the freedoms guaranteed under Part III of the Constitution.¹

The emergence of digital privacy has consequently expanded the traditional understanding of privacy from physical and spatial protection to informational self-determination and control over personal data. The enactment of the Digital Personal Data Protection Act, 2023 represents an important legislative development in this field.² Nevertheless, legal protection alone cannot resolve the socio-legal problems created by digitalisation. The effectiveness of privacy protection depends upon awareness, digital literacy, institutional accountability, technological safeguards, accessible remedies, responsible corporate practices, and meaningful limitations on State power. Vulnerable groups, including children, economically weaker persons, rural populations, and persons with limited digital literacy, face particularly serious risks because they may have little practical ability to understand or control the collection and use of their personal data. This paper examines the evolution, constitutional foundation, statutory framework,

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

² Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

judicial interpretation, and socio-legal dimensions of digital privacy in India. It argues that privacy should not be understood merely as an individual right against unauthorized disclosure, but as a broader constitutional guarantee necessary for dignity, autonomy, equality, freedom of expression, and democratic participation in the digital age.

KEYWORDS:

Digital Privacy, Right to Privacy, Article 21, Personal Data, Informational Privacy, Puttaswamy, Data Protection, Surveillance, Artificial Intelligence, Socio-Legal Study.

I. INTRODUCTION

Digitalization has become one of the defining characteristics of contemporary Indian society. Communication, education, employment, healthcare, financial transactions, shopping, entertainment, government services, and political participation increasingly take place through digital platforms. A person may generate hundreds of digital records in a single day through mobile applications, websites, online payments, social networking platforms, location services, biometric authentication, and internet-connected devices. Information that was traditionally considered private can now be collected, stored, analyzed, shared, monetized, and potentially transferred across technological and geographical boundaries. The digital environment therefore presents a fundamental legal question: to what extent should an individual be able to control information concerning his or her private life?

Privacy has historically been associated with the protection of the home, family, correspondence, bodily integrity, and personal space. Digital technology has expanded the scope of this concept considerably. Today, privacy also concerns search histories, photographs, biometric identifiers, financial information, health records, location data, online communications, passwords, preferences, purchasing behavior, social relationships, and inferred characteristics. Even information that an individual voluntarily provides for one purpose may subsequently be combined with other datasets to produce detailed profiles about that person. Digital privacy is therefore not merely about secrecy. It concerns the conditions under which personal information is collected and processed and the power relationships between individuals and entities controlling such information.

The Indian constitutional framework did not originally contain an express provision titled “right to privacy.” Nevertheless, the Supreme Court gradually developed privacy protection through Articles 14, 19, and 21 of the Constitution. Early decisions displayed considerable uncertainty regarding whether privacy constituted a constitutionally protected right. In *M.P. Sharma v.*

Satish Chandra, the Supreme Court rejected a broad recognition of privacy in the context of search and seizure.³ In *Kharak Singh v. State of Uttar Pradesh*, the Court examined police surveillance and recognized aspects of personal liberty, although the judges adopted different approaches to privacy.⁴ Later decisions such as *Gobind v. State of Madhya Pradesh* and *People's Union for Civil Liberties v. Union of India* gradually strengthened the constitutional protection of privacy.⁵

The legal position was conclusively transformed by the nine-judge bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*. The Court unanimously recognized privacy as a fundamental right protected by the Constitution.⁶

The judgment was particularly significant because it connected privacy with human dignity, individual autonomy, bodily integrity, family life, sexual orientation, personal choices, and informational control. The Court also recognized informational privacy as an important dimension of the right. This constitutional development has profound consequences for digital governance because modern governance and commerce depend heavily upon the collection and processing of personal information.

The socio-legal importance of digital privacy lies in the fact that legal rules operate within a society characterized by unequal access to technology, varying levels of digital literacy, economic dependence upon online services, and significant differences in bargaining power. A person may technically consent to a privacy policy but may have no meaningful ability to negotiate its terms or refuse data collection while continuing to access an essential service. Similarly, a citizen may be subject to extensive digital monitoring without fully understanding the consequences. Consequently, privacy protection requires examination not only of statutes and judicial decisions but also of the social realities in which those laws operate.

II. OBJECTIVES

The problem addressed by this paper is the gap between the constitutional recognition of privacy as a fundamental right and the practical ability of individuals to exercise meaningful control over their personal information in an increasingly digital society. Although India has developed important constitutional and statutory protections, technological development frequently occurs faster than legal and institutional responses. The collection of large quantities

³ M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India).

⁴ Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).

⁵ Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148 (India); People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).

⁶ Puttaswamy, (2017) 10 SCC 1.

of personal information by governmental institutions and private platforms creates new forms of power and vulnerability that traditional concepts of privacy may not adequately address.

The primary objective of this study is to examine the constitutional evolution of the right to privacy in India and its application to digital environments. The paper also analyses the Digital Personal Data Protection Act, 2023, judicial developments relating to privacy, State surveillance, Aadhaar, online expression and informational autonomy, and the challenges arising from artificial intelligence, profiling, data breaches, social media, and digital exclusion. A further objective is to examine digital privacy from a socio-legal perspective by considering how legal rights interact with social inequalities, digital literacy, economic dependence, and technological power.

The study adopts a doctrinal and socio-legal methodology. The doctrinal component analyses constitutional provisions, legislation, judicial decisions, and comparative legal principles. The socio-legal component considers the practical consequences of digital data collection for individuals and social groups. The paper relies primarily upon Indian constitutional jurisprudence while making a limited comparison with the European Union's General Data Protection Regulation ("GDPR") to identify principles relevant to strengthening privacy protection in India.

III. CONCEPT AND MEANING OF DIGITAL PRIVACY

Digital privacy refers to the protection of an individual's personal information, digital identity, communications, activities, and choices from unjustified collection, surveillance, disclosure, manipulation, or misuse. It encompasses both the confidentiality of information and the individual's ability to exercise meaningful control over the circumstances in which information concerning him or her is collected and processed. Digital privacy therefore operates at the intersection of technology, law, human rights, and social relations.

The concept is broader than the traditional idea that privacy simply means the "right to be left alone." In the digital environment, an individual can be continuously observed without anyone physically entering the person's private space. A smartphone may disclose location, contacts, browsing behavior, application usage, photographs, communications, and purchasing patterns. A social media platform may use interactions to infer interests, relationships, political preferences, or behavioral tendencies. Artificial intelligence can further transform apparently unrelated pieces of information into sophisticated predictions about individuals. Digital privacy consequently includes protection against the creation and use of such informational profiles.

Informational privacy is particularly important because information can influence the

opportunities available to an individual. Financial data can affect access to credit; health data can reveal sensitive medical conditions; location information can reveal religious, political, or personal associations; and online behavior can influence advertising, employment, insurance, or other decisions. The misuse of information can therefore cause consequences extending far beyond embarrassment or unwanted publicity. Privacy is connected with equality because discriminatory decisions can be based upon personal data and algorithmic profiles. The Supreme Court's recognition of informational privacy in *Puttaswamy* is consequently important. The Court recognized that privacy includes control over the dissemination of personal information and that an individual has an interest in controlling the use of information concerning his or her person.⁷

IV. EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA

The Indian Supreme Court's privacy jurisprudence developed gradually. In *M.P. Sharma v. Satish Chandra*, the Court considered whether search and seizure violated constitutional protections and declined to recognize a general right to privacy comparable to the protection against unreasonable searches under the United States Constitution.⁸ The decision reflected an early and relatively narrow understanding of privacy. In *Kharak Singh v. State of Uttar Pradesh*, the Court considered police surveillance of an individual.⁹ Although the majority did not expressly establish privacy as a fundamental right, it recognized that certain forms of surveillance could interfere with personal liberty. Justice Subba Rao's dissent was particularly significant because it treated privacy as an essential component of personal liberty. The dissent later became influential in the development of Indian privacy jurisprudence.

In *Gobind v. State of Madhya Pradesh*, the Court considered regulations permitting surveillance of persons considered habitual offenders.¹⁰ The Court accepted that privacy could be regarded as a constitutional right, while also recognizing that privacy was not absolute. Restrictions could potentially be justified where they satisfied constitutional requirements.

The decision in *R. Rajagopal v. State of Tamil Nadu* further strengthened privacy protection in relation to publication of private facts.¹¹ The Court recognized a “right to be let alone” and held that an individual has a right to protect the privacy of matters relating to the individual's home, family, marriage, procreation, motherhood, child-bearing, education, and other personal

⁷ Id.

⁸ M.P. Sharma, AIR 1954 SC 300.

⁹ Kharak Singh, AIR 1963 SC 1295.

¹⁰ Gobind, (1975) 2 SCC 148

¹¹ R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (India).

matters. The judgment also recognized the tension between privacy and freedom of expression. In *People's Union for Civil Liberties v. Union of India*, popularly known as the telephone tapping case, the Supreme Court held that telephone conversations were an important aspect of private life and that telephone tapping could violate privacy.¹² The Court prescribed procedural safeguards for interception, thereby demonstrating that technological surveillance must operate within constitutional limitations.

In *District Registrar & Collector v. Canara Bank*, the Supreme Court recognized privacy interests in financial and banking information.¹³ The case demonstrated that privacy is not confined to the home or physical space but can extend to information held by institutions.

The development culminated in *Justice K.S. Puttaswamy (Retd.) v. Union of India*. The nine-judge bench unanimously held that privacy is a fundamental right protected by the Constitution.¹⁴ The judgment overruled aspects of earlier decisions to the extent that they denied constitutional protection to privacy.

V. CONSTITUTIONAL RECOGNITION IN PUTTASWAMY

The Puttaswamy judgment represents the constitutional foundation of India's modern privacy regime. The Court explained that privacy is not an isolated or narrowly defined interest but an essential condition for the exercise of other freedoms. Privacy protects the ability of individuals to make personal decisions without unjustified interference. It also protects the individual against excessive State power and social control.

Article 21 provides that no person shall be deprived of life or personal liberty except according to procedure established by law.¹⁵ The Supreme Court has interpreted Article 21 expansively to include several rights necessary for a life of dignity. Privacy fits naturally within this constitutional framework because meaningful liberty is impossible if every aspect of an individual's life can be monitored or controlled. Article 14 is also relevant because privacy restrictions must not operate arbitrarily or discriminatorily. State collection and processing of personal information should therefore satisfy requirements of fairness and non-arbitrariness. Article 19 provides additional protection where privacy restrictions affect speech, association, movement, or other freedoms. The constitutional protection of privacy must consequently be understood through the combined framework of Articles 14, 19, and 21.

¹² *People's Union for Civil Liberties*, (1997) 1 SCC 301.

¹³ *District Registrar & Collector, Hyderabad v. Canara Bank*, (2005) 1 SCC 496 (India).

¹⁴ *Puttaswamy*, (2017) 10 SCC 1.

¹⁵ INDIA CONST. art. 21.

The Court in Puttaswamy identified several dimensions of privacy, including bodily privacy, spatial privacy, decisional autonomy, and informational privacy.¹⁶ This classification is particularly relevant to digital technology. Information about a person's health, sexuality, finances, location, communications, and personal choices can reveal intimate aspects of identity. Digital privacy therefore protects not simply data as an economic resource but the human person represented through that data. The judgment also established that privacy is not absolute. Any invasion of privacy must satisfy constitutional standards. Subsequent constitutional analysis has generally required legality, a legitimate State objective, proportionality, and appropriate procedural safeguards. This framework is important because technological capability by itself cannot justify governmental intrusion. The fact that information can technically be collected does not mean that it should legally or constitutionally be collected.

VI. PRIVACY, DIGNITY AND INDIVIDUAL AUTONOMY

Privacy is closely connected with dignity because individuals require a protected sphere in which they can form relationships, develop identities, make decisions, and express themselves without constant observation.

The relationship between privacy and autonomy was emphasized in decisions following Puttaswamy. In *Navtej Singh Johar v. Union of India*, the Supreme Court relied upon constitutional values of dignity, autonomy, privacy, and individual choice in protecting intimate personal relationships.¹⁷ Similarly, *Joseph Shine v. Union of India* recognized constitutional values of autonomy and dignity in striking down the criminalization of adultery.¹⁸ These cases demonstrate that privacy is not merely a shield against information disclosure; it is a constitutional principle protecting the ability of individuals to make fundamental choices about their lives. Digital platforms complicate this autonomy. When online behaviour is continuously tracked, choices can be influenced through personalized recommendations, targeted advertising, and algorithmic design.

VII. STATUTORY FRAMEWORK: INFORMATION TECHNOLOGY

ACT, 2000

Before the enactment of comprehensive data protection legislation, the Information Technology Act, 2000 provided important statutory protections concerning digital information. Section

¹⁶ Puttaswamy, (2017) 10 SCC 1.

¹⁷ *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1 (India).

¹⁸ *Joseph Shine v. Union of India*, (2019) 3 SCC 39 (India).

43A introduced liability for failure by a body corporate to implement reasonable security practices in relation to sensitive personal data or information.¹⁹ The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 subsequently provided a regulatory framework concerning sensitive personal information.

Sections 72 and 72A of the Information Technology Act also address confidentiality and disclosure of information.²⁰ These provisions demonstrate the gradual development of legal protection for information in India's digital environment. However, the framework was not originally designed as a comprehensive constitutional data-protection regime. It contained sectoral and fragmented protections and did not comprehensively address modern problems such as large-scale profiling, automated processing, algorithmic decision-making, data portability, or comprehensive individual rights.

VIII. DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 represents a significant development in India's data protection framework.²¹ The legislation regulates the processing of digital personal data and establishes obligations for entities processing such data while recognizing certain rights of individuals. It adopts concepts such as “Data Principal” for the individual to whom personal data relates and “Data Fiduciary” for the entity determining the purpose and means of processing. The Act is important because it attempts to create a statutory relationship between individuals and entities processing their personal data. The principles governing processing, consent, legitimate uses, obligations of Data Fiduciaries, and rights of Data Principals collectively provide a legal structure for digital data governance.

Consent is a significant element of the framework, but consent should not be treated as a complete answer to privacy concerns. A formal consent mechanism may fail to provide meaningful protection where individuals cannot understand lengthy privacy notices, where refusal prevents access to essential services, or where the individual has little bargaining power. The effectiveness of consent depends upon transparency, accessibility, comprehensibility, and genuine choice.

The Act also recognizes the importance of protecting children in the digital environment. Children's data requires heightened protection because children may not fully understand the

¹⁹ Information Technology Act, No. 21 of 2000, § 43A, Acts of Parliament, 2000 (India).=

²⁰ Id. §§ 72, 72A.

²¹ Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

long-term consequences of sharing information online. Digital profiles created during childhood may persist for many years and influence future opportunities.

At the same time, the effectiveness of any data protection legislation depends upon institutional enforcement, awareness, compliance mechanisms, remedies, and the ability of individuals to challenge unlawful processing. A strong statutory framework must therefore be accompanied by effective implementation.

IX. DIGITAL PRIVACY AND STATE SURVEILLANCE

State surveillance creates one of the most serious constitutional challenges to digital privacy. Modern technology enables governments to collect and analyze information on a scale that was difficult to imagine in the analogue era. Telecommunications interception, internet monitoring, facial recognition, biometric identification, location tracking, and large databases can potentially provide authorities with detailed information about individuals.

The constitutional legitimacy of surveillance cannot be determined solely by the government's assertion of public interest. Surveillance may be necessary for national security, prevention of crime, and protection of public safety, but such objectives must operate within constitutional limitations. In *PUC*, the Supreme Court recognized the privacy implications of telephone interception and insisted upon procedural safeguards.²² The principles developed in *Puttaswamy* reinforce the need for legality, necessity, proportionality, and safeguards. available, and the degree of interference should not be excessive in relation to the public interest sought to be achieved. Without such limitations, surveillance can become disproportionate and undermine the constitutional promise of personal liberty.

The digital environment also creates concerns regarding function creep. Data collected for one purpose may subsequently be used for another purpose.

X. AADHAAR AND DIGITAL IDENTITY

The Aadhaar Programme represents an important example of the relationship between digital identity, welfare administration, and privacy. Biometric identification can improve authentication and facilitate delivery of services, but it also involves the collection and centralization of highly sensitive personal information.

The Supreme Court considered Aadhaar-related constitutional questions in *K.S. Puttaswamy*

²² People's Union for Civil Liberties, (1997) 1 SCC 301.

(*Retd.*) v. *Union of India*, commonly referred to as the Aadhaar judgment.²³ The Court examined questions concerning privacy, informational autonomy, proportionality, surveillance, and the use of Aadhaar for public services.

The socio-legal importance of Aadhaar lies in the tension between inclusion and privacy. Digital identification can facilitate access to welfare schemes and reduce duplication, but authentication failures or exclusion can disproportionately affect economically vulnerable individuals. At the same time, large-scale identity databases create risks if information is improperly accessed, combined, or misused.

A rights-based digital identity system must therefore ensure that technological efficiency does not override human dignity. Individuals should not be forced to surrender excessive personal information merely to access essential services.

XI. SOCIAL MEDIA AND DIGITAL PRIVACY

Social media has transformed privacy from a primarily private matter into a complex public and commercial issue. Individuals voluntarily upload photographs, personal opinions, relationship information, locations, educational details, professional information, and other personal content. However, the fact that information is voluntarily posted does not necessarily mean that individuals understand all consequences of its subsequent processing. Social media platforms operate through data-driven business models. User behaviour may be analyzed to personalize content and advertisements. Algorithms can determine which information individuals see, potentially shaping preferences and perceptions.

Privacy problems also arise from third-party sharing, unauthorized screenshots, impersonation, cyberstalking, doxxing, and non-consensual dissemination of intimate material. Victims may experience reputational, psychological, professional, and social consequences even when the original information was shared in a different context. The right to privacy must therefore be balanced with freedom of expression. *Shreya Singhal v. Union of India* is important in this context because the Supreme Court protected online freedom of expression by striking down Section 66A of the Information Technology Act.²⁴ The judgment illustrates that regulation of the internet must respect constitutional freedoms and cannot rely upon vague restrictions.

²³ K.S. Puttaswamy (*Retd.*) v. *Union of India*, (2019) 1 SCC 1 (India).

²⁴ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

XII. DATA BREACHES AND CYBERSECURITY

A major threat to digital privacy arises from data breaches. Personal information stored by banks, hospitals, educational institutions, government departments, e-commerce platforms, and social media companies can become vulnerable through hacking, technical weaknesses, insider misconduct, or inadequate security measures.

The consequences of a breach may extend beyond immediate financial loss. Stolen identity documents can facilitate identity fraud; leaked health information can cause stigma; exposed photographs can lead to harassment; and compromised financial information can facilitate fraud. Data breaches can therefore directly affect dignity, autonomy, security, and economic interests.

Cybersecurity should consequently be understood as a component of privacy protection. A legal right is ineffective if personal information is routinely exposed because organizations fail to implement adequate security measures. Data minimization, encryption, access controls, regular security audits, employee training, breach response mechanisms, and accountability should form part of a comprehensive privacy framework.

The responsibility should not rest entirely upon individuals. It is unrealistic to expect ordinary users to protect themselves against sophisticated cyber threats while large organizations possess superior technological resources. The entities collecting and processing data should bear substantial responsibility for securing that information.

XIII. DIGITAL PRIVACY AND VULNERABLE GROUPS

The socio-legal dimension of privacy becomes particularly visible when examining vulnerable groups. Digital technologies can create unequal risks for individuals based on economic status, age, education, gender, location, and technological literacy.

Individuals with limited digital literacy may accept terms and conditions without understanding how their information will be used. In rural and economically disadvantaged communities, access to digital services may itself be mediated by intermediaries. This creates the possibility that individuals may lose control over personal information when relying on others to complete digital transactions.

Women may face specific privacy threats, including cyberstalking, image-based abuse, online harassment, impersonation, and unauthorized dissemination of intimate material. Children and adolescents may be exposed to targeted advertising, excessive data collection, online grooming, and permanent digital footprints.

Privacy protection must therefore be sensitive to social inequalities. A formally equal right may produce unequal outcomes when people possess different capacities to exercise it. Effective privacy law must provide accessible remedies and educational mechanisms for persons who cannot easily navigate complex digital systems.

XIV. CHILDREN AND DIGITAL PRIVACY

Children constitute a particularly vulnerable category because they may not possess sufficient maturity to understand the long-term implications of data disclosure. Children's online activities can create permanent records concerning interests, behaviour, education, health, and social relationships.

The protection of children's privacy requires a balance between parental responsibility, children's developing autonomy, and the legitimate interests of digital services. Excessive surveillance by parents or institutions can itself raise privacy concerns, while inadequate safeguards may expose children to exploitation.

The Digital Personal Data Protection Act, 2023 contains specific provisions relating to children's personal data.²⁵ The broader policy objective should be to ensure that children's data is not exploited for behavioral manipulation or commercial purposes without appropriate safeguards. Privacy education should also become part of digital education. Children should be taught how personal information can be used, why strong passwords and security practices matter, and why seemingly harmless online disclosures may create long-term consequences.

XV. ARTIFICIAL INTELLIGENCE, PROFILING AND PRIVACY

Artificial intelligence presents new challenges because AI systems can derive information about individuals rather than merely store information explicitly provided by them. Algorithms can analyse photographs, browsing patterns, purchasing behaviour, location histories, voice recordings, and other datasets to make predictions or classifications.

Profiling creates privacy concerns because individuals may not know what information has been inferred about them. An algorithm may classify a person according to characteristics that the person never voluntarily disclosed. Such inferences can influence advertising, employment, credit, insurance, education, or access to services.

Facial recognition technology raises additional concerns because it enables identification in public or semi-public spaces. The traditional distinction between public and private

²⁵ Digital Personal Data Protection Act, No. 22 of 2023, § 9, Acts of Parliament, 2023 (India).

information becomes complicated when technology allows continuous tracking of individuals. A person walking through a public place may reasonably expect to be observed by other people, but may not expect to be systematically identified, recorded, and profiled.

AI therefore requires privacy principles based on transparency, accountability, purpose limitation, data minimization, fairness, and human oversight. The legal framework must also address the problem of automated decision-making where individuals are affected by decisions that they cannot understand or challenge.

XVI. THE RIGHT TO BE FORGOTTEN

The “right to be forgotten” refers broadly to the individual's interest in preventing continued accessibility of certain personal information in circumstances where its continued availability is unjustified. Digital information can remain accessible indefinitely, meaning that a past event may continue to affect an individual's reputation long after its relevance has diminished.

Indian courts have considered the right to privacy in relation to online availability of personal information. The right to be forgotten must, however, be balanced against freedom of speech, freedom of the press, public records, and the public interest in access to information.

The constitutional basis for such a right can be connected with dignity and informational autonomy, but it should not become an unrestricted power to erase legitimate public information. A carefully structured approach should consider the nature of the information, its age, its relevance, the person's public role, the potential harm caused by continued availability, and competing public interests.

XVII. PRIVACY AND FREEDOM OF EXPRESSION

Privacy and freedom of expression are not necessarily competing rights. Both protect individual autonomy and democratic participation. Privacy allows people to think, communicate, associate, and develop opinions without fear of constant observation, while freedom of expression allows individuals to communicate those opinions publicly.

Excessive surveillance can produce a chilling effect on expression. If citizens believe that their online searches, communications, or associations are being monitored, they may avoid legitimate political or social participation. Privacy therefore contributes positively to democratic freedom.

At the same time, privacy cannot be used to prevent legitimate journalism or public-interest reporting. R. Rajagopal illustrates the need to balance privacy with freedom of expression and

publication.²⁶ The appropriate approach is therefore not to treat either right as absolute but to examine the nature and purpose of the interference and the competing constitutional interests.

XVIII. DIGITAL PRIVACY AS A SOCIO-LEGAL PROBLEM

A purely doctrinal analysis of digital privacy is insufficient because the practical exercise of privacy rights is shaped by social and economic conditions. Privacy law assumes that individuals can make informed choices about their information, but actual digital environments frequently undermine this assumption.

The first problem is unequal bargaining power. A major platform may offer services on a “take it or leave it” basis. Users cannot negotiate privacy policies individually. Even if an individual refuses to provide certain data, avoiding data collection may mean losing access to communication, banking, employment, education, or not understand how their information is collected or combined. Consent in such circumstances can become formal rather than substantive.

The third problem is digital dependency. Digital services have become increasingly necessary for social and economic participation. Privacy cannot therefore be protected simply by telling individuals to stop using technology. The law must regulate the conditions under which technology operates.

The fourth problem is the unequal distribution of privacy harms. A data breach affecting a wealthy individual and a data breach affecting a person dependent upon welfare services may have very different consequences. The latter may face greater difficulty obtaining legal assistance or correcting inaccurate records.

XIX. MEANINGFUL CONSENT AND INDIVIDUAL CONTROL

Consent is a central concept in modern data protection law, but the quality of consent is more important than its mere existence. Meaningful consent requires that an individual understands what data is being collected, why it is collected, how long it will be retained, and with whom it may be shared.

Long and technical privacy policies often fail to provide meaningful information. Users commonly click “accept” without reading extensive terms because refusal may prevent access to the service. This creates a gap between legal consent and genuine autonomy.

A more effective approach would require privacy notices to be concise, intelligible, accessible

²⁶ R. Rajagopal, (1994) 6 SCC 632.

in Indian languages where appropriate, and presented at relevant stages of data collection. Individuals should have practical mechanisms to withdraw consent or exercise other legal rights without disproportionate difficulty.

The law should also distinguish between genuinely optional data processing and processing necessary for providing a service. Organizations should not obtain broad consent for unrelated purposes merely because they possess the technological ability to collect additional information.

XX. DIGITAL DIVIDE AND PRIVACY INEQUALITY

India's digital transformation has generated substantial benefits, but digital access remains unequal. Differences in internet connectivity, device ownership, education, language, and digital literacy influence the ability to protect personal information.

Digital literacy should therefore include privacy literacy. Citizens need to understand phishing, fraud, passwords, application permissions, privacy settings, location sharing, biometric authentication, and the consequences of uploading personal information. Awareness programs should be designed particularly for rural communities, older persons, children, and economically vulnerable groups.

Government agencies, educational institutions, civil society organizations, and technology companies should participate in privacy education. Privacy should not become a privilege available only to technologically sophisticated users.

XXI. COMPARATIVE PERSPECTIVE: INDIA AND THE GDPR

The European Union's General Data Protection Regulation provides an influential comparative framework for understanding data protection. The GDPR emphasizes principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. It also recognizes several individual rights, including rights concerning access, rectification, erasure, restriction, and data portability.

India's data protection framework has developed within a different constitutional and socio-economic environment. Nevertheless, the GDPR demonstrates the value of treating data protection as a continuing responsibility rather than merely a matter of obtaining initial consent. The comparative experience also highlights the importance of institutional accountability. Data protection requires effective supervisory mechanisms, meaningful remedies, and sanctions for

serious violations. At the same time, Indian law must remain sensitive to the country's large population, digital inclusion objectives, governmental welfare systems, and diverse technological infrastructure.

XXII. CHALLENGES IN ENFORCEMENT

One of the greatest challenges is the rapid development of technology. Legislation is generally enacted through relatively slow democratic processes, whereas technological products and data practices can change within months or even weeks. Legal rules must therefore be sufficiently adaptable without becoming vague.

Another challenge is jurisdiction. Digital information can cross national boundaries almost instantaneously. An Indian user's information may be stored on servers located in another country and processed by entities incorporated elsewhere. Effective privacy protection consequently requires international cooperation and mechanisms for cross-border enforcement. Institutional capacity is another concern. Data protection authorities require adequate technical expertise, financial resources, independence, and investigative powers. Courts and regulators must also develop technological understanding to assess complex data-processing practices. Finally, individuals require accessible remedies. A constitutional right that can be enforced only through expensive and lengthy litigation cannot provide effective protection to every citizen. Complaint mechanisms, regulatory intervention, alternative dispute resolution, and simplified procedures are therefore important.

XXIII. NEED FOR A RIGHTS-BASED APPROACH

Digital privacy should be approached as a constitutional and human-rights issue rather than merely a matter of commercial regulation. Personal data is not simply an economic commodity. It can represent identity, personality, relationships, health, beliefs, preferences, and choices. A rights-based framework should begin with dignity and autonomy. Data collection should have a legitimate purpose, and the quantity of information collected should be proportionate to that purpose. Individuals should receive meaningful information and effective control. Organizations should be accountable for security and misuse.

The State must also be subject to stronger constitutional scrutiny when it exercises surveillance powers because the relationship between the State and citizen involves a significant imbalance of power. National security and public safety are legitimate objectives, but they cannot automatically justify unlimited collection of personal information.

XXIV. SUGGESTIONS AND RECOMMENDATIONS

First, privacy awareness should be incorporated into digital literacy programs. Citizens should be educated about personal data, consent, cybersecurity, application permissions, online fraud, social media risks, and available legal remedies.

Second, privacy-by-design should become a fundamental principle of digital governance. Privacy should be incorporated into technological systems from the beginning rather than treated as an afterthought following a data breach or public controversy.

Third, organizations should adopt data minimization. Information that is unnecessary for a legitimate purpose should not be collected merely because future technological use may be possible.

Fourth, stronger safeguards should apply to sensitive categories of information, particularly health, biometric, financial, children's, and intimate personal data.

Fifth, surveillance practices should be governed by clear legal standards, independent oversight, necessity, proportionality, and effective remedies. Secret or indefinite surveillance without adequate safeguards creates serious constitutional risks.

Sixth, privacy notices should be simplified and made understandable. Where appropriate, information should be provided in regional languages and through accessible formats.

Seventh, children should receive enhanced privacy protection. Digital platforms should avoid exploitative practices involving children's data and should design services according to the principle of the best interests of the child.

Eighth, AI systems involving personal data should be subject to transparency and accountability requirements. Individuals should have appropriate mechanisms to challenge consequential automated decisions.

Ninth, effective institutional enforcement is essential. Regulatory bodies must have sufficient technical expertise and resources to investigate large technology companies and government data-processing systems.

Tenth, privacy protection should be integrated with cybersecurity. Organizations holding personal information should adopt reasonable technical and organizational safeguards and maintain effective breach-response mechanisms.

Finally, Indian privacy jurisprudence should continue developing in accordance with constitutional principles while recognizing the social realities of India's digital transformation. The objective should not be to prevent technological progress but to ensure that technology develops consistently with dignity, liberty, equality, and democratic values.

XXV. FINDINGS OF THE STUDY

The study demonstrates that digital privacy has evolved from a narrow concept associated with physical seclusion into a comprehensive constitutional interest involving informational autonomy, dignity, identity, and individual choice. Indian constitutional jurisprudence has played a central role in this transformation. The Supreme Court's decisions in *Kharak Singh*, *Gobind*, *PUCL*, *Rajagopal*, and other cases progressively developed privacy protection, culminating in the authoritative recognition of privacy as a fundamental right in *Puttaswamy*. The study further finds that statutory protection is necessary but cannot by itself guarantee effective privacy. The Digital Personal Data Protection Act, 2023 represents an important legislative development, but implementation, awareness, institutional capacity, technological safeguards, and accessible remedies determine the practical effectiveness of the legal framework.

The research also finds that privacy violations have unequal social consequences. Persons with limited digital literacy, children, economically weaker groups, and individuals dependent upon digital welfare or essential services may face greater difficulty exercising control over their information. Privacy is therefore connected with equality and social justice.

The study further establishes that digital privacy cannot be separated from freedom of expression. Excessive surveillance may discourage legitimate speech and association, while unrestricted privacy claims may interfere with journalism and public-interest communication. Constitutional balancing is therefore necessary.

Finally, emerging technologies such as artificial intelligence, facial recognition, predictive analytics, and large-scale profiling require the continued development of privacy principles. Traditional legal concepts must be adapted to technological environments in which information can be inferred, combined, and processed on a scale previously unknown.

XXVI. CONCLUSION

Digital privacy has become an essential constitutional concern in India because modern life increasingly depends upon the collection and processing of personal information. The transformation from an analogue to a digital society has changed the nature of privacy itself. Individuals no longer face privacy threats only when someone physically enters their homes or intercepts their communications. They may be exposed through databases, smartphones, biometric systems, social media platforms, online transactions, artificial intelligence, facial recognition, and algorithmic profiling.

The constitutional recognition of privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India provides the normative foundation for addressing these challenges. By connecting privacy with dignity, liberty, autonomy, and individual identity, the Supreme Court established that privacy is central to constitutional democracy. The subsequent development of data protection legislation demonstrates the movement from constitutional recognition towards a structured statutory framework.

However, the protection of digital privacy cannot be achieved through legislation alone. The socio-legal reality of India demonstrates that individuals possess unequal capacities to understand and exercise privacy rights. Consent may become meaningless when users lack bargaining power. Digital literacy may be insufficient when technology is deliberately complex. Legal remedies may be ineffective when individuals cannot easily identify or challenge misuse. Similarly, technological efficiency cannot justify unrestricted State surveillance or unlimited corporate data collection.

The future of digital privacy in India therefore requires a balanced rights-based approach. Such an approach must encourage technological innovation while placing meaningful limits on the misuse of personal information. Privacy-by-design, data minimization, transparency, accountability, cybersecurity, effective regulatory oversight, child protection, and accessible remedies should become integral components of India's digital governance framework.

Ultimately, digital privacy is not an obstacle to development. It is a condition for sustainable and democratic development. A society in which citizens can communicate, associate, think, transact, and make personal decisions without unjustified surveillance is more consistent with the constitutional promise of liberty and dignity. The challenge before Indian law is therefore not whether society should become digital, but how digital transformation can be achieved without sacrificing the constitutional rights of the individuals whom technology is intended to serve.