CONSTITUTIONAL APPROACHES TO DATA PROTECTION AND PRIVACY IN THE AGE OF SURVEILLANCE: A COMPARATIVE ANALYSIS OF INDIA, THE USA AND THE EUROPEAN UNION

Abhimanyu Paliwal, Maharashtra National Law University Nagpur

Sidra Ahmed, Maharashtra National Law University Nagpur

ABSTRACT

In today's digital world as governments and corporations expand their surveillance capabilities, data protection and privacy has become a crucial concern. Different legal systems take unique constitutional approaches to safeguarding personal data, reflecting their historical, cultural, and legal priorities. This study examines how India, the United States of America, and the European Union address these challenges. In the U.S., privacy rights have evolved through Supreme Court rulings, but the absence of a comprehensive federal data protection law leaves gaps in enforcement. The European Union's General Data Protection Regulations (GDPR) sets a global standard for strong privacy protections, prioritizing individual rights and strict compliance. India, recognizing privacy as a fundamental right, is still developing a comprehensive legal framework to balance innovation with data security. This paper explores the effectiveness of these approaches in addressing modern surveillance challenges and how each legal system adapts to evolving threats. By comparing these models, it aims to highlight best practices and potential reforms that can strengthen global data protection while respecting regional legal traditions. Ultimately, this research contributes to the ongoing debate on how to balance privacy, security, and technological progress in an increasingly interconnected world.

Keywords: Data Protection, Privacy Rights, Constitutional Law, Comparative Legal Frameworks

1. INTRODUCTION

> *"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."*[1]

In the digital age, where vast amount of personal data is stored in the cyberspace, the concept of right to privacy must be revisited. There is a necessity to move beyond the traditional understanding of the right to privacy and examining it through the lens of data surveillance. The data stored is linked to an individual's identity, reputation, and personality, and its breach may result into breach of fundamental rights.

The United States, the European Union, and India represent three distinct legal traditions with varying perspectives on data privacy. In the United States, the concept of privacy has evolved from early common law principles, emphasizing personal security and liberty, to a complex web of federal and state regulations. Landmark decisions such as *Griswold v. Connecticut*[2] and *Roe v. Wade*[3] established privacy rights within specific constitutional contexts, yet the regulatory landscape remains fragmented. Modern privacy challenges, exacerbated by advanced surveillance technologies and data collection practices, continue to test the robustness of American privacy protections.

In contrast, the European Union has adopted a comprehensive and cohesive approach through the General Data Protection Regulation (GDPR)[4]. The GDPR embodies principles such as transparency, accountability, and consent, setting a high standard for data protection and privacy. Its emphasis on individual rights and regulatory oversight aims to address the challenges posed by algorithmic decision-making and the growing capabilities of data-driven technologies. The European model offers a significant contrast to the more decentralized approach seen in the United States.

India, having recently enacted the Digital Personal Data Protection (DPDP) Act, is in the process of developing a structured framework for data protection. The DPDP Act reflects an

[1] Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160.
[2] Griswold v. Connecticut, 381 U.S. 479 (1965).
[3] Roe v. Wade, 410 U.S. 113 (1973).
[4] *General Data Protection Regulation, Regulation (EU) 2016/679.*

attempt to align with global standards while addressing local concerns about data privacy and security. This recent legislative development follows a landmark judgment by the Supreme Court of India recognizing the right to privacy as a fundamental right under the Constitution. However, the practical implementation of this right and the effectiveness of the new regulatory framework remain subjects of ongoing scrutiny and debate.

The primary objective of this paper is to conduct a comparative analysis of the constitutional approaches to data protection and privacy in the United States, the European Union, and India. By examining the historical development, current legislative frameworks, and the challenges each region faces, the paper aims to elucidate the strengths and limitations of these approaches in safeguarding privacy in the digital age.

2. EVOLUTION OF THE RIGHT TO PRIVACY

The right to privacy has long been a fundamental aspect of human dignity. Historically, it has been understood as the "right to be let alone", the right to be free from unwarranted governmental interference, and the right to make personal choices without external intrusion.[5] The historical evolution of privacy rights can be traced back to ancient legal traditions. In ancient Indian law, both Hindu and Islamic legal texts emphasized the protection of individual integrity and property, implicitly recognizing the importance of privacy. Similarly, early legal frameworks in Europe addressed aspects of privacy protection. The Judicial Peace Act of 1831 highlighted the need for confidentiality in judicial records, while the Swedish Parliament, in 1766, enacted one of the earliest laws aimed at safeguarding private records. Norway also recognized privacy rights, with its Criminal Code incorporating provisions to prevent unwarranted intrusion into private life.[6]

A key distinction in privacy discourse today is between corporeal privacy and informational privacy. Traditionally, privacy was primarily concerned with protecting bodily integrity, personal property, and physical space from unauthorized intrusion. In contrast, with the rise of the digital age, the scope of privacy has expanded to include data protection and informational self-determination. This form of privacy, often associated with classical liberalism, emphasized safeguarding individuals from state surveillance and interference. Informational privacy

[5] Li, Q. (2023). Neil Richards, Why Privacy Matters. *Edinburgh Law Review*, *27*(1), 125–127. https://doi.org/10.3366/elr.2023.0822
[6] Glancy, D. (1979). The Invention of the Right to Privacy.

addresses the protection of personal data, digital footprints, and online identities. This shift reflects the growing importance of data security in an era where vast amounts of personal information are stored, processed, and shared digitally.

One of the most influential modern interpretations of privacy comes from Alan Westin's seminal work, Privacy and Freedom (1967)[7], where he defines privacy as an individual's right "*to control, edit, manage, and delete information about themselves and decide when, how, and to what extent such information is shared with others*." This perspective acknowledges the evolving nature of privacy concerns, moving beyond mere physical intrusion to include the digital realm.

With rapid advancement of technology and mass surveillance, privacy has come into the spotlight, necessitating legal frameworks that protect personal data from both governmental and corporate misuse. This evolution reflects a broader shift from traditional notions of privacy as mere physical autonomy to a more nuanced understanding that includes control over personal information in the digital space.

3. DATA PRIVACY MODELS ACROSS THE BORDERS

Across the globe, countries have adopted distinct models of data protection, primarily categorized into two main approaches: the European Model and the American Marketplace Model. The European approach, particularly embodied in the GDPR[8], is rights-based and offers robust protections for privacy and personal data. In contrast, the United States lacks a single comprehensive data protection law, opting instead for a sector-specific regulatory framework. U.S. privacy protections vary by state and industry, with federal laws like the Electronic Communications Privacy Act of 1986 and the Gramm-Leach-Bliley Act (GLBA) addressing government and financial data separately. Meanwhile, private sector data practices are largely governed by the Federal Trade Commission Act. Both models have informed the development of data protection laws in other jurisdictions, including India, which has drawn from these

[7] Leubsdorf, J., & Westin, A. F. (1968). Privacy and Freedom. *Harvard Law Review*, *81*(6), 1362. https://doi.org/10.2307/1339271.
[8] *Regulation (EU) 2016/679 of the European Parliament and of the Council.*

frameworks in crafting its own regulations.[9]

The GDPR, implemented by the European Union in 2018, represents a milestone in data privacy law, setting forth principles such as lawfulness, fairness, transparency, and accountability. It grants individuals rights over their personal data and imposes obligations on data controllers, emphasizing the importance of data protection by design and the need for Data Protection Impact Assessments (DPIAs) to manage privacy risks. The regulation's extraterritorial scope ensures that even organizations outside the EU are subject to its requirements when processing EU citizens' data.[10]

In contrast, the U.S. continues to rely on a fragmented sectoral approach, with no overarching federal privacy law. Noteworthy legislation includes the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data and the (GLBA for financial information. Recent efforts indicate growing momentum toward federal privacy legislation, with states like California leading the way through laws like the California Consumer Privacy Act (CCPA), which grants residents specific rights over their personal information.[11]

Canada has also developed a strong privacy framework with the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs private-sector organizations and mirrors several principles found in the GDPR, such as the emphasis on consent and data accuracy. However, provinces like Quebec and British Columbia have enacted additional privacy laws, demonstrating the interplay between federal and provincial regulations in Canada.[12]

The Asia-Pacific region displays diverse privacy laws. Japan's Act on the Protection of Personal Information (APPI) focuses on fairness and purpose limitation, while Australia employs a sectoral approach with its Privacy Act of 1988. India, with its recently introduced Personal Data Protection Act aims to establish comprehensive data protection standards and set up a Data Protection Authority. Additionally, regional efforts like the Asia-Pacific

[9] Bradford, L., Aboy, M., & Liddell, K. (2020). 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. https://doi.org/10.1093/jlb/lsaa055.
[10] Desafíos, E., & Implicaciones, E. (2018). Unification of Personal Data Protection in the European Union: Challenges and Implications.
[11] Baik, J. (2020). Data Privacy Against Innovation or Against Discrimination?: The Case of the California Consumer Privacy Act (CCPA). *Consumer Law eJournal*. https://doi.org/10.1016/j.tele.2020.101431.
[12] Trinxet, S. (2015). Personal Information Protection and Electronic Documents Act.

Economic Cooperation (APEC) Privacy Framework seek to harmonize privacy standards across the region.[13]

Globally, data privacy laws are shaped by regional legal traditions, historical developments, and technological advancements. The GDPR has set the benchmark for comprehensive privacy regulation, influencing global standards, while the U.S. continues to manage a decentralized system. As privacy concerns grow, especially with rapid technological innovations, global cooperation remains essential to address these challenges.

4. INDIAN CONSTITUTIONAL APPROACH

India's constitutional stance on data protection and privacy has undergone significant evolution, shaped by both judicial pronouncements and legislative developments. The Supreme Court's judgment in *Justice K.S. Puttaswamy v. Union of India*[14], was pivotal in establishing privacy as a fundamental right. In this case, the court held that the right to privacy is intrinsic to the right to life and personal liberty under Article 21.

Historically, privacy was not explicitly recognized as a fundamental right in India. Early cases such as *M.P. Sharma v. Satish Chandra*[15] and *Kharak Singh v. State of Uttar Pradesh*[16] denied the existence of a constitutional right to privacy. In *M.P. Sharma*, the Supreme Court ruled that the framers of the Constitution did not intend to include a right to privacy, citing the lack of provisions akin to the U.S. Constitution's Fourth Amendment. Similarly, in *Kharak Singh*, the Court refused to recognize privacy as a right under Article 21, though dissenting opinions in these cases laid the groundwork for future developments.

The *Puttaswamy* judgment marked a turning point by overturning these precedents and explicitly recognizing privacy as a fundamental right under Article 21. The Court emphasized that privacy encompasses the protection of personal data and informational privacy, establishing a basis for future legal frameworks aimed at curbing intrusive data collection and surveillance practices.

[13] Greenleaf, G. (2007). Asia-Pacific Developments in Information Privacy Law and its Interpretation. *Public International Law eJournal*. https://doi.org/10.2139/SSRN.952578.
[14] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[15] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[16] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

4.1. Judicial Evolution of Privacy Rights

Various judicial pronouncements have shaped the contours of the right to privacy, balancing individual liberties against state interests. A pivotal case in this evolution is *People's Union for Civil Liberties (PUCL) v. Union of India*[17], where the Court addressed the issue of telephone tapping under Section 5(2) of the Telegraph Act, 1985. The Court held that such surveillance infringed upon the right to privacy protected under Article 21 of the Constitution, emphasizing that any restriction on this right must align with Article 17 of the International Covenant on Civil and Political Rights, 1966. This judgment underscored the necessity for procedural safeguards to prevent arbitrary violations of privacy.

In *Gobind v. State of Madhya Pradesh*[18], the Court acknowledged the implicit nature of the right to privacy within the realm of personal liberty under Article 21. However, it also noted that this right is not absolute and must be weighed against compelling state interests. Similarly, in *Malak Singh v. State of Punjab & Haryana*[19], the Court examined the legitimacy of police surveillance on habitual offenders. While recognizing the necessity of such measures for maintaining public order, the Court cautioned that surveillance must not infringe upon the freedoms guaranteed under Articles 21 and 19(1)(d), thereby highlighting the delicate balance between individual rights and societal security.

The Court's stance on evidence obtained through questionable means was articulated in *Puran Mal v. Director of Inspection (Investigation) of Income Tax, New Delhi*[20]. Here, it was determined that evidence collected from illegal searches should not be excluded solely on the grounds of privacy infringement, especially in the absence of an explicitly defined fundamental right to privacy at that time. This perspective was further elaborated in *State of Punjab v. Baldev Singh*[21], where the Court emphasized the mandatory nature of procedural safeguards during searches under Section 50 of the Criminal Procedure Code. However, it also allowed for the admissibility of evidence obtained in violation of these procedures, reflecting a pragmatic approach to the administration of justice.

[17] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
[18] Gobinda v. State of M.P., (1975) 2 SCC 148.
[19] Malak Singh v. State of P&H, (1981) 1 SCC 420.
[20] Puran Mal v. Director of Inspection (Investigation) of Income Tax, New Delhi, (1974) 1 SCC 345.
[21] State of Punjab v. Baldev Singh, (1999) 6 SCC 172.

In *V.S. Kuttan Pillai v. Ramakrishnan*[22], the Court upheld the issuance of general warrants for document searches, reasoning that state interests could, in certain circumstances, outweigh individual privacy concerns. Conversely, in *District Registrar and Collector v. Canara Bank*[23], the Court struck down an amendment to the Indian Stamp Act that permitted the search and seizure of private documents without just cause, thereby reinforcing the sanctity of privacy. The tension between privacy and public interest was also evident in *PUCL v. Union of India*[24], where the Court ruled that the electorate's right to information about a political candidate's criminal record and assets superseded the candidate's privacy claims. This decision underscored the principle that privacy rights may be curtailed when outweighed by a compelling public interest.

In the realm of personal matters, *Sharda v. Dharmpal*[25] addressed the issue of medical examinations in divorce proceedings. The Court held that such examinations, when necessary for public policy purposes, could override individual privacy concerns. Similarly, in *R. Rajagopal v. State of Tamil Nadu*[26], the Court affirmed the right of individuals to protect the privacy of their personal lives. However, it also recognized that publishing a public figure's autobiography does not constitute a privacy violation unless it delves into private matters unrelated to public interest. Lastly, in *Mr. A v. Hospital B*[27], the Court dealt with the disclosure of a patient's medical condition, ruling that sharing such information with those directly involved did not violate privacy rights, especially when it served a greater societal good.

Eventually, the position was settled by the 9 judges bench judgment in 2017. The judges unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution. In the year 2012, Justice K.S. Puttaswamy filed a petition in 2012, challenging the constitutionality of the Aadhaar Act on privacy grounds. The government, relying on the *M.P. Sharma* and *Kharak Singh* rulings, argued against privacy as a fundamental right. As a result, the issue of whether right to privacy is a fundamental right, was referred to a larger bench. The judgment clarified that privacy is indeed intrinsic to personal liberty, refuting the government's claims. The judgment paved the way for a larger legal debate as to how data

[22] V.S. Kuttan Pillai v. Ramkrishnan, (1980) 1 SCC 261.
[23] District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496.
[24] People's Union for Civil Liberties (PUCL) v. Union of India, (2003) 4 SCC 399.
[25] Sharada v. Dharmpal, (2003) 4 SCC 493.
[26] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[27] A v. Hospital B, (1997) 2 SCC 716.

protection laws should evolve to safeguard individual privacy in the digital age.[28]

Collectively, these judgments reflect the Indian judiciary's nuanced approach to the right to privacy, acknowledging its fundamental nature while permitting reasonable restrictions in the interest of public welfare and security. The courts have consistently endeavored to strike a balance between individual freedoms and state responsibilities, ensuring that any encroachment on privacy is justified, proportionate, and accompanied by adequate safeguards against abuse.

4.2. Legislative Framework for Data Protection

India's legislative framework derives its authority from the division of legislative subjects between the Union and the States, as outlined in Part IX of the Constitution. Articles 246 and 248 delineate the subjects on which Parliament and State legislatures can legislate. Data protection and privacy laws are not explicitly mentioned in the Union List (List I), State List (List II), or Concurrent List (List III). However, Article 248 and Entry 97 of the Union List, which pertain to Parliament's residuary powers, allow for the legislature to enact laws on matters not specifically enumerated in the State or Concurrent Lists. In the *H.S. Dhillon* case[29], the Supreme Court affirmed the exclusive legislative power of the Parliament over subjects not covered by the State or Concurrent Lists. As data protection and privacy are modern issues not explicitly listed, they fall under Parliament's legislative domain.

The Personal Data Protection Bill, 2019, which later evolved into the Digital Personal Data Protection (DPDP) Act, 2023, is India's first cross-sectoral data protection law. The legislative intent behind this law was shaped by the recommendations of the Srikrishna Committee (2018), which advocated for a comprehensive framework similar to the European Union's General Data Protection Regulation (GDPR).[30]

The DPDP Act aims to regulate the collection, processing, and storage of personal data across sectors. It establishes several key provisions: it mandates that individuals must be informed about data collection practices and must provide explicit consent; it imposes specific obligations on data fiduciaries regarding data security and accuracy; it confers upon data

[28] Ran, S. (2023). A Comparative Examination of Privacy Jurisprudence: India and the USA. *Russian Law Journal*. https://doi.org/10.52783/rlj.v11i1s.362.
[29] H.S. Dhillon v. Union of India, (1972) 2 SCC 33.
[30] *Srikrishna Committee, Report on Comprehensive Data Protection Framework.* (2018).

principals the rights to access, correct, erase, and port their personal data; it restricts cross-border transfers of sensitive data; and it provides for the creation of a Data Protection Authority (DPA) to oversee and enforce these rules.[31] While the DPDP Act draws inspiration from the GDPR, it also incorporates unique features tailored to India's governance needs, including exemptions for certain state functions such as law enforcement and national security and innovative mechanisms like "consent managers" to help individuals manage their consent preferences.

While the Indian approach borrows heavily from the GDPR, its structure is also distinct, particularly in its handling of state functions and exemptions. For instance, certain government activities, like law enforcement and national security, are exempted from the full scope of the law.[32] The DPDP Act also introduces mechanisms like "consent managers", intermediaries who facilitate individuals in managing their consent preferences with various businesses.

5. AMERICAN CONSTITUTIONAL APPROACH

The American constitutional framework on data privacy has developed through historical legal interpretations, despite privacy not being explicitly mentioned in the U.S. Constitution. Key privacy protections have emerged through case laws and particularly under the Fourth and Fourteenth Amendments. As technology continues to advance, especially in the digital era, the legal system has struggled to keep pace with emerging challenges related to data collection and surveillance.

The modern concept of privacy in U.S. jurisprudence was first articulated in the seminal 1890 article The Right to Privacy by Warren and Brandeis, which advocated for a "right to be let alone" as fundamental to personal liberty.[33] The U.S. Supreme Court acknowledged privacy as a constitutional right for the first time in *Griswold v. Connecticut*[34], recognizing a right to marital privacy found within the "penumbras" of other constitutional guarantees, such as those in the Bill of Rights. This concept was further expanded in *Roe v. Wade*[35], where the Court

[31] Bhushan, V. (2024). Empowering Individuals: A Deep Dive into the Digital Personal Data Protection Act, 2023. *International Journal of Advanced Research*. https://doi.org/10.21474/ijar01/18799.
[32] Rahul, R. (2024). Outlining Principle of Data Protection through various Indian Legislations with comparison to The Digital Personal Data Protection Act, 2023. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2024.v06i04.25534.
[33] Warren, supra, note 1, 1.
[34] Griswold v. Connecticut, 381 U.S. 479 (1965).
[35] Roe v. Wade, 410 U.S. 113 (1973).

held that the Fourteenth Amendment's Due Process Clause protects a woman's right to privacy regarding her decision to have an abortion, thus broadening privacy protections to include aspects of personal autonomy.

Although these landmark cases laid the foundation for privacy rights, the rise of digital technologies has introduced new legal complexities. The Fourth Amendment, which protects citizens from unreasonable searches and seizures, is central to ongoing debates about privacy in the digital age. The shift was first reflected in *Carpenter v. United States*[36], where the Supreme Court ruled that the government's collection of cell phone records, which enabled tracking of a person's movements, constituted a search under the Fourth Amendment. This marked a pivotal recognition that technological advancements necessitate reevaluating traditional legal interpretations to protect citizens' privacy.

The increasing use of surveillance technologies and data collection tools has also raised significant privacy concerns for marginalized communities, who often face disproportionate surveillance. Technologies like reproductive health tracking apps and location-based services, used by both government agencies and private companies, amass vast amounts of sensitive data, exacerbating privacy risks. For example, in the aftermath of the Supreme Court's *Dobbs* decision[37], which overturned *Roe v. Wade*, data collection practices by private companies tracking reproductive health or location data have sparked concerns about privacy erosion, particularly for women and minorities who are already vulnerable to intensified monitoring in the absence of comprehensive legal protections.

5.1. Sector specific legislations

The U.S., presently relies on sector-specific regulations like the Health Insurance Portability and Accountability Act (HIPAA)[38] for health data or the Children's Online Privacy Protection Act (COPPA)[39] for children's privacy. However, there is no comprehensive legislation for addressing data privacy in the USA.[40] Although the Supreme Court has addressed certain privacy concerns, the rapid evolution of technology continues to outpace the judiciary's ability

[36] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[37] Dobbs v. Jackson Women's Health Organization, 597 U.S. (2022).
[38] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936
[39] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.
[40] Bradford, supra, note 9, 3.

to provide comprehensive solutions.[41] The Fourth Amendment alone cannot address all the nuances of modern surveillance and data collection. To fill this gap, legislative action has been proposed, most notably in the form of the American Data Privacy Protection Bill.

The proposed federal privacy law aims to establish robust data protection measures by incorporating key principles that ensure individuals' privacy rights are safeguarded. One of the primary principles is data minimization, which mandates that organizations collect only the personal data strictly necessary for the service they provide. By limiting data collection, this approach reduces the risks of privacy violations and minimizes the chances of misuse or unauthorized access to personal information.[42]

Another crucial aspect of the law is transparency, which requires companies to clearly disclose how they collect, process, store, and share personal data. By enforcing greater transparency, individuals will have a better understanding of how their data is being utilized, enabling them to make informed decisions and allowing for greater regulatory oversight. Additionally, the law seeks to empower consumers with fundamental rights, such as the ability to access, correct, and delete their personal data. In a digital environment where data flows are often complex and opaque, these rights would give individuals more control over their personal information, ensuring they have a say in how their data is managed and used.

The ADPPA, if enacted, would mark a significant step towards aligning American privacy laws with the realities of digital surveillance and data collection, providing more robust protections to individuals against both governmental and corporate misuse of data.

6. EUROPEAN CONSTITUTIONAL APPROACH

In the European Union, driven by a combination of historical, constitutional, and technological factors, the right to privacy and data protection has been enshrined as a fundamental right. The EU Charter of Fundamental Rights enshrines both the right to privacy and the right to data protection as distinct rights.[43] Article 8 of the Charter specifically introduces a stand-alone right to data protection, which is unique to the EU legal order. This right is separate from the right to privacy, providing individuals with enhanced control over their personal data and addressing

[41] Bradford, supra, note 9, 3.
[42] DiPersio, D. (2022). Data Protection, Privacy and US Regulation.
[43] McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4. https://doi.org/10.1177/2053951716686994.

power asymmetries between individuals and data processors.[44] The General Data Protection Regulation (GDPR)[45] serves as the most prominent legal instrument in this domain, reflecting a shift from the traditional concept of privacy as a negative right (the right to be left alone) to a positive right, ensuring the protection of personal data. This transition emphasizes individual autonomy, human dignity, and informational self-determination, with its roots in historical experiences, such as the misuse of personal data during World War II.[46] Landmark European legal cases, such as the German Federal Constitutional Court's decision in the *Volkszahlungsurteil* case, recognized the need for strong safeguards against mass data collection and established the right to "informational self-determination."[47] This constitutional interpretation focuses on protecting individuals from excessive state and corporate surveillance, placing human dignity at the core of data protection.

The European approach treats data protection as both a personal and public good, essential to maintaining individual autonomy in the face of increasing surveillance and data-driven decision-making by both public authorities and private corporations.[48] The GDPR incorporates principles such as transparency, accountability, and the requirement of consent, ensuring individuals have control over how their data is processed. Automation and the rise of AI technologies have further heightened the need for robust data protection laws, as the potential for abuse of personal information has expanded with the growth of algorithmic decision-making.

6.1. Data Protection as a Personal and Public Good

In Europe, data protection fundamentally aims to safeguard individuals from the dangers posed by the misuse of their personal information. This legal protection enables individuals to retain control over their personal data, thereby preserving their privacy, identity, and autonomy in the digital world. However, data protection also serves a wider public interest by regulating the collection, processing, and sharing of personal data, fostering transparency and

[44] Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3, 222-228. https://doi.org/10.1093/IDPL/IPT017.
[45] General Data Protection Regulation, Regulation (EU) 2016/679.
[46] Voss, G. (2017). European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. *Business Lawyer*, 72, 221-233.
[47] Fischer-Hübner, S. (2011). Census 2011 and Privacy, 53, 3 - 4. https://doi.org/10.1524/itit.2011.9067.
[48] Kokott, supra, note 46, 11.

accountability.[49] This regulation is critical for maintaining public trust in digital platforms, public services, and technological innovations.

The importance of data protection is heightened by the increasing surveillance conducted by both government bodies and corporations. While governments collect personal data to enhance security, companies often gather vast amounts of information to fuel data-driven business models for profit. The European approach aims to balance these competing interests by imposing stringent regulations on data collection and use, ensuring that individual rights are not sacrificed for economic or security objectives.

The General Data Protection Regulation (GDPR) is built on key principles such as transparency, accountability, and consent, all of which empower individuals to take control of their personal data.[50] Transparency is a fundamental requirement under the GDPR, ensuring that organizations clearly inform individuals about how their data is being collected, processed, stored, and shared. This principle extends to disclosing the specific purposes of data collection and informing individuals about their rights, including access to and correction of their personal information. By enforcing transparency, GDPR aims to prevent the opaque handling of data, allowing individuals to understand how their personal information is being used and giving them the ability to make informed decisions.

Equally important is accountability, which mandates that organizations take full responsibility for the data they collect and process. GDPR requires companies to implement stringent compliance measures, including appointing Data Protection Officers (DPOs), conducting data audits, and performing impact assessments to mitigate risks. Organizations must also be able to demonstrate compliance with data protection laws, ensuring they uphold privacy rights. The regulation imposes heavy fines for non-compliance, reinforcing the importance of prioritizing data protection and security in all organizational practices.

Consent is another cornerstone of the GDPR, giving individuals greater control over their personal data. Organizations must obtain explicit and informed consent before collecting or processing any personal information, and individuals retain the right to withdraw their consent

[49] Desafios, supra, note 10, 4.
[50] Hoofnagle, C., Van Der Sloot, B., & Borgesius, F. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28, 65 - 98. https://doi.org/10.1080/13600834.2019.1573501.

at any time. To ensure fairness, consent must be freely given, specific, and unambiguous, reflecting a strong commitment to individual autonomy. This principle empowers individuals to make active choices about their data, reinforcing the idea that personal information belongs to the data subject and not the organization handling it.

7. COMPARATIVE ANALYSIS

The digital era, marked by pervasive surveillance and technological innovation has necessitated robust legal frameworks that protect individual privacy and data in a landscape. A comparative look at the United States, the European Union, and India reveals three distinct approaches shaped by unique constitutional traditions and socio-political priorities.

In the United States, privacy rights have largely evolved through judicial interpretations of the Fourth Amendment and the Due Process Clause. Landmark decisions such as *Warren v. Brandeis* and *Katz v. United States*[51] have historically underscored the need to safeguard individuals from intrusive state actions. However, the U.S. system relies on a patchwork of sector-specific laws like HIPAA for health data and COPPA for children's privacy which, while providing critical protections, result in a fragmented regime that struggles to address the comprehensive data landscape in today's digital world.[52]

Conversely, the European Union has embraced a holistic statutory approach with the General Data Protection Regulation (GDPR) at its core. The GDPR codifies data protection as a fundamental right tied to human dignity and autonomy, imposing clear obligations on organizations regarding data minimization, consent, and the right to erasure.[53] This unified framework not only sets a high global standard but also challenges businesses with its rigorous compliance demands.

India, at a nascent stage, presents a hybrid model that has rapidly evolved over recent years. The landmark *Puttaswamy v. Union of India* judgment established privacy as a fundamental right under Article 21, thereby mandating protection from both governmental and corporate intrusions. Building on this judicial foundation, India is developing a comprehensive legislative framework, illustrated by the Digital Personal Data Protection Act, that seeks to balance robust

[51] Katz v. United States, 389 U.S. 347 (1967).
[52] Bradford, supra, note 9, 3.
[53] Baumer, D., Earp, J., & Poindexter, J. (2004). Internet privacy law: a comparison between the United States and the European Union. *Comput. Secur.*, 23, 400-412. https://doi.org/10.1016/j.cose.2003.11.001.

individual rights with the state's economic and security concerns. Nonetheless, practical challenges, including limited public awareness and enforcement issues persist.

Collectively, these regimes reflect differing strategies: the U.S. emphasizes judicially derived rights with sector-specific protections, the EU provides a uniform and stringent statutory model, and India navigates a transitional path by integrating constitutional principles with emerging legislation. Understanding these diverse approaches is crucial for shaping future reforms that harmonize privacy protection with the demands of modern governance.

8. SUGGESTIONS

It is advisable for all stakeholders to work together in aligning privacy standards on a global level. By joining forces, they can bridge the gaps between various regional and national regulations, creating a more consistent framework for data protection. Additionally, exploring international treaties and agreements could help establish a common set of principles that honor cultural differences while providing reliable privacy safeguards for ever. Following are the suggestions:

1. Global Harmonization: Promote collaboration between nations to establish unified data protection standards that respect constitutional frameworks.

2. Surveillance Oversight: Strengthen constitutional safeguards against mass surveillance with judicial oversight and clear limitations on data collection.

3. Technological Adaptability: Constitutions should include adaptable legal frameworks that evolve with technological advancements in surveillance.

4. Public Awareness: Encourage educational campaigns to raise awareness about privacy rights in the digital age, fostering informed civic engagement.

5. Cross-border Data Flows: Enhance cooperation between regulatory bodies for managing cross-border data flows, ensuring privacy is protected across jurisdictions.

By embracing these measures, stakeholders can create a balanced and forward-looking privacy framework that upholds individual rights while adapting to evolving technological and regulatory landscapes. A collaborative and informed approach will ensure stronger data

protection and greater trust in the digital age.

9. CONCLUSION

The age of surveillance has brought unique challenges with different regions adopting varied responses to address and regulate its impact. The different approaches are rooted in their constitutional, historical and cultural priorities. The European Union, through the GDPR, recognizes data protection as a fundamental right, emphasizing transparency, accountability, and individual control. The United States, on the other hand, relies on a patchwork of sector-specific regulations and Fourth Amendment protections, resulting in a fragmented privacy framework. India, influenced by the landmark Puttaswamy judgment, is shaping its approach with the DPDP Act, 2023, which seeks to balance individual privacy with state and corporate interests.

As surveillance technologies advance, the tension between privacy, national security, and economic growth becomes more pronounced. While governments argue that data collection is essential for law enforcement and national security, unchecked surveillance poses serious risks to civil liberties. The challenge lies in crafting legal frameworks that protect individual rights without stifling innovation. Global cooperation and harmonization of privacy laws are increasingly necessary to address cross-border data flows and ensure uniform protections. The need for stringent safeguards, independent oversight, and strong enforcement mechanisms remains critical. Moving forward, striking a balance between privacy rights and state imperatives will require continuous legal evolution, international collaboration, and a commitment to upholding constitutional principles in the digital era.