Volume 45, May 2026 ISSN 2581-5504

"Privacy Rights in The Digital Era - A Comparative Analysis of India, The United States, and The European Union"

Mayank Arora
Research Scholar
Soban Singh Jeena University
Almora, Uttarakhand

ABSTRACT

The digital technologies coupled with the rapid growth of artificial intelligence, biometric governance, and data-driven economies have made privacy one of the most important constitution-related issues in the 21st century. There's a concern about surveillance and the misuse of personal data in the era where information is almost always collected, processed, stored, and transferred by both State and non-State actors. This research examines the digital privacy frameworks of India, the US and the E.U. through a comparison of their Constitutions, laws, and policies. This comparative study also covers the development of privacy laws in India which confirmed that privacy is a fundamental right in the Constitution of India. This research will look at the Digital Personal Data Protection Act, 2023, taking into account international privacy standards. This study analyzes the development of India's privacy laws, the sector-based privacy laws in the US, and the rights-based privacy laws of the EU in the context of the General Data Protection Regulation (GDPR). Through a comparative approach, the study will examine the issues of surveillance and data protection, as well as the governance of algorithms and the accountability of institutions in relation to the rights of individuals. This study will present the argument that the protection of digital privacy is especially important in a democratic country, and although India has achieved a lot in this regard, a lot is still left to be desired in this area, especially relating to the rights and the powers of the government and the mechanisms of implementation. This study achieves the argument that democratic control, international engagement, and the balance of technology regulation and the Constitution will achieve the protection of digital privacy in India.

Keywords: *Digital Privacy, Right to Privacy, Data Protection, GDPR, DPDP Act, Informational Privacy, Surveillance, Constitutional Law, Digital Governance, Comparative Constitutionalism.*

1. INTRODUCTION

The digital age has thoroughly disrupted the ways in which people connect, transact, and organize. Novel ways of producing and distributing information, having to do with AI, the cloud, biometrics and social media, bring with them increased concerns around digital privacy and the freedom to control one's own information. The 21st century includes a vast, complex digital structure in which

Volume 45, May 2026 ISSN 2581-5504

every interaction generates data. Of the many rights and concerns for individuals in a modern, functioning democracy, the right to privacy is paramount.[1]

The concept of privacy has traditionally been associated with protection from uninvited access to one's personal space. The threats to privacy that arise from modern technologies expand unsettling access to one's information and control over one's decisions and communications to a person's ability to protect their data. The ability of governments and corporations to collect, retain, and monetize personal data enables surveillance and data-driven practices that manipulate and control behavior and leave individuals vulnerable to identity theft and the loss of freedom and expression.

Digital privacy is connected to many Constitution values, e.g., dignity, liberty, autonomy, and equality. Limitless surveillance discourages political and social activities, which is detrimental to democratic governance. Likewise, social exclusion and discrimination create equity gaps that can be reinforced by artificial intelligence and algorithmic social media. As a result, most constitutional democracies view privacy not simply as an individual choice, but as a legitimate democratic right.[2]

Different countries have different techniques for digital privacy. The GDPR interprets the right to privacy and the right to digital safety as inseparable to human dignity and democratic governance, and adopts a comprehensive, rights-based system. The US employs a fragmented, sector-based, liberal, consumer, and market-driven right law, which includes the protection of digital safety and privacy in the context of national security. India is in between, slowly developing a constitution and a comprehensive, legislated right to maintain online privacy within the bounds of digital entrepreneurship and digital governance.

In India, privacy law has been built slowly and with great intensity of judicial interpretation. There was no reference to privacy in the Constitution. The first laws and judgments that created the right to privacy were very uncertain. But the rapid development of technology and growing State surveillance made the reconsideration of the Constitution inevitable. This was made possible by the unanimous judgment in *Justice K.S. Puttaswamy v. Union of India*,[3] where the Supreme Court confirmed that Privacy is a fundamental right of individuals and is protected in Articles 14, 19, 21 of the Indian Constitution.

India established the Digital Personal Data Protection Act, 2023 to provide a legal framework for the processing of personal data and digital privacy. Although this Act attempts to provide a

[1] Hemendra Singh, *Legal Frameworks for Privacy and Digital Freedoms*, in *Championing Civil Rights in the Digital Era* 339–364 (IGI Global Scientific Publishing 2025), https://doi.org/10.4018/979-8-3693-3920-6.ch013.
[2] Anuttama Ghose, Neha Agashe & S. M. Aamir Ali, *Digital Governance, Security, and Privacy Rights in India*, in *Championing Civil Rights in the Digital Era* 445–468 (IGI Global Scientific Publishing 2025), https://doi.org/10.4018/979-8-3693-3920-6.ch018.
[3] (2017) 10 SCC 1.

comprehensive legal framework, issues of extensive governmental exemptions, surveillance, lack of robust oversight, and executive control within the structure of law remain.[4]

This paper presents a comparative study of the digital privacy frameworks of India, the United States, and the European Union. It includes analysis of the underpinning constitutions, evolution of case law pertaining to the balance of personal liberty and prevalent legal provisions, and current issues of surveillance and data governance and control. It seeks to answer the question of whether the current Indian privacy framework is able to meet the protection of the fundamental rights enshrined in the Constitution and maintain the demand of a democracy on the balance of defense and technology.

Privacy is an expanding and complex idea that includes autonomy, dignity, confidentiality, identity, and the control of one's information. The legal principle of privacy began as protection from arbitrary interference of the State in the private life of citizens. In their famous article entitled "The Right to Privacy" in 1890, Samuel Warren and Louis Brandeis argued that privacy is the right to be let alone. Current definitions of privacy go well beyond protection from physical interferences of the State.[5]

Privacy today is unique and includes concerns like informational privacy, decisional privacy, communication privacy, and privacy against algorithmic surveillance. Digital privacy is a subset of privacy. It is concerned with the privacy of information that is generated, stored, processed, and communicated through digital technologies.[6] Digital privacy is different from traditional privacy concerns, which are mostly about physical searches and physical surveillance. Traditional privacy concerns are much simpler and include concerns like biometric data. Traditional privacy concerns also include issues like online profiling, facial recognition, data mining, and ads that are targeted and personalized as a result of artificial intelligence and behavioral manipulation.

The digital world also allows the State and non-State actors to collect and use a lot of data about individuals. Governments are using digital technology to control people in the welfare, policing, taxation, administration, and security systems. On the other hand, the corporate sector uses digital technology to control consumers through targeted ads and behavioral control and commercial

[4] Saumya Gupta, *Data Privacy in the Digital Era: Balancing Innovation and Intellectual Property Rights*, in *Intellectual Property Rights: Issues and Challenges* 241–258 (The Bhopal School of Social Sciences 2025), https://doi.org/10.51767/c250615.

[5] Avani Singh & Tina Power, *Understanding the Privacy Rights of the African Child in the Digital Era*, 21(1) Afr. Hum. Rts. L.J. (2021), https://doi.org/10.17159/1996-2096/2021/v21n1a6.

[6] *Human Rights in the Digital Era: The Right to Privacy at Stake*, Int'l J. Afr. & Asian Stud. (2022), https://doi.org/10.7176/jaas/80-08.

profiling. Therefore, privacy is breached in a lot of ways, and it can be said that privacy is breached by the automated and persistent collection of data.[7]

The dignity of individuals and the constitutional rights of liberty and equality are fundamentally related to the right to privacy. The right to privacy is also related to the right to freedom of expression. Individuals should have the right to privacy in relation to their thoughts and beliefs as a way to protect their personal autonomy. Continuous collection and surveillance of data decimate the autonomy of individuals and result in a "chilling effect" on democracy by discouraging the expression of dissent.

The right to privacy has also been recognized and incorporated in international law as a fundamental human right. A number of different international legal instruments, including the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), recognize the right to privacy and other related rights. Article 12 of the UDHR and Article 17 of the ICCPR are fundamentally concerned with the privacy of individuals and prohibit arbitrary interference with the privacy, family, and domicile of a person, as well as their communication. These rights have inspired the case law and scholarship on the right to privacy in different jurisdictions and constitutional democracies.[8]

Current data protection laws show how countries are moving from secrecy-based privacy protection to privacy protection based on individual rights. Most modern data protection laws contain the principles of informed consent, purpose specification and limitation, transparency, accountability, data minimization, and limitation of storage. One of the most comprehensive frameworks of this type of legislation is the GDPR.

India's modernization of its privacy laws marks a similar positive shift toward embracing informational autonomy as a fundamental constitutional value. However, as far as the balance between the accommodation of rapid technological advancement and digital governance, economic growth, and the rights of the individual, remains a concern for Indian constitutionalism.[9]

2. MODERN DEVELOPMENTS OF PRIVACY LAWS IN INDIA

2.1 The Early Constitutional Position

The constitution of India is silent on the right to privacy and does not ingratiate it as a fundamental right. In the initial constitutional phase, the courts of India functioned in the realm of a narrow

[7] *Digital Rights and Privacy* (Greenhaven Publishing LLC 2023).
[8] Michael A. Einhorn, *Digital Rights Management, Licensing, and Privacy*, SSRN (2002), https://doi.org/10.2139/ssrn.332720.
[9] Jodi Kearns, *Privacy Rights in the Digital Age*, 31(2) Reference Revs. 9–10 (2017), https://doi.org/10.1108/RR-11-2016-0260.

meaning of personal liberty under Article 21. When deliberating on the scope of powers in the context of searches and seizures, the Supreme Court in *M.P. Sharma v. Satish Chandra*[10] held that there is no general right to privacy embedded in the Constitution.

More or less the same position was taken in *Kharak Singh v. State of Uttar Pradesh*.[11] In both cases, the majority ruled that privacy was not a right embedded in the Constitution. However, in the same case, Justice Subba Rao was of the opinion that unauthorised surveillance is a violation of the right to personal liberty as well as dignity.

Judicial advancements over time continued to increase the scope of constitutional safeguards relating to autonomy and privacy. The Supreme Court in *Gobind v. State of Madhya Pradesh*[12] held that privacy can be interpreted under Article 21, albeit with limitation of overriding concerns of the State. Similarly, in *R. Rajagopal v. State of Tamil Nadu*,[13] the Court held that an individual has the right to protect the privacy of his/her personal life against unauthorised publications.

With the increasing use of electronic surveillance and interception of communications, concerns of privacy grew. The Supreme Court, in *People's Union for Civil Liberties v. Union of India*,[14] considered telephone conversations to be a part of the right to privacy and provided safeguards against arbitrary interception.

The extension of the scope of Article 21 through judicial interpretation provided a bedrock for the recognition of privacy as a constitutional right in India. Not having the right explicitly in the Constitution, notwithstanding judicial interpretation, created a lot of ambiguity, which ended after the landmark Puttaswamy verdict.

2.2 Justice K. S. Puttaswamy v. Union of India

It is the leading case for the constitutional recognition of privacy in India. The case emerged from the many constitutional petitions that were filed against the Aadhaar scheme, a program that collects and stores biometrics and demographic data of the residents of India. All nine Judges of the Constitutional Bench of the Supreme Court unanimously held that the Right to Privacy is a fundamental right and is enshrined in Articles 14, 19 and 21 of the Constitution of India. The Court overruled the earlier case law in M P Sharma and Kharak Singh (where the right to privacy was not recognized as a constitutional right and thus denied constitutional recognition).[15]

[10] AIR 1954 SC 300.
[11] AIR 1963 SC 1295.
[12] (1975) 2 SCC 148.
[13] (1994) 6 SCC 632.
[14] (1997) 1 SCC 301.
[15] Kamshad Mohsin & Zainab Zaya Khan, *Right to Privacy in Digital Era*, SSRN (2020), https://doi.org/10.2139/ssrn.3678224.

Chandrachud J. in his judgment observed that privacy is the core of liberty, dignity, and of autonomy and individuality. The judgment has recognized the following dimensions of the right to privacy -

- Bodily privacy,
- Informational privacy,
- Privacy of one's decisions,
- Privacy of one's communications.

The Court recognized that in this digital age, a Government/Corporation can collect and store so much personal data about an individual that can be of a very personal and private nature, it can be of even the most intimate nature and, therefore, protection has to be given to the Right to Privacy.[16] The judgment established the test of proportionality with respect to the right to privacy and held that the right to privacy can be infringed only if the following four requirements are satisfied in relation to the infringement -

- The infringement must be a legal infringement,
- It must aim to achieve a legitimate purpose of the State,
- It must be necessary and proportionate to achieve the said purpose,
- There must be adequate legal provisions to ensure that the infringement is not misused.

The Puttaswamy judgment is one of the most progressive constitutional formulations of the right to privacy globally and has transformed Indian constitutional law by recognizing privacy as being integral for the protection of dignity and democratic participation. The judgment, however, acknowledged that the right to privacy is not an absolute right.

2.3 Aadhaar Judgment and Privacy of Information

Within the context of the nine-judge bench decision, the Supreme Court analyzed the constitutionality of the Aadhaar program in the case of *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*.[17] The core opinion considered the Aadhaar project a constitutionally valid project. The Court compared biometric identification in the Aadhaar project to the achievement of a legitimate welfare goal. It further deemed Aadhaar as facilitating an effective system for the provision of welfare benefits and public services. The Court also placed some restrictions on the private sector's access to information contained in Aadhaar.

[16] Maria Pislaruc, *Privacy Regulations and Their Role in Protecting Employee Rights in the Digital Era*, in *Rule of Law and Economic Resilience in the Context of Moldova's Accession to the European Union* 147–154 (Moldova State Univ. 2025), https://doi.org/10.59295/rler2024.16.
[17] (2019) 1 SCC 1.

Volume 45, May 2026 ISSN 2581-5504

The judgment, although constitutionally valid in nature, was met with considerable criticism with respect to Aadhaar and its potential for surveillance and undermining the right to informational autonomy. Critics were of the opinion that centralised biometric systems are conducive to mass surveillance, profiling and exclusion. Justice Chandrachud, in his dissent, pointed out that the Aadhaar system is disproportionate to the aim sought to be achieved and breaches the right to privacy, which is guaranteed by the Constitution.

The Aadhaar case highlighted the conflict that exists in a democracy between digital governance and privacy in India. It can be argued that while the Aadhaar biometric digital identity systems may serve to enhance the efficiency of welfare administration and governance, they also extend the potential for State surveillance of citizens and increase the potential for the abuse of citizens' private data.

3. STATUTORY FRAMEWORK FOR DIGITAL PRIVACY IN INDIA

3.1 Information Technology Act, 2000

Before comprehensive data protection legislation was introduced, India had to rely on the Information Technology Act, 2000 to some degree to regulate digital information and cyber activities. Section 43A made body corporates liable for the negligent implementation of reasonable security practices with respect to the protection of sensitive personal data, and Section 72A made the breach of contract disclosure of information obtained from a lawful contract without the consent of the individual a criminal offense.[18]

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, introduced further specifics relating to the obligation of consent, privacy policy, and the protection of sensitive personal information. Nevertheless, the framework suffered a number of flaws[19] -

- Validity applied principally to corporations and not to the government;
- The data subject rights were not comprehensive;
- The gaps in the optionality were extended to enforcement;
- An independent regulatory body was not established.

Thus, the IT Act, on its own, was inadequate to address the modern issues of digital privacy and bulk processing of data.

[18] Anita Gurumurthy, *Towards Feminist Futures in the Platform Economy: Four Stories from India*, in *Epistemic Rights in the Era of Digital Disruption* 113–126 (Springer Int'l Publ'g 2024), https://doi.org/10.1007/978-3-031-45976-4_8.

[19] Vivek Kumar Gupta, *The Dual Edges of Digital Privacy: WhatsApp Security Strategies and User Rights in India*, 4(1) Int'l J. Civ. L. & Legal Rsch. 194–200 (2024), https://doi.org/10.22271/civillaw.2024.v4.i1c.79.

3.2 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is India's first complete law that regulates the processing of personal data. The provisions of this law apply to the digital personal data processed in India, and to some processing activities that take place outside of India and affect persons in India.[20] With this Act the following constructs are introduced -

- Data Principal;
- Data Fiduciary;
- Consent-based processing;
- Obligations related to the processing of data in a lawful manner;
- Rights to Data Principal for grievance redressal;
- Rights to Data Principal for correction and erasure of personal data;
- Liabilities for breach of the Act;

The Act provides rights of access, correction, erasure and grievance redressal to Data Principals. Data Fiduciaries are required to implement reasonable security safeguards, refrain from data breaches, and ensure that the data is processed for a lawful purpose. This Act is a pivotal move in formalizing India's digital privacy law, but some gaps and concerns on the structure and implementation of the law do exist.[21]

The broad exemptions to government agencies under the Act is one of the most criticized provisions. The Central Government can exempt certain entities from the application of the Act on grounds such as the sovereignty and security of the State, public order and the prevention of offences. These exemptions are seen as allowing for illogical and excessive use of executive power, with no judicial oversight, and are in direct conflict with the principles laid down in the Puttaswamy case.

In contrast to the GDPR, the Indian law does not create a data protection authority that is completely independent of the executive. Hence, there are concerns about the regulatory structure's independence, efficiency, and accountability. The Act takes a more flexible position on international data transfers. Although the government can limit data transfers to certain jurisdictions, the framework does not include adequacy requirements as in the GDPR.

[20] Amit Singh & Praveen Singh Chauhan, *The Dual Edges of Digital Privacy: WhatsApp's Security Strategies and User Rights in India*, 4(2) Int'l J. Civ. L. & Legal Rsch. 148–154 (2024), https://doi.org/10.22271/civillaw.2024.v4.i2b.102.

[21] Mary Johnson Angel & Vipin Das R. V., *Regulating Digital Journalism: Striking a Balance Between Press Freedom and Privacy Rights in India* (2025), https://doi.org/10.5281/zenodo.15173487.

Volume 45, May 2026 ISSN 2581-5504

The Act does not make comprehensive reforms to India's surveillance framework by amending the laws of the Telegraph Act and the IT Act. Thus, there continues to be concern about powers of interception, monitoring, and mass surveillance. The Digital Personal Data Protection Act, 2023, will be the first major step towards establishing a comprehensive framework for protection of digital privacy in India.

4. PRIVACY FRAMEWORK IN THE UNITED STATES

The United States takes a piecemeal and sector-specific stance in relation to privacy laws. It is in contrast to the European Union, where the United States does not have a sole comprehensive federal data protection law that governs all the sectors. Privacy is not expressly included in the United States Constitution. Nevertheless, the Supreme Court has acknowledged privacy as a right in numerous judgments.

In *Griswold v. Connecticut*,[22] the Supreme Court acknowledged marital privacy under the penumbras of constitutional guarantees. Subsequently *Roe v. Wade*[23] affirmed the privacy right to make a decision about one's reproductive rights, despite the fact that subsequent legal reforms have substantially altered its position.

The Fourth Amendment is really important when it comes to privacy and surveillance. In the case of *Katz v. United States*[24] the Court decided that people have a right to expect some privacy. This means that the government cannot just do whatever it wants to get information about someone. The Court said that this right to privacy is not about physical places, it is also about other things.

New technology has made things more complicated for the Fourth Amendment. In the case of *Carpenter v. United States*[25] the Supreme Court said that people have a right to privacy when it comes to their cell phone location history. The Court understood that technology can be used to track people all the time.

There are some laws in the United States that are supposed to protect people's privacy. These laws are -

- Health Insurance Portability and Accountability Act (HIPAA)
- Children's Online Privacy Protection Act (COPPA)
- Gramm-Leach-Bliley Act (GLBA)
- Electronic Communications Privacy Act (ECPA)
- California Consumer Privacy Act (CCPA)

[22] 381 U.S. 479 (1965).
[23] 410 U.S. 113 (1973).
[24] 389 U.S. 347 (1967).
[25] 138 S.Ct. 2206 (2018).

Volume 45, May 2026 ISSN 2581-5504

These laws do not really treat privacy as a right. Instead they try to balance privacy with things that are important like making it easy for businesses to do what they want. This is different from the EU, where privacy is treated as an important right. In the US companies that use technology have a lot of power. The Fourth Amendment and privacy laws are still really important because they help to protect people's privacy. The Health Insurance Portability and Accountability Act and the Fourth Amendment are both about protecting people's privacy.[26]

5. SURVEILLANCE AND NATIONAL SECURITY IN THE UNITED STATES

The way the United States handles privacy has been criticized a lot especially after Edward Snowden revealed what the National Security Agency was doing. The National Security Agency is a part of the United States government. The US PATRIOT Act and the Foreign Intelligence Surveillance Act gave the government power to watch people and collect information after the September 11 attacks.[27]

These laws were made to keep the country safe from terrorism. However some people think that the government is watching people too much and that this is not fair. They are worried that the government is collecting too much information and that people do not have enough privacy. There are courts that are supposed to make sure the government does not do anything like the Foreign Intelligence Surveillance Court.[28]

Some people think that the government is not transparent enough and that the courts are not doing a good job. The United States is very focused on security and also has a big technology industry. There are some laws to protect people's privacy. They are not very strong. The government and companies are more focused on security and making money than on protecting people's privacy.

6. PRIVACY FRAMEWORK IN THE EUROPEAN UNION

The European Union has strong laws to protect people's privacy. The European Union thinks that privacy is a right that is connected to dignity and democracy. The European Union has a document called the Charter of Fundamental Rights that says people have the right to privacy. Article 7 of

[26] Maria Pislaruc, *Privacy Regulations and Their Role in Protecting Employee Rights in the Digital Era*, in *Rule of Law and Economic Resilience in the Context of Moldova's Accession to the European Union* 147–154 (Moldova State Univ. 2025), https://doi.org/10.59295/rler2024.16.
[27] Shirin Elahi, *Privacy and Consent in the Digital Era*, 14(3) Info. Sec. Tech. Rep. 113–118 (2009), https://doi.org/10.1016/j.istr.2009.10.004.
[28] Kundalakesi M., *Cybersecurity – Safeguarding Privacy in the Digital Era*, Int'l Rsch. J. Educ. & Tech. 53–67 (2024), https://doi.org/10.70127/irjedt.vol.7.issue03.67.

Volume 45, May 2026 ISSN 2581-5504

the Charter of Fundamental Rights of the European Union says that people have the right to a life.[29]

Article 8 says that people have the right to protection of their information. The European Court of Human Rights also says that people have the right to privacy. The European Union has made some decisions to protect people's privacy. For example in the case of *Digital Rights Ireland Ltd v. Minister for Communications*[30] the court said that a law that made companies keep people's information for a time was not fair.

In another case *Schrems v. Data Protection Commissioner,*[31] the court said that companies could not send people's information to the United States because the United States did not have enough laws to protect people's privacy. The EU made GDPR that states how companies can use people's information.[32] The law is based on some principles -

- Companies have to be honest and transparent about how they use people's information.
- Companies can only use people's information for a purpose.
- Companies have to make sure people's information is accurate.
- Companies have to keep people's information safe.
- Companies have to be responsible for how they use people's information.

The law also gives people some rights -

- People have the right to see what information companies have about them.
- People have the right to correct information that's wrong.
- People have the right to delete their information.
- People have the right to object to how companies use their information.
- People have the right to take their information to another company.

Companies also have some responsibilities -

- They have to design their systems to protect people’s information.
- They have to tell people if their information is stolen.
- They have to do assessments to make sure they are protecting people’s information.
- They have to appoint a person to be in charge of protecting people’s information.

[29] Muge Fazlioglu, *Negotiating Privacy - Bipartisan Agreement on Privacy Rights*, SSRN (2022), https://doi.org/10.2139/ssrn.4227239.
[30] Joined Cases C-293/12 and C-594/12.
[31] C-362/14.
[32] Riduan Siagian, Leonard Siahaan & Muhammad Ichwan Hamzah, *Human Rights in the Digital Era: Online Privacy, Freedom of Speech, and Personal Data Protection*, 2(4) J. Digit. Learning & Distance Educ. 513–523 (2023), https://doi.org/10.56778/jdlde.v2i4.149.

Volume 45, May 2026 ISSN 2581-5504

7. COMPARATIVE ANALYSIS OF INDIA, THE US AND THE EU

India, the US and the EU have approaches to privacy. The EU and India think that privacy is a right. The US does not have a law that says privacy is a fundamental right. The EU has a law to protect people's privacy. The US has laws for different areas like healthcare and finance. India is trying to make a new law to protect people's privacy. It is not finished yet. All three countries are trying to balance privacy with security. The EU is more strict about how the government can watch people. India and the US give the government power to watch people, which is a concern for some people.

The EU has authorities to enforce the law. The US has regulators, which can make it hard to enforce the law. India's authorities are not independent which is a concern for some people. The EU gives people the rights when it comes to their information. India's law gives people some rights. Not as many as the EU. The US has laws that give people different rights depending on the area.

Aspect	India	United States	European Union
Constitutional Status	Privacy recognised as a fundamental right in *Puttaswamy*	No explicit constitutional right; derived through judicial interpretation	Privacy and data protection explicitly recognised as fundamental rights
Nature of Framework	Emerging comprehensive framework under DPDP Act, 2023	Fragmented sector-specific model	Comprehensive GDPR framework
Key Legislation	DPDP Act, 2023; IT Act, 2000	HIPAA, COPPA, CCPA, ECPA	GDPR
Regulatory Approach	Executive-centric regulatory structure	Market-oriented and sectoral	Rights-based and harmonised
Data Protection Authority	Limited institutional independence	Multiple regulators	Independent supervisory authorities

Volume 45, May 2026 ISSN 2581-5504

User Rights	Access, correction, erasure, grievance redressal	Varies across sectors	Extensive rights including portability and right to be forgotten
Surveillance Oversight	Broad executive powers	Strong national security orientation	Strict proportionality standards
Cross-Border Data Transfers	Flexible and government-controlled	Comparatively liberal	Strict adequacy standards
Enforcement	Developing framework	Fragmented enforcement	Strong penalties and institutional enforcement
Philosophical Basis	Balance between development and privacy	Consumer protection and innovation	Human dignity and informational autonomy

8. CONCLUSION

Digital privacy is a big deal these days. It is one of the important things that people are worried about when it comes to the law and the constitution. With all the technology and artificial intelligence and stuff things have changed a lot between people, companies and the government. Digital privacy is not about keeping people from barging into your home, it is also about being able to control your own information and make your own decisions.

If you look at how India, the US and the EU handle privacy you can see that they all have different ideas about it. The EU has a set of rules called the GDPR that is all about protecting people's dignity and making sure that institutions are accountable. The US has a lot of rules for different areas and they are often influenced by what companies want and what the government thinks is best for national security. India is in the middle trying to balance peoples rights with the need for technology and development.