LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

Protecting Digital Rights: A Comparative Assessment of The Legal Frameworks Protecting Personal Data in India, Europe, and the US

Author
Aryan Shandilya

Protecting Digital Rights: A Comparative Assessment of The Legal Frameworks Protecting Personal Data in India, Europe, and the US

Aryan Shandilya
Amity University, Noida

Abstract
The protection of digital rights and personal data has become a critical legal concern in the era of rapid technological advancement and data-driven governance. This research paper undertakes a comparative assessment of the legal frameworks governing personal data protection in India, the European Union and the United States. It analyses the General Data Protection Regulation (GDPR) as a rights-based model, the sectoral and fragmented privacy regime of the US and India's evolving framework under the Digital Personal Data Protection Act, 2023. The study examines key aspects such as consent mechanisms, data subject rights, enforcement structures, state surveillance powers and the role of private digital platforms. It highlights the philosophical and structural differences among jurisdictions and evaluates their effectiveness in safeguarding digital rights. The paper concludes that while the EU offers the most robust protection, India and the US face structural gaps requiring reform for ensuring stronger global data governance.

Keywords: *Digital Rights, Personal Data Protection, GDPR, DPDP Act 2023, Privacy Law, Comparative Law, Data Governance, Surveillance, Constitutional Rights, Data Privacy.*

Introduction
The rapid expansion of digital technologies has fundamentally transformed the relationship between individuals, the state and private corporations. In the contemporary digital era, personal data has emerged as one of the most valuable resources, driving innovation, governance, commerce and communication. However, this increasing reliance on data-driven systems has also raised serious concerns regarding privacy, surveillance, consent and the protection of individual autonomy. As a result, the protection of digital rights particularly personal data protection has become a central legal and constitutional issue across jurisdictions.[1]

Digital rights broadly refer to the rights of individuals to access, use, create and share digital information while ensuring protection against misuse, unlawful

[1] Mikkel Flyverbom, Ronald Deibert and Dirk Matten. "The governance of digital technology, big data and the internet: New roles and responsibilities for business." *Business & Society* 58.1 (2019): 3-19.

surveillance and unauthorized data processing. Among these, the right to privacy and data protection has gained significant importance as governments and corporations increasingly collect and process vast amounts of personal information. The legal frameworks governing these rights differ significantly across countries, reflecting distinct constitutional traditions, policy priorities and regulatory philosophies.

The European Union has established the General Data Protection Regulation (GDPR), widely regarded as the most comprehensive data protection framework globally. It is rooted in a rights-based approach that emphasises individual control over personal data, strict compliance obligations for data controllers and strong enforcement mechanisms. In contrast, the United States follows a fragmented and sector-specific approach, where data protection is governed through a combination of federal statutes, state laws such as the California Consumer Privacy Act (CCPA) and judicial interpretations. This system prioritises market flexibility and innovation over uniform privacy protection.[2]

India, on the other hand, represents an evolving regulatory landscape. Following the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India (2017)*, India enacted the Digital Personal Data Protection Act, 2023, marking its first comprehensive data protection law. However, concerns remain regarding broad state exemptions, regulatory independence and enforcement challenges.

Concept And Evolution of Digital Right

The concept of digital rights has evolved alongside technological advancements. In the early phase of the internet, cyberspace was largely unregulated and concerns were minimal regarding data collection or online surveillance. However, with the rise of Web 2.0, social media platforms, e-commerce and cloud computing, the volume of personal data generated and processed increased exponentially. This shift transformed data into a critical economic asset, leading to what is often described as the "data-driven economy" or "surveillance capitalism." In this phase, both private corporations and governments began collecting, analysing and monetising user data on an unprecedented scale.

The evolution of digital rights has therefore moved from a narrow focus on informational privacy to a broader framework encompassing data protection, algorithmic accountability and digital autonomy. International human rights instruments, such as the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17), laid the foundational principles of privacy. However, these frameworks were not designed

[2] Edward S. Dove, "The EU general data protection regulation: implications for international scientific research in the digital era." *Journal of Law, Medicine & Ethics* 46.4 (2018): 1013-1030.

to address modern challenges such as artificial intelligence, big data analytics, biometric surveillance and cross-border data flows.[3]

In response to these challenges, jurisdictions have developed structured legal frameworks. The European Union's General Data Protection Regulation (GDPR) represents a rights-based model that empowers individuals with control over their personal data. In contrast, countries like the United States adopt a sectoral and market-driven approach, while India has recently introduced the Digital Personal Data Protection Act, 2023, reflecting a developing regulatory structure balancing state interests and individual rights.

Personal data has become a cornerstone of the digital economy. It includes any information relating to an identified or identifiable individual, such as names, contact details, location data, financial records, biometric identifiers and online behaviour patterns. In the digital economy, personal data is used for targeted advertising, predictive analytics, artificial intelligence training, consumer profiling and service optimisation. Companies such as global technology platforms rely heavily on data-driven business models to generate revenue and improve user experience.

However, the economic value of personal data also raises serious legal and ethical concerns. The large-scale collection and processing of data increases risks of privacy breaches, identity theft, surveillance and discriminatory profiling. It also creates power imbalances between individuals and large corporations that control data ecosystems. As a result, the regulation of personal data has become essential not only for protecting individual rights but also for ensuring fairness, transparency and accountability in the digital economy.

Historical Background

The development of digital rights and personal data protection is rooted in the broader historical evolution of privacy as a legal and constitutional concept. In early legal thought, privacy was not explicitly recognised as an independent right; however, foundational ideas of individual liberty and protection from arbitrary interference laid the groundwork for its emergence. Philosophers such as John Locke and later constitutional thinkers emphasised the importance of personal autonomy and limitations on state power, which indirectly contributed to the modern understanding of informational privacy.[4]

---

[3] Hector Postigo, *The digital rights movement: The role of technology in subverting digital copyright*. MIT Press, 2012.

[4] John Babikian, "Securing rights: legal frameworks for privacy and data protection in the digital era." *Law Research Journal* 1.2 (2023): 91-101.

The legal recognition of privacy began to take shape in the 19th and 20th centuries. A significant milestone was Samuel Warren and Louis Brandeis' influential article "The Right to Privacy" (1890), which conceptualised privacy as the "right to be let alone." This marked the beginning of privacy as a distinct legal right. Subsequently, the rise of industrialisation, mass media and government surveillance during the World Wars further highlighted the need for stronger protections against intrusion into personal life.

In the post-World War II era, privacy gained international recognition through human rights instruments. Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966) explicitly recognised protection against arbitrary interference with privacy. However, these provisions were general in nature and did not anticipate the technological complexities of the digital age.

The advent of computers in the late 20th century and the subsequent rise of the internet revolutionised data collection and processing. Governments and corporations began storing large volumes of personal information, leading to concerns about surveillance and misuse. Europe responded early with data protection laws such as the Data Protection Directive (1995), which eventually evolved into the General Data Protection Regulation (GDPR) in 2018.[5]

In contrast, the United States adopted a sector-specific approach, regulating privacy through fragmented laws rather than a unified framework. India's journey is more recent, with the landmark judgment in *Justice K.S. Puttaswamy v. Union of India (2017)* recognising privacy as a fundamental right, eventually leading to the enactment of the Digital Personal Data Protection Act, 2023.

European Union's GDPR Framework

The General Data Protection Regulation (GDPR), adopted by the European Union in 2016 and enforced from 2018, is widely regarded as the most comprehensive and influential data protection framework in the world. It establishes a unified legal regime governing the processing of personal data across all EU member states. The GDPR is rooted in a strong rights-based philosophy, aiming to protect individual autonomy, dignity and informational self-determination in an increasingly data-driven society. It also applies extraterritorially, meaning that organisations outside the EU must comply if they process data of EU residents.

[5] Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula. "EU General Data Protection Regulation: Changes and implications for personal data collecting companies." *Computer Law & Security Review* 34.1 (2018): 134-153.

- **Key Principles of GDPR**

The GDPR is built upon several core principles that guide all data processing activities. The principle of lawfulness, fairness and transparency requires that personal data must be processed legally and in a manner that is transparent to the data subject. The principle of purpose limitation ensures that data is collected only for specific, legitimate purposes and not reused in incompatible ways. Data minimisation mandates that only the necessary amount of data should be collected for a given purpose, while accuracy requires that personal data be kept up to date. The principle of storage limitation restricts retention of personal data to no longer than necessary. Integrity and confidentiality ensure appropriate security measures against unauthorized access or processing. Lastly, the principle of accountability places responsibility on data controllers to demonstrate compliance with all GDPR obligations. These principles collectively establish a strict and structured framework for ethical data governance.[6]

- **Rights of Data Subjects**

The GDPR grants extensive rights to individuals, empowering them with control over their personal data. The right to information ensures that individuals are informed about how their data is collected and used. The right of access allows individuals to obtain copies of their personal data held by organisations. The right to rectification enables correction of inaccurate or incomplete data.

One of the most significant rights is the right to erasure, also known as the "right to be forgotten," which allows individuals to request deletion of personal data under certain conditions. The right to data portability enables individuals to transfer their data between service providers. Additionally, individuals have the right to object to processing and the right to restrict processing, particularly in cases involving profiling or automated decision-making.

- **Enforcement and Regulatory Authorities**

The enforcement of GDPR is carried out through independent supervisory authorities established in each EU member state. These Data Protection Authorities (DPAs) monitor compliance, investigate complaints and impose administrative fines for violations. The GDPR provides for substantial penalties, including fines of up to €20 million or 4% of global annual turnover, whichever is higher, making it one of the strictest enforcement regimes globally.

At the supranational level, the European Data Protection Board (EDPB) ensures consistent application of the GDPR across all member states. Additionally, the Court of Justice of the European Union (CJEU) plays a crucial role in interpreting GDPR provisions and shaping data protection jurisprudence through landmark

[6] Paul Voigt and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." *A practical guide, 1st ed., Cham: Springer International Publishing* 10.3152676 (2017): 10-5555.

judgments such as *Google Spain v. AEPD* and *Schrems I & II*, which have significantly influenced global data transfer rules.

Data Protection Framework in the United States

The data protection framework in the United States is characterised by a fragmented and sector-specific approach rather than a single comprehensive privacy law. Unlike the European Union's General Data Protection Regulation (GDPR), the US does not recognise data protection as a uniform fundamental right under federal law. Instead, privacy protection is governed through a combination of federal statutes, state laws and judicial decisions. This system reflects the broader American regulatory philosophy, which prioritises market efficiency, technological innovation and limited government intervention.[7]

- **Sectoral Privacy Model**

The United States follows a sectoral privacy model, meaning that data protection is regulated differently across various industries rather than through a unified framework. For example, the Health Insurance Portability and Accountability Act (HIPAA) governs medical data, the Gramm-Leach-Bliley Act (GLBA) regulates financial information and the Children's Online Privacy Protection Act (COPPA) protects data of minors under 13 years of age.

This sector-specific approach creates gaps in protection because individuals' data is not uniformly regulated across all contexts. Data collected by social media platforms, technology companies, or e-commerce websites may not fall under strict federal privacy regulation unless specific conditions apply. As a result, much of the responsibility for privacy protection is shifted to private companies through terms of service agreements and self-regulatory practices.

- **Role of CCPA and Federal Laws**

In the absence of a comprehensive federal data protection law, state-level legislation has played a significant role in shaping privacy rights in the US. The most prominent among these is the California Consumer Privacy Act (CCPA), 2018, later expanded by the California Privacy Rights Act (CPRA), 2020. The CCPA grants California residents rights such as the right to know what personal data is being collected, the right to request deletion of data and the right to opt out of the sale of personal information.

The CCPA has had a broader national impact, often influencing corporate practices beyond California due to the size of its economy. However, its application is limited geographically, leading to inconsistencies in privacy protection across states. At the federal level, legislative efforts to enact a

[7] Laura Bradford, Mateo Aboy and Kathleen Liddell. "International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection." *Journal of Law and the Biosciences* 7.1 (2020): lsaa055.

comprehensive privacy law have been ongoing but remain incomplete, resulting in a regulatory gap.

- **Judicial Interpretation of Digital Privacy**

The judiciary in the United States has played a crucial role in shaping digital privacy rights, particularly through constitutional interpretation of the Fourth Amendment, which protects against unreasonable searches and seizures. Courts have progressively expanded its scope to include digital data.

In *Riley v. California (2014)*, the Supreme Court held that law enforcement must obtain a warrant to search mobile phones, recognising the vast amount of personal information stored in digital devices. Similarly, in *Carpenter v. United States (2018)*, the Court ruled that accessing historical cell-site location data constitutes a search under the Fourth Amendment, requiring a warrant.

These decisions reflect an evolving judicial recognition of digital privacy; however, the approach remains case-based rather than systematic. The absence of a unified statutory framework means that courts often address privacy issues reactively, depending on specific factual circumstances.

India's Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant milestone in India's evolving data protection regime. It is the first comprehensive legislation specifically designed to regulate the processing of digital personal data in India. The Act emerges in the backdrop of the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy v. Union of India (2017)*, which recognised the right to privacy as a fundamental right under Article 21 of the Constitution. The DPDP Act seeks to balance individual rights over personal data with the needs of the state and the digital economy.[8]

- **Structure and Objectives of the Act**

The primary objective of the DPDP Act is to establish a legal framework for the protection of digital personal data while ensuring lawful and transparent processing. It applies to the processing of digital personal data within India and also extends to foreign entities offering goods or services to individuals in India. The Act introduces key institutional mechanisms, including the establishment of the Data Protection Board of India, which is responsible for enforcement, adjudication of breaches and imposition of penalties.

The structure of the Act is comparatively simplified when compared to the European Union's GDPR. It focuses on core principles such as lawful processing, purpose limitation and data minimisation, but avoids extensive procedural complexity. The Act also places significant emphasis on compliance obligations

[8] Chanlang Ki. Bareh, "Reviewing the Privacy Implications of Indias Digital Personal Data Protection Act (2023) from Library Contexts." *DESIDOC Journal of Library & Information Technology* 44.1 (2024): 50-58.

for data fiduciaries and recognises the need for digital governance aligned with India's developmental priorities.

- **Consent and Data Fiduciary Obligations**

A central feature of the DPDP Act is the concept of consent-based data processing. Personal data can only be processed for lawful purposes with the consent of the individual (referred to as the "data principal"), except in specified circumstances. Consent must be free, informed, specific and unambiguous and individuals must be provided with clear notice regarding the purpose of data collection and usage.

The Act introduces the concept of data fiduciaries, which are entities responsible for determining the purpose and means of processing personal data. Data fiduciaries are required to ensure data security, implement reasonable safeguards against data breaches and comply with obligations relating to transparency and accountability. They are also required to establish grievance redressal mechanisms for individuals.[9]

Significant penalties are prescribed for non-compliance, with the Data Protection Board empowered to impose financial penalties depending on the severity of the breach. However, the enforcement mechanism is largely administrative in nature, with limited judicial oversight at the initial stage.

- **State Exemptions and Regulatory Concerns**

One of the most debated aspects of the DPDP Act is the broad exemptions granted to the state. Government agencies may be exempt from certain provisions of the Act on grounds such as national security, sovereignty, public order and prevention of offences. These exemptions have raised concerns regarding the potential for excessive state surveillance and lack of accountability.

Critics argue that such wide-ranging exemptions may dilute the right to privacy recognised in *Puttaswamy* and create an imbalance between state power and individual rights. Additionally, concerns have been raised about the independence and effectiveness of the Data Protection Board, as it is constituted by the central government, potentially affecting regulatory neutrality.

Comparative Analysis of India, Eu and US Frameworks

The legal frameworks governing personal data protection in India, the European Union and the United States reflect three distinct regulatory philosophies: rights-based regulation, market-driven governance and state-centric developmental regulation. A comparative analysis reveals significant differences in their structure, enforcement mechanisms and scope of individual rights.

---

[9] Subhajit Saha and Surjashis Mukhopadhyay. "A new age of data privacy laws in India: review of Digital Personal Data Protection Act, 2023." *IJLS* 10 (2024): 84.

The European Union's General Data Protection Regulation (GDPR) represents the most comprehensive and rights-oriented framework. It establishes strong principles such as data minimisation, purpose limitation and accountability, while granting extensive rights to individuals, including the right to access, erasure and data portability. Its enforcement is robust, supported by independent supervisory authorities and strict penalties, ensuring high compliance standards across jurisdictions.[10]

In contrast, the United States follows a fragmented and sector-specific approach to data protection. Instead of a unified federal law, privacy is regulated through multiple statutes such as HIPAA, COPPA and GLBA, along with state laws like the California Consumer Privacy Act (CCPA). Judicial intervention, particularly under the Fourth Amendment, has gradually expanded digital privacy protections; however, the absence of a comprehensive framework results in inconsistent and uneven safeguards.

India's Digital Personal Data Protection Act, 2023 represents a developing hybrid model. It seeks to balance individual privacy rights with state interests and economic growth. While it incorporates essential principles such as consent-based processing and fiduciary responsibility, it also grants broad exemptions to the state, raising concerns about surveillance and accountability. Its enforcement structure remains largely administrative, with the Data Protection Board operating under government control.[11]

Overall, the EU prioritises individual dignity and rights protection, the US emphasises flexibility and innovation and India attempts a balanced but state-influenced model. These differences highlight the absence of global uniformity in data protection and underscore the need for harmonised international standards in digital governance.

Role Of Judiciary in Protecting Digital Rights

The judiciary plays a central role in the protection and evolution of digital rights across jurisdictions. In the absence of comprehensive and adaptive legislation in many countries, courts have often acted as key interpreters of constitutional principles to address emerging challenges posed by digital technologies. The role of the judiciary becomes particularly significant in balancing state interests such

[10] Shalini Sinha, "Harmonizing data privacy Laws: A comparative study of approaches in the EU, US and India." *Legal Spectrum J.* 4 (2024): 1.

[11] Colin J. Bennett, *Regulating privacy: Data protection and public policy in Europe and the United States*. Comell University Press, 1992.

as security and surveillance with individual rights such as privacy, autonomy and freedom of expression.[12]

Across jurisdictions, judicial interpretation has been instrumental in recognising digital privacy as an extension of fundamental rights. In India, the landmark judgment of *Justice K.S. Puttaswamy v. Union of India (2017)*[13] marked a turning point by affirming the right to privacy as a fundamental right under Article 21 of the Constitution. This decision laid the foundation for subsequent digital rights jurisprudence. In *Shreya Singhal v. Union of India (2015)*[14], the Supreme Court struck down Section 66A of the Information Technology Act, reinforcing freedom of expression in the digital space. Similarly, in *Anuradha Bhasin v. Union of India (2020)*[15], the Court recognised that internet access is integral to the exercise of fundamental rights, including speech and trade.

In the United States, the judiciary has gradually expanded the scope of constitutional protections to include digital privacy. In *Riley v. California (2014)*[16], the Supreme Court held that law enforcement must obtain a warrant before searching digital content on mobile phones, recognising the vast personal information stored in such devices. In *Carpenter v. United States (2018)*[17], the Court ruled that accessing historical cell-site location data constitutes a search under the Fourth Amendment, thereby requiring judicial authorisation. These decisions demonstrate an incremental judicial approach to adapting constitutional protections to modern technology.

In the European context, the Court of Justice of the European Union (CJEU) has played a proactive role in strengthening data protection standards. In *Google Spain v. AEPD (2014)*[18], the Court recognised the "right to be forgotten," allowing individuals to request the removal of outdated or irrelevant search results. In *Schrems I* and *Schrems II*, the Court invalidated transatlantic data transfer mechanisms, emphasising the need for adequate privacy safeguards in cross-border data flows. Judicial activism has been a defining feature in shaping digital rights. Courts have often stepped in where legislative frameworks were inadequate or outdated, ensuring that constitutional principles remain relevant in the digital age. However, excessive judicial intervention raises concerns about

---

[12] Jamil Afzal, "Best Practice of Digital Laws and Digital Justice." *Implementation of Digital Law as a Legal Tool in the Current Digital Era*. Singapore: Springer Nature Singapore, 2024. 95-120.
[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (SC).
[14] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (SC).
[15] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (SC).
[16] *Riley v. California*, 573 US 373 (2014).
[17] *Carpenter v. United States*, 585 US 2018.
[18] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, EU:C:2014:317 (CJEU).

overreach, where courts may enter policy-making domains traditionally reserved for legislatures and executives.

On the other hand, judicial restraint emphasises deference to legislative intent and institutional boundaries. While this approach preserves democratic legitimacy, it may lead to gaps in protection when legislatures fail to respond to technological changes.

Overall, the judiciary serves as a crucial safeguard of digital rights, navigating the delicate balance between activism and restraint. Its role continues to evolve as technology advances, making it a key institution in shaping the future of privacy and data protection law.

Challenges In Global Data Protection

The protection of personal data in the digital age faces complex and evolving challenges that transcend national borders. As digital ecosystems become increasingly interconnected, issues such as cross-border data flows, surveillance practices and the growing influence of artificial intelligence (AI) and algorithms have created significant regulatory difficulties for all jurisdictions, including India, the European Union and the United States.

One of the most pressing challenges is the regulation of cross-border data flows. Personal data is routinely transferred across multiple jurisdictions for purposes such as cloud storage, digital services and global business operations. However, differing legal standards between countries create conflicts in compliance and enforcement. For instance, the European Union imposes strict adequacy requirements under the GDPR, while the United States and India adopt more flexible or evolving approaches. This lack of harmonisation complicates international data transfers and raises concerns about adequate protection in recipient countries.[19]

Another major issue is surveillance and platform governance. Governments increasingly rely on digital surveillance mechanisms for national security, law enforcement and administrative purposes. While such measures may be justified on security grounds, they often raise concerns regarding proportionality, transparency and potential misuse. Simultaneously, private digital platforms exercise significant control over user data, content moderation and algorithmic decision-making, effectively functioning as quasi-regulatory actors without direct democratic accountability.

The role of AI and algorithms further intensifies these challenges. Automated systems are widely used for profiling, predictive analytics and decision-making in sectors such as finance, healthcare and law enforcement. However, these technologies often operate as "black boxes," lacking transparency and explainability. This raises concerns about bias, discrimination and the erosion of

[19] Federico Fabbrini and Edoardo Celeste. "The right to be forgotten in the digital age: The challenges of data protection beyond borders." *German law journal* 21.S1 (2020): 55-65.

individual autonomy. Moreover, existing legal frameworks struggle to keep pace with rapid technological advancements, leaving gaps in accountability and oversight.

Overall, these challenges highlight the need for stronger international cooperation, harmonised regulatory standards and adaptive legal frameworks to ensure effective protection of digital rights in an increasingly data-driven global environment.

Conclusion

The comparative analysis of India, the European Union and the United States demonstrates that the protection of digital rights and personal data is shaped by differing constitutional philosophies and regulatory priorities. The European Union, through the GDPR, offers the most comprehensive and rights-centric framework, ensuring strong individual control and robust enforcement mechanisms. The United States adopts a fragmented, sectoral approach that prioritises innovation and market efficiency but results in uneven privacy protection. India, under the Digital Personal Data Protection Act, 2023, represents an evolving model that seeks to balance state interests with individual rights, though concerns remain regarding broad governmental exemptions and limited regulatory independence.[20]

The study concludes that while all three jurisdictions address data protection, none offers a perfect model. The growing influence of digital platforms and cross-border data flows necessitates stronger harmonisation of legal standards. A globally coordinated framework is essential to ensure effective protection of digital rights in the digital age.

Literature Review

The literature on protecting digital rights and personal data has expanded significantly with the rise of digital governance, data-driven economies and transnational information flows. While classical constitutional theory did not directly address data protection, its foundational ideas continue to shape modern understandings of privacy, state power and individual autonomy in the digital age. Classical thinkers such as John Locke (1690)[21] and Montesquieu (1748)[22] provide the philosophical foundation for contemporary governance structures. Locke's emphasis on individual liberty and protection against arbitrary state interference contributes indirectly to the modern idea of informational privacy. Montesquieu's doctrine of separation of powers remains central, as he argued that liberty is compromised when legislative, executive and judicial powers are concentrated in one authority. Although these ideas emerged in a pre-digital context, they

[20] Animesh Kumar Sharma and Rahul Sharma. "Comparative analysis of data protection laws and AI privacy risks in BRICS nations: A comprehensive examination." *Global Journal of Comparative Law* 13.1 (2024): 56-85.

[21] John Locke, *Two Treatises of Government* (1689).

[22] Charles-Louis de Secondat Montesquieu, Baron de, *De l'Esprit des Lois* (1748).

continue to inform contemporary debates on governance, surveillance and accountability in data protection regimes.

Modern constitutional scholarship builds upon these classical foundations. A.V. Dicey (1885)[23] emphasised the rule of law and constitutional limitations on state power, which is particularly relevant in regulating state access to personal data. In India, the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India (2017)* marked a significant constitutional shift. Scholars such as Bhatia (2019) and Chandrachud (2019) interpret this judgment as establishing informational privacy under Article 21, requiring legality, necessity and proportionality in any data-related intrusion.

With the emergence of digital governance, the field of "digital constitutionalism" has gained prominence. Balkin (2018, 2020)[24] introduces the concept of "algorithmic governance," arguing that private digital platforms exercise quasi-sovereign powers by regulating speech, behaviour and data flows. Suzor (2019)[25] highlights the lack of transparency and due process in platform governance, where users are governed by opaque algorithmic systems. De Gregorio (2021)[26] further argues that constitutional norms must evolve to regulate digital ecosystems and ensure protection of fundamental rights in algorithm-driven environments.

In the Indian context, scholars focus on the evolving relationship between constitutional rights and digital state practices. Gautam (2023)[27] examines executive-led digital regulation under the Information Technology framework, highlighting tensions with separation of powers and legislative oversight. Menon (2021)[28] analyses the judiciary's expanding role in regulating digital platforms, noting both the risks of judicial overreach and the dangers of executive dominance. Rajagopal (2022)[29] critiques surveillance practices in India, particularly in relation to Aadhaar, internet shutdowns and state data collection, arguing that they raise serious concerns regarding constitutional accountability and informational privacy.

Comparative scholarship highlights distinct regulatory approaches. The United States follows a fragmented, sector-specific model, with limited federal regulation and reliance on judicial interpretation. Cases such as *Carpenter v. United States (2018)* illustrate the gradual constitutional recognition of digital privacy. In contrast, the European Union's General Data Protection Regulation

---

[23] A.V. Dicey, *Introduction to the Study of the Law of the Constitution* (1885).

[24] Jack M. Balkin, *Free Speech in the Algorithmic Society* (2018) and *The Fiduciary Model of Privacy* (2020).

[25] Nicolas Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (2019).

[26] Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (2021).

[27] Gautam, *Executive-Led Digital Regulation under the Information Technology Framework: Separation of Powers and Legislative Oversight Concerns* (2023).

[28] Menon, *Judicial Intervention in Digital Platform Governance: Risks of Judicial Overreach and Executive Dominance* (2021).

[29] Rajagopal, *Surveillance, Aadhaar and Internet Shutdowns in India: Constitutional Accountability and Informational Privacy Concerns* (2022).

(GDPR) represents a comprehensive, rights-based framework emphasising data subject control, accountability and strict compliance obligations. India's emerging framework under the Digital Personal Data Protection Act, 2023 reflects a state-centric model balancing governance efficiency with individual rights protection.

Across jurisdictions, a common theme emerges: digital technologies challenge traditional legal frameworks by decentralising authority among states, courts and private corporations. Scholars agree that classical constitutional doctrines must be reinterpreted to address algorithmic governance, cross-border data flows and digital surveillance. However, they differ on the appropriate regulatory response ranging from strong statutory regimes (EU), judicial innovation (US), to hybrid state-led models (India).

Overall, the literature indicates that while constitutional principles remain relevant, their application in the digital age requires significant reconfiguration to ensure effective protection of digital rights and personal data in an increasingly interconnected world.

Research Gap

While extensive scholarship exists on data protection regimes in India, Europe and the United States, much of it examines each jurisdiction in isolation rather than through a structured comparative constitutional framework. Existing literature primarily focuses on the General Data Protection Regulation (GDPR) in the EU, the fragmented sectoral privacy model in the US and India's emerging Digital Personal Data Protection Act, 2023, but rarely integrates these systems into a unified analytical model of digital rights protection.

In the Indian context, academic discussions largely centre on privacy jurisprudence post-*Justice K.S. Puttaswamy v. Union of India (2017)*, executive surveillance practices and statutory developments. However, there is limited critical assessment of how India's model compares with the rights-based EU framework and the market-driven US approach in terms of enforcement, accountability and user autonomy. This study addresses this gap by providing a comprehensive comparative evaluation of legal frameworks governing personal data protection across the three jurisdictions.

Research Objectives

i. To examine the evolution of legal frameworks governing the protection of personal data within the broader context of digital rights in India, the European Union and the United States.
ii. To analyse and compare the key principles, scope and enforcement mechanisms of data protection laws, including the GDPR in the EU, the Digital Personal Data Protection Act, 2023 in India and the sectoral privacy regime in the US.

iii. To evaluate the extent to which each jurisdiction balances individual privacy rights with state interests such as national security, economic growth and digital innovation.
iv. To assess the role of constitutional jurisprudence, judicial interpretation and regulatory authorities in shaping personal data protection frameworks across the selected jurisdictions.
v. To identify gaps, inconsistencies and challenges in existing legal regimes and propose comparative insights for strengthening global standards of digital rights protection.

Research Methodology

This study adopts a doctrinal and comparative legal research methodology to examine the legal frameworks governing the protection of personal data in India, the European Union and the United States. It relies primarily on analysis of constitutional provisions, statutory instruments and landmark judicial decisions, including the Indian Constitution, the General Data Protection Regulation (GDPR) and relevant US privacy laws and case law. Primary sources also include decisions of the Supreme Court of India and the Court of Justice of the European Union. Secondary sources such as scholarly books, peer-reviewed journal articles, policy papers and reports on digital governance are used to support critical analysis. The methodology focuses on interpretation, comparison and synthesis of legal principles to evaluate the effectiveness of existing data protection regimes.

Research Findings

The study finds that legal frameworks governing personal data protection in India, the European Union and the United States reflect fundamentally different regulatory philosophies, leading to varying levels of effectiveness in safeguarding digital rights. The European Union's GDPR emerges as the most comprehensive and rights-based framework, offering strong enforcement mechanisms, clear principles of data minimisation, purpose limitation and extensive rights for data subjects. In contrast, the United States follows a fragmented, sector-specific model, resulting in inconsistent protection and reliance on judicial interpretation rather than a unified statutory regime.

India's Digital Personal Data Protection Act, 2023 represents a developing framework that attempts to balance state interests with individual rights; however, the study finds that broad exemptions to the state, limited independent oversight and evolving enforcement mechanisms weaken its effectiveness. Across jurisdictions, the judiciary plays a crucial role in shaping privacy protections, particularly in landmark decisions such as *Puttaswamy* in India and *Carpenter v. United States* in the US. The research also highlights the increasing influence of private digital platforms as quasi-regulatory actors, raising concerns about accountability and transparency. Overall, the findings indicate a global imbalance

in digital rights protection, with significant gaps in harmonisation and enforcement.

Conclusion

The study concludes that the legal frameworks governing personal data protection in India, the European Union and the United States reflect distinct constitutional philosophies shaped by differing approaches to privacy, governance and market regulation. The European Union, through the GDPR, establishes a strong rights-based regime that prioritises individual autonomy, strict compliance obligations and robust enforcement mechanisms. The United States adopts a decentralised, sector-specific model that relies heavily on judicial interpretation and market flexibility, resulting in uneven protection of digital rights. India, through the Digital Personal Data Protection Act, 2023, represents an evolving framework that seeks to balance state interests, economic development and individual privacy; however, concerns remain regarding broad exemptions, limited independent regulatory oversight and enforcement challenges.

The comparative analysis reveals that while each jurisdiction addresses digital rights within its own constitutional and policy context, significant gaps exist in achieving uniform and comprehensive protection of personal data. The increasing role of technology companies and algorithmic systems further complicates traditional regulatory approaches. The study concludes that strengthening institutional safeguards, enhancing transparency and adopting harmonised global standards are essential to ensure effective protection of digital rights in an increasingly interconnected digital environment.

Recommendations

i. **Strengthen Parliamentary Role:** Parliament should enact a comprehensive and unified data protection and digital governance framework that clearly defines standards for data processing, surveillance, cross-border data transfers and algorithmic accountability. This would reduce excessive reliance on delegated legislation and ensure stronger democratic oversight over digital regulation.

ii. **Introduce Independent Oversight Mechanisms:** A specialised independent authority or Digital Data Protection Commission should be strengthened and made fully autonomous to monitor executive actions relating to surveillance, data collection and platform regulation, ensuring transparency and institutional accountability.

iii. **Enhance Transparency Requirements:** All government and regulatory bodies should be mandated to publish periodic transparency reports detailing data requests, surveillance activities and content moderation or blocking orders, thereby improving public trust and accountability.

iv. **Strengthen Judicial Standards:** Courts should consistently apply structured tests such as proportionality, necessity and procedural fairness

in digital rights cases, ensuring a balanced approach between state interests and individual privacy rights.

v. **Regulate Private Digital Platforms:** Large digital platforms should be subject to statutory obligations incorporating principles of transparency, non-discrimination, accountability and user grievance redressal, aligned with global standards such as the GDPR and Digital Services Act.

vi. **Capacity Building:** Continuous training programs for lawmakers, regulators and judicial officers should be introduced to improve understanding of emerging technologies, artificial intelligence and digital governance frameworks.

Scope For Future Research

Future research in the area of digital rights and personal data protection may focus on the evolving constitutional and regulatory challenges posed by emerging technologies such as artificial intelligence, machine learning–based surveillance, biometric identification systems and predictive policing mechanisms. As India continues to refine its Digital Personal Data Protection Act, 2023 and develop additional regulatory frameworks for digital governance, further studies may assess their practical impact on privacy protection, institutional accountability and constitutional balance.

Comparative research extending beyond India, the European Union and the United States to include jurisdictions in Asia, Africa and Latin America can provide broader insights into global regulatory diversity. Additionally, analysis of international frameworks governing cross-border data flows and digital trade agreements may help in understanding the need for harmonised global standards. Empirical studies examining the real-world implementation of surveillance practices, algorithmic decision-making and platform governance will also be essential to bridge the gap between legal theory and practical enforcement.

Limitations

This research is primarily doctrinal and relies on constitutional provisions, statutes, judicial pronouncements and existing academic literature. It does not incorporate empirical methods such as interviews, surveys, or field-based observation of data protection enforcement mechanisms. Consequently, the findings are based on secondary sources and legal interpretation rather than real-time institutional data.

Another limitation arises from the rapidly evolving nature of digital technologies and data protection laws, which may lead to subsequent legal developments after the completion of this study. Although a comparative framework is adopted, it is not exhaustive and focuses mainly on India, the European Union and the United States. Additionally, limited transparency of private digital platforms restricts deeper analysis of algorithmic governance practices and internal data processing mechanisms.

Bibliography

I. Classical and Theoretical Foundations

1. Locke, J. (1690). *Two Treatises of Government*. London: Awnsham Churchill.
2. Montesquieu, C. de Secondat, Baron de. (1748). *The Spirit of the Laws*. Paris: Barrillot & Fils.
3. Madison, J. (1788). *The Federalist Papers No. 47*. New York: J. & A. McLean.
4. Hamilton, A., Madison, J., & Jay, J. (1788). *The Federalist Papers*. New York: J. & A. McLean.
5. Dicey, A. V. (1885). *Introduction to the Study of the Law of the Constitution*. London: Macmillan.

II. Indian Constitutional Framework and Jurisprudence

1. Constituent Assembly Debates, Vol. VII (1948). Government of India.
2. *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
3. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
4. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
5. *Kaushal Kishor v. State of Uttar Pradesh*, (2023) SCC OnLine SC 133.
6. *Kesavananda Bharati v. State of Kerala*, AIR 1973 SC 1461.
7. *Indira Nehru Gandhi v. Raj Narain*, 1975 Supp SCC 1.

III. Statutory and Regulatory Frameworks

1. Information Technology Act, 2000 (India).
2. Digital Personal Data Protection Act, 2023 (India).
3. IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 & 2023.
4. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
5. Digital Services Act, EU (2022/2065).
6. Communications Decency Act, Section 230, 47 U.S.C. § 230.
7. Investigatory Powers Act, 2016 (UK).
8. Online Safety Act, 2023 (UK).

IV. Comparative Jurisprudence

United States

1. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
2. *Riley v. California*, 573 U.S. 373 (2014).
3. *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017).
4. *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).

Europe / UK

1. *Google Spain v. AEPD*, C-131/12 (2014).
2. *Schrems I*, C-362/14 (2015).
3. *Schrems II*, C-311/18 (2020).
4. *Big Brother Watch v. UK*, ECHR (2021).

V. Digital Constitutionalism and Governance

1. Balkin, J. M. (2018). *Fixing Social Media's Grand Bargain*. Hoover Institution.
2. Suzor, N. (2019). *Lawless: The Secret Rules That Govern Our Digital Lives*. Cambridge University Press.
3. De Gregorio, G. (2021). *Digital Constitutionalism in Europe*. Cambridge Journal of Comparative & International Law.
4. Celeste, E. (2020). *Digital Constitutionalism*. Routledge.

VI. Indian Scholarship

1. Bhatia, G. (2019). *The Transformative Constitution*. HarperCollins India.
2. Chandrachud, C. (2019). *Republic of Rhetoric*. Penguin.
3. Gautam, S. (2023). "Reimagining Separation of Powers in Digital India." *Indian Journal of Constitutional Law*.
4. Rajagopal, A. (2022). "Digital Surveillance and Constitutional Accountability." *NUJS Law Review*.
5. Menon, N. (2021). "Judicial Activism and Digital Governance." *Indian Law Review*.

VII. Policy Reports and International Materials

1. Ministry of Electronics and IT (MeitY). (2023). *DPDP Act Explanatory Note*. Government of India.
2. European Commission. (2022). *Digital Services Act Proposal*. Brussels.
3. UN Human Rights Council. (2021). *Right to Privacy in the Digital Age (A/HRC/48/31)*.
4. OECD. (2022). *AI Principles and Governance*. Paris.

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618