**Educational Administration: Theory and Practice**
2023, 29(04), 5262-5273
ISSN: 2148-2403
https://kuey.net/

**Research Article**

# A Comparative Study of Digital Privacy in Europe, America, And India

Rachna Yadav*

*Ph.D. Scholar, MVN University, Under the supervision and guidance of Dr. Rahul Varshney, Dean, School of Law, MVN University, Haryana

**Citation:** Rachna Yadav, (2023) A Comparative Study Of Digital Privacy In Europe, America, And India. *Educational Administration: Theory and Practice*, 29(04) 5262-5273
Doi: 10.53555/kuey.v29i4.10123

**ARTICLE INFO**

**ABSTRACT**

In an increasingly digital world, privacy has emerged as a crucial concern for individuals, governments, and organizations. This comparative study examines the frameworks, policies, and cultural approaches to digital privacy in Europe, America, and India. Europe, with its General Data Protection Regulation (GDPR), represents a robust and citizen-centric model emphasizing user consent and data protection. In contrast, the United States adopts a sectoral approach driven largely by corporate interests and market dynamics, leading to fragmented and less comprehensive privacy protections. India, while still developing its digital privacy regime, is guided by the Supreme Court's recognition of privacy as a fundamental right and the ongoing implementation of the Digital Personal Data Protection Act (DPDPA) of 2023. This study highlights the differences in regulatory environments, enforcement mechanisms, and public awareness across these regions. It also explores how cultural values, legal traditions, and political structures shape digital privacy norms. By drawing comparisons, the research offers insights into global privacy challenges and suggests pathways for harmonizing data protection standards in a connected world.

***Keywords:*** Digital Privacy, GDPR, Data Protection, Privacy Laws, Comparative Study, DPDPA 2023, Information Security, etc.

## 1. INTRODUCTION

One of the most important issues facing people, businesses, and governments alike in the digital era is privacy. Depending on their legal systems, cultural norms, and technical environments, countries have adopted a variety of strategies to protect digital privacy as personal data becomes a valuable commodity. In order to provide insight into how each location handles data protection, user consent, monitoring, and regulatory enforcement, this comparative research examines the digital privacy conditions in Europe, America, and India. Europe has established a worldwide standard for privacy rights and accountability with its historic GDPR. The US, on the other hand, has a more corporate-driven and sectoral strategy, prioritising market flexibility and innovation, often at the expense of thorough user protection. With historic court rulings and new laws like the DPDPA, India, a democracy that is quickly digitising, is changing its privacy architecture. By examining these many models, this research seeks to draw attention to the advantages and disadvantages of each system and provide guidance for creating a fair and efficient digital privacy law on a worldwide scale[1].

With an emphasis on comprehending how each location handles the protection of personal data in the digital era, the primary goal of this research is to analyse the digital privacy laws and regulations in Europe, America, and India. It seeks to pinpoint significant parallels and divergences between these regions' data protection policies and enforcement systems. The research also aims to investigate the legislative and cultural elements that influence how each area views digital privacy. Lastly, it aims to pinpoint the main issues with current frameworks and provide potential fixes to support more robust and cohesive international digital privacy standards[2].

[1] European Union, *General Data Protection Regulation (EU) 2016/679*, Official Journal of the European Union, L 119, 4 May 2016, pp. 1–88.
[2] Government of India, *The Digital Personal Data Protection Act, 2023*, Act No. 22 of 2023, Ministry of Law and Justice (Legislative Department), 11 August 2023.

### 1.1 Importance of digital privacy

In recent years, maintaining one's privacy online has become a more urgent issue due to technological advancements as well as the rise in the quantity of data kept digitally. As more and more of our lives are conducted online, we are giving digital platforms and companies more and more personal information[3].

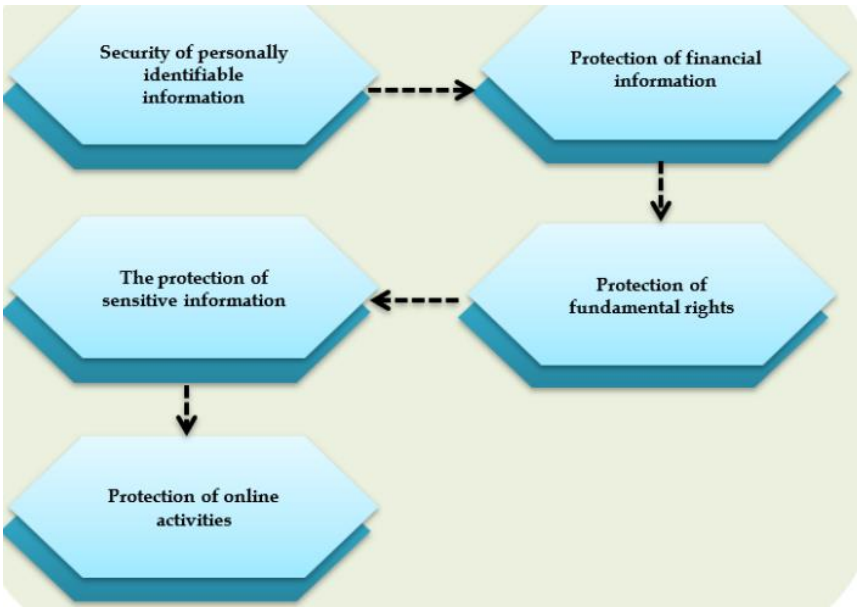


**Figure 1: Importance of Digital Privacy**

As a result, these platforms and companies are more vulnerable to data breaches as well as inappropriate information usage. In the modern world, protecting one's online privacy is crucial for many reasons, such as the following:

Security of personally identifiable information: One of the main reasons digital privacy is so important is to prevent unauthorised individuals from accessing or using our personal information. Identity thieves and fraudsters might use details like our names, addresses, phone numbers, and email addresses to commit crimes. Additionally, we might be stalked or harassed using this information.

Protection of financial information: Our bank account and credit card information are among the other financial facts we keep online. Hackers or cybercriminals may use these facts, which include our bank account and credit card information, if our digital privacy is not safeguarded.

The protection of sensitive information: If the wrong people access sensitive personal information, such as our medical history, sexual orientation, religious views, or political affiliations, it may be misused for improper reasons. Maintaining the anonymity of this information is crucial if we want to prevent persecution, harassment, or discrimination based on our personal convictions.

Protection of online activities: If we want to stop others from seeing or recording our online activity, we must have control over our digital privacy. In order to better target their consumers with advertising or surveillance, many companies and government organisations increasingly monitor their online activity to get greater insight into their preferences, habits, and behaviours.

Protection of fundamental rights: Lastly, maintaining our digital privacy is essential to defending our rights to freedom of expression, assembly, as well as association. This is the last justification for the significance of safeguarding our online privacy. If our internet behaviour is tracked and restricted, we may be less inclined to express ourselves freely. This may have detrimental effects on our democracy and society[4].

---

[3] Solove, Daniel J., *Understanding Privacy*, Harvard University Press, 2008, p. 1–25.

[4] Schneier, Bruce, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company, 2015, pp. 35–72.

## 2. LITERATURE REVIEW

| Author(s) | Year | Key Focus | Findings |
|---|---|---|---|
| **Anisha Agarwal et al.** | **2020** | Analyzes data protection laws in USA, UK, as well as India in light of GDPR. | Highlights India's efforts towards GDPR compliance, focusing on post-Puttuswamy privacy rights and the potential for legislative reform[5]. |
| **Dev Kaur et al.** | **2024** | Examines legal frameworks and judicial interpretations regarding privacy in India and UK. | Discusses how both countries safeguard privacy through distinct legal paths, emphasizing cultural and political influences on cyber law effectiveness[6]. |
| **Swapneel Sheth et al.** | **2014** | Survey-based study on online privacy concerns. | Users equate privacy with security; developers prioritize technical measures. Regional differences noted in privacy awareness[7]. |
| **Edda Humprecht et al.** | **2020** | Cross-national study of disinformation impact in democracies. | Countries with strong democratic structures (e.g., Northern Europe) show higher resilience. Framework offers insight into combating online disinformation[8]. |
| **Evelyn Nakano Glenn et al.** | **2020** | Structural analysis of U.S. race and gender through settler colonialism. | Illustrates how U.S. race/gender constructs evolved via exclusionary practices and coerced labor[9]. |
| **Kimberly Bloom-Feshbach et al.** | **2013** | Global analysis of influenza and RSV seasonal trends. | Seasonal patterns vary by latitude; tropical regions exhibit unique epidemic timelines. Recommends linking patterns with climate and demographic data[10]. |
| **Riyad A. Shahjahan et al.** | **2022** | Review of literature on decolonization in global academia. | Defines meanings, implementations, and challenges of decolonizing pedagogy, stressing contextual differences. |
| **Payam Hanafizadeh et al.** | **2013** | Systematic review of 165 articles (1999–2012). | Categorizes research into descriptive, relational, and comparative. Identifies research gaps for future exploration[11]. |
| **Abbas Razaghpanah et al.** | **2018** | Empirical study using mobile data (Lumen Monitor). | Identifies over 2,000 tracking services; many unknown. Highlights risks and implications under GDPR[12]. |
| **Tamar Sharon et al.** | **2021** | Analysis of Apple-Google COVID-19 API. | Reflects on how tech firms became perceived privacy advocates, raising concerns about corporate power in public governance[13]. |

[5] A. Agarwal, "Sanctity of Personal Data: A Comparative Study of Data Privacy Laws in EU, US and India" (2020) 6(3) *International Journal of Legal Developments and Allied Issues* 152–189.

[6] I. Y. Brain et al., "A Comparative Study of the Evaluation on the Right to Privacy in India and the UK, Their Legal Frameworks and Judicial Interpretation: A Cyber Law Perspective" (2024) *International Journal of Legal Science* 600–628.

[7] S. Sheth, G. Kaiser & W. Maalej, "Us and Them: A Study of Privacy Requirements Across North America, Asia, and Europe" (2014) 1 *Proceedings of the International Conference on Software Engineering* 859–870 https://doi.org/10.1145/2568225.2568244.

[8] E. Humprecht, F. Esser & P. Van Aelst, "Resilience to Online Disinformation: A Framework for Cross-National Comparative Research" (2020) 25(3) *International Journal of Press/Politics* 493–516 https://doi.org/10.1177/1940161219900126

[9] E. N. Glenn, "Settler Colonialism as Structure: A Framework for Comparative Studies of U.S. Race and Gender Formation" (2015) 1(1) *Sociology of Race and Ethnicity* 52–72 https://doi.org/10.1177/2332649214560440

[10] K. Bloom-Feshbach et al., "Latitudinal Variations in Seasonal Activity of Influenza and Respiratory Syncytial Virus (RSV): A Global Comparative Review" (2013) 8(2) *PLoS ONE* 3–4 https://doi.org/10.1371/journal.pone.0054445.

[11] P. Hanafizadeh, B. W. Keating & H. R. Khedmatgozar, "A Systematic Review of Internet Banking Adoption" (2014) 31(3) Telematics and Informatics 492–510 https://doi.org/10.1016/j.tele.2013.04.003.

[12] A. Razaghpanah et al., "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem" (2018) *25th Annual Network and Distributed System Security Symposium (NDSS)* https://doi.org/10.14722/ndss.2018.23353.

[13] T. Sharon, "Blind-sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers" (2021) 23(s1) *Ethics and Information Technology* 45–57 https://doi.org/10.1007/s10676-020-09547-x.

| | | | |
|---|---|---|---|
| **Andrew M. Guess et al.** | **2020** | Media literacy tips reduced perceived accuracy of false headlines; effects strongest in US, weaker in rural India. | Emphasizes need for education-based interventions to strengthen digital literacy and combat disinformation[14]. |
| **Jan Henrik Ziegeldorf et al.** | **2014** | Identifies IoT privacy threats such as tracking, profiling, and lack of control; calls for privacy-aware data management. | Foundational work highlighting IoT privacy risks and guiding design of privacy-preserving technologies[15]. |

### 2.1 Research gap

Despite the fact that digital privacy has received a lot of attention lately, thorough comparative studies that look at privacy regimes in Europe, America, and India are few. The majority of current research often ignores India's changing regulatory environment in favour of concentrating mostly on the GDPR in Europe and the sectoral regulations in America. Furthermore, little research has been done on how privacy practices in these areas are influenced by cultural norms, public knowledge, and the efficiency of enforcement. The necessity for current and inclusive research is further highlighted by the rapid development of digital technology and cross-border data flows. By providing a comprehensive assessment of digital privacy regimes from legal, social, and technical viewpoints, this research fills up these gaps.

## 3. RESEARCH METHODOLOGY

This comparative study examines the digital privacy frameworks in Europe, America, and India using a qualitative research technique. Academic journals, official government publications, legislative papers, reports from international organisations, and reliable internet sites are the main sources of secondary data used in this study. To investigate the parallels and discrepancies in privacy laws, enforcement strategies, and public attitudes across the three locations, a comparative analysis method is used. To comprehend the ethical and legal underpinnings of data protection, important laws including India's DPDPA, the California Consumer Privacy Act (CCPA) in the US, as well as the GDPR in Europe are examined. The research also takes into account how privacy regulations are influenced by political, cultural, and technical variables. This technique attempts to give a thorough and nuanced view of the worldwide digital privacy environment by combining information from many sources.

## 4. LEGAL AND REGULATORY FRAMEWORK

### 4.1 European Union - Data Privacy and Protection

The GDPR of the European Union went into effect on May 25, 2018. It governs the handling and transfer of personal data pertaining to individuals within the EU. All companies, no matter their size or industry, are subject to the GDPR. The Data Protection Directive of 1995/46 is superseded by it. We are aiming for the same things with both measures: a set of rules for data transmission and privacy protection.

### Key Provisions:

GDPR utilises wide terminology and has a broad reach. Any information pertaining to a live, identifiable person (the data subject), such as a name, email address, tax ID number, online identity, etc., is considered "personal data." "Data collection, recording, storage, as well as transmission are all considered forms of "processing" data[16].

Companies whose headquarters are outside of the EU may nonetheless be subject to the Regulation if they handle personal data belonging to individuals residing in the EU or an EEA member state (including Norway, Lichtenstein, and Switzerland):

a) If the company offers goods or services to data subjects in the EU; or,
b) If the company is monitoring data subjects' behavior taking place within the EU.

Other proof of the intention to sell products or services in the EU would be necessary, but the mere availability of a firm's website in the EU is not enough to subject the company to GDPR.

Generally speaking, businesses that are subject to GDPR but are not based in the EU are required to appoint an EU representative in writing for GDPR compliance. This rule does not apply to small-scale, infrequent processing of non-sensitive data.

---

[14] A. M. Guess et al., "A Digital Media Literacy Intervention Increases Discernment Between Mainstream and False News in the United States and India" (2020) 117(27) *PNAS USA* 15536–15545 https://doi.org/10.1073/pnas.1920498117.

[15] J. H. Ziegeldorf, O. G. Morchon & K. Wehrle, "Privacy in the Internet of Things: Threats and Challenges" (2014) 7(12) *Security and Communication Networks* 2728–2742 https://doi.org/10.1002/sec.795.

[16] European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016* on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

Up to 20 million euros (or 4 percent of annual worldwide sales, whichever is greater) may be fined for noncompliance. Legal counsel can assist companies of all sizes and in all sectors incorporate GDPR into their comprehensive compliance plan[17].
To aid companies in their compliance process, formal guidelines have been released by the European Commission and Data Protection Authorities. Data protection impact assessments, how to notify individuals of a data breach, and the data protection officer's duties are all covered in these documents.

### 4.2 Digital Privacy in the United States

In the US, privacy rules and regulations are a hodgepodge of federal, state, as well as local statutes. There is currently no nationwide privacy law in the US. Although there are a plethora of state and local laws regarding data security and privacy in the US, "there are also a number of federal restrictions, most of which are industry-specific. Beginning with California in 2018, other states have begun to draft and enact their own extensive privacy laws. Legislation has been draughted by both parties since then, but efforts to pass a comprehensive bill have been blocked by shifting political winds, corporate influence, and the increasing complexity of privacy concerns. Therefore, it is unlikely that a comprehensive federal privacy legislation will be passed very soon[18].

### 4.3 Federal and State Privacy Laws and Regulations

The federal government has enacted a number of rules and regulations pertaining to many industries, including banking, telecommunications, healthcare, credit reporting, driving records, biometrics, telemarketing, digital marketing, and online privacy for minors.
Some state privacy laws are either entirely or partly superseded by federal privacy laws; moreover, there are many state data security and privacy requirements that could overlap with federal laws. Some US states have data security rules that apply to all businesses and go beyond what is necessary by federal law. These laws include secure destruction laws, online privacy laws, biometric information privacy laws, and data breach notification laws, among others. Generally speaking, these state laws cover personal data pertaining to citizens or events that take place in each of these states, accordingly. Consequently, many US-based businesses must comply not just with applicable federal laws, but also with a patchwork of state privacy and security statutes[19].
One example is the extensive CCPA, which is only one of over 25 privacy and data security laws in California. It places standards and limits on the gathering, using, disclosing, as well as processing of personal information of California citizens. It provides definitions as well as extensive individual rights. The CCPA stands out from other state-level privacy statutes since it regulates not only business-to-business and HR transactions, but also consumer personal data. After the revised CCPA rules were finished on March 29, 2023, the newly formed California Privacy Protection Agency, also referred to as the "CPPA" or the "Agency," started implementing them on March 29, 2024. Additional CCPA rulemaking on the following regulatory subjects will begin on November 8, 2024," according the Agency Board's decision: Updates on CCPA, Risk Assessments, Cybersecurity Audits, ADMT, and Insurance Companies[20]. Here are some of the main goals of the proposed regulations: (1) to bring the CCPA regulations up to date; (2) to mandate annual cybersecurity audits and privacy risk assessments for certain businesses; (3) to define who can access and who can opt out of ADMT; and (4) to clarify when insurance companies must comply with the CCPA. This set of proposed regulations will be open for public discussion until February 19, 2025[21].
Additionally, the CPPA enforces the "Delete Act," which goes into effect on January 1, 2024, and places deletion duties on data brokers. This makes it easier for customers to remove their personal information that is kept by data brokers in California. under January 1, 2026, the CPPA is required under the Delete Act to provide an easily accessible deletion method. The purpose of this technique is to enable customers to request the deletion of their data from data brokers and the related contractors or service providers in a single, verified request.
The California Age-Appropriate Design Code (CAADC), passed by the California legislature in August 2022, was set to go into effect on July 1, 2024, and would apply to businesses that fit the CCPA's definition of "business" and offer online services that people under the age of 18 are likely to access. On the basis of the First Amendment, a California District Court, however, granted an injunction on September 18, 2023, preventing

---

[17] European Commission, "Guidelines on Data Protection Officers ('DPOs')" (2017) WP243 rev.01, Article 29 Data Protection Working Party https://ec.europa.eu/newsroom/article29/items/612048
[18] United States Congress, *California Consumer Privacy Act of 2018*, Cal. Civ. Code §§ 1798.100–1798.199 (as amended by the California Privacy Rights Act of 2020), enforced by the California Privacy Protection Agency, https://oag.ca.gov/privacy/ccpa
[19] United States Senate, *American Privacy Rights Act of 2024*, Draft Bill, introduced April 2024, available at https://www.commerce.senate.gov/services/files/72F6FA9D-FEC5-47D3-9C95-23276CFA09B5
[20] California State Legislature, *California Consumer Privacy Act of 2018*, Cal. Civ. Code §§ 1798.100–1798.199 (amended by the California Privacy Rights Act of 2020), enforced by the California Privacy Protection Agency, https://cppa.ca.gov/regulations/
[21] California State Legislature, *Senate Bill 362 (Delete Act)*, Chapter 393, Statutes of 2023, codified at Cal. Civ. Code § 1798.99.82, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB362

the legislation from taking effect. The future of the statute is now unknown after the California Attorney General's office filed an appeal with the Ninth Circuit. You may learn more about the CAADC here.
Likewise, Connecticut modified its Consumer Data Protection Act to provide comparable safeguards for children's personal data, while Maryland passed the "Kids Code." Additionally, major revisions to the federal Children's Online Privacy Protection Act (COPPA) were finalised by the Federal Trade Commission (FTC) in January 2025. Although the FTC evaluates the COPPA regulation on a regular basis, these adjustments are the first since 2013. The FTC claims that the final modified regulation is meant to improve children's online safety and takes into account technical developments since COPPA was last updated. You may find more details about the revised regulation online. The goal of federal and state authorities working together is to create a safer online environment and guarantee that children's privacy is given first priority in a world that is becoming more interconnected[22].
Beyond California's CCPA, additional comprehensive state privacy laws have also taken effect, including the

- Colorado Privacy Act,
- Connecticut Data Privacy Act (including amendments regulating consumer health data, children's data, and social media platforms),
- Delaware Personal Data Privacy Act,
- Florida Data Privacy and Security Act,
- Iowa Consumer Data Protection Act,
- Montana Consumer Data Privacy Act,
- Nebraska Data Privacy Act,

All of these state privacy laws are different from one another, but with the exception of the CCPA, they are quite similar. Scope, disclosures of privacy notices, privacy rights, and precise definitions are some areas where there could be variations. Additionally, personal information gathered and processed in the course of business and employee interactions is often exempt from these state regulations. Although the CCPA and these state laws have certain practical parallels, the CCPA adopts more detailed definitions, criteria, and prohibitions that differ significantly from existing laws. This is especially true for personal information gathered from California residents in B2B and employment situations[23].
Also, health data has come a long way since 2023, when the landmark My Health My Data Act (MHMD) was signed in Washington. Despite claims to the contrary, the legislation's expansive language, private right of action, and broad definitions mean it might include data that many companies would not typically consider "health" data. The MHMD Act is available online for your perusal. Following MHMD's lead, several states have done the same. For instance, on October 1, 2023," "Connecticut's Consumer Data Privacy Act was revised to incorporate similar provisions for the protection of consumer health data; on March 31, 2024, the Nevada Consumer Health Data Privacy Law was enacted by Senate Bill 370 in Nevada[24].
Lastly, the following states have passed their own complete privacy laws or versions thereof, and many more states are draughting similar legislation, demonstrating the general acceleration of state privacy legislation:

- Tennessee (effective July 1, 2025)
- Minnesota (effective July 21, 2025)
- Maryland (effective November 1, 2025)
- Indiana (effective January 1, 2026)

### 4.4 Enforcement of Unfair and Deceptive Trade Practices

U.S. consumer protection laws, which prohibit deceitful and unfair business practices, provide another mechanism for holding corporations to account for their privacy and security policies.
The Federal Trade Commission (FTC) is a federal agency that investigates and prosecutes businesses that breach customers' rights to privacy and data security as well as those who engage in unfair or misleading business practices. There are many reasons why the FTC initiates enforcement procedures and conducts investigations into businesses, like as:

- Not putting in place appropriate data security procedures
- Making security and privacy claims, especially in privacy policies, that are noticeably false or deceptive.
- Not adhering to the relevant industry self-regulation guidelines
- In a bankruptcy or merger and acquisition transaction, transferring or trying to transfer zersonal data to an acquiring firm in a way not specifically stated on the relevant consumer privacy policy.

---

[22] United States District Court for the Northern District of California, *NetChoice, LLC v. Bonta*, No. 5:22-cv-08861-BLF, Preliminary Injunction Order dated 18 September 2023, https://www.courtlistener.com/docket/66677606/netchoice-llc-v-bonta/
[23] Washington State Legislature, *My Health My Data Act*, Chapter 19.373 RCW, Laws of 2023, https://app.leg.wa.gov/rcw/default.aspx?cite=19.373
[24] Nevada Legislature, *Senate Bill No. 370 (Consumer Health Data Privacy Law)*, 82nd Session (2023), effective 31 March 2024, https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10838/Overview

- Violating consumer privacy rights by gathering, using, disclosing, or failing to properly secure customer data, as per the guidelines set out in their previous enforcement precedents

Several state solicitors general share similar enforcement authorities against unfair and dishonest business practices that harm consumers in their territories. These acts might include failing to implement proper security measures and violations of consumer privacy rights. Furthermore, state solicitors may work together in enforcement actions against companies for actions that affect customers in many states (e.g., data breaches).

### 4.5 Key Areas of Privacy Class Action

The United States continues to face a significant threat from privacy class actions involving biometric privacy (as per the Illinois Biometric Privacy Act), text messaging (as per the federal This includes accusations including wiretapping, call recording, and similar issues (as per the California Invasion of Privacy Act, the Video Privacy Protection Act (VPPA), and other state legislation). Tracking and targeting online, particularly using "session replay" technologies, chatbots, and "cookies," is a contentious issue among regulators and plaintiff's lawyers. A private right of action may be asserted under the CCPA in the event of a data breach caused by inadequate security measures. They emphasise the need of firms adhering to stringent data protection regulations to avoid legal difficulties and highlight the shifting landscape of privacy lawsuits[25].

### 4.6 Digital Privacy in India

In today's increasingly data-driven culture, personal information is highly prized. As more and more individuals put their faith in digital services and online platforms, robust data security measures are becoming more crucial. Indian law, as passed in 2023, Protecting individuals' privacy in India is one of the primary goals of the Data Protection and Privacy Act (DPDPA)". This article delves into the DPDPA's safeguards, "painting a vivid picture of the data types that are protected by this landmark legislation.

According to this long-ago law, the India Protecting people's privacy in the digital era is the main goal of DPDPA. The legislation, which went into effect on September 1, 2023, applies to all businesses that handle personal information of consumers India.

### DPDPA

The Data Protection and Privacy Act (DPDPA) ensures the security of personal data handled in India, regardless of the nation of origin. The Act regulates the processing of personal information pertaining to Indian individuals regardless of whether the processing takes place inside or outside of India[26].

The DPDPA does not apply to personal data that is:

- Used for the following reasons:
- Reporting news stories or expressing creative vision
- Internal family or personal matters

### 4.7 Key principles of the DPDPA

Six fundamental ideas form the foundation of the DPDPA:

1. **Lawfulness:** Fairness, transparency, and legal compliance are essential in processing personal data.
2. Purpose Limitation: Any collection of personally identifiable information must have transparent, explicit, and legitimate purposes; any subsequent use of that data must not compromise those aims.
3. **Data Minimisation:** Given the purposes for which it is used, personal data must be adequate, relevant, and minimal.
4. **Accuracy:** Accurate and up-to-date personal information is required.
5. **Limitation on Storage:** Data subjects' personally identifiable information must be retained in a manner that permits identification for no longer than is necessary for the data processing purposes.
6. **Integrity and Confidentiality:** Safeguards against unlawful or unauthorised access, use, or disclosure of personally identifiable information must be in place throughout data processing. processing, and also against accidental destruction, loss, or damage by means of appropriate organisational or technological protections[27].

### 4.8 Rights of data principals

Individuals have many rights under the DPDPA over their personal data, including:

- The right to access their personal data
- The right to rectification of inaccurate personal data
- The right to erasure of their personal data
- The right to restrict the processing of their personal data

---

[25] Illinois Biometric Privacy Act, 740 ILCS 14/1, https://www.illinois.gov/

[26] India Digital Personal Data Protection Act, 2023, Ministry of Electronics and Information Technology, Government of India, https://meity.gov.in

[27] India Digital Personal Data Protection Act, 2023, Ministry of Electronics and Information Technology, Government of India, https://meity.gov.in

### 4.9 Enforcement of the DPDPA

The Data Protection Authority of India (DPA), an impartial organisation tasked with monitoring the Act's application, enforces the DPDPA. The DPA has the authority to look into complaints, impose penalties, and direct businesses to abide with the Act.

### Final thoughts

One important piece of law that will significantly affect how Indian organisations gather, utilise, and exchange personal data is the DPDPA. The Act gives people more control over their personal information and places more stringent requirements on businesses that handle personal information. Organisations covered by the DPDPA need to take action to guarantee that they abide with the Act[28].

## 5. COMPARATIVE ANALYSIS

Significant differences in how various areas view, govern, and implement the protection of personal data are reflected in the worldwide conversation on digital privacy. This section compares the digital privacy policies of Europe, America, and India, looking at their respective ideologies, legal systems, methods of enforcement, and public perceptions.

### 5.1 Philosophical and Cultural Differences in Privacy

Because of the post-war focus on individual liberty and dignity, Europe considers digital privacy to be a basic human right. The GDPR, which prioritises individual rights in data governance, is based on this idea[29].

The United States, on the other hand, views privacy more as a consumer right, emphasising market-driven safeguards and the avoidance of unfair corporate activities. Commercial interests and national security sometimes take precedence over privacy.

India is at a transitional phase as a burgeoning digital economy. India's legal system is now being shaped by the Supreme Court's 2017 recognition of privacy as a basic right, which strikes a balance between citizen rights, fast digitisation, and government-led data projects.

### 5.2 Regulatory Approaches: Centralized vs Sectoral

Europe follows a centralized and comprehensive regulatory model. The GDPR is a unified law applicable across all EU member states, ensuring consistent standards for consent, data processing, breach notification, and penalties.

The U.S. adopts a sectoral and fragmented approach. Laws like HIPAA (healthcare), COPPA (children), and CCPA (California) protect privacy within specific domains, leading to inconsistencies and loopholes across industries and states.

India is moving towards a centralized model with the DPDPA 2023, but its framework is still evolving. The Act aims to regulate data processing, storage, and transfers, although implementation remains a challenge due to infrastructural and administrative constraints.

### 5.3 Enforcement Mechanisms and Penalties

With strong data protection authorities (DPAs) spread across the EU and the authority to impose hefty fines up to 4% of a company's worldwide revenue under the GDPR Europe's enforcement is strict.

Enforcement in the United States is often decentralised, with organisations such as the Federal Trade Commission (FTC) acting in response to particular infractions. The severity of penalties varies greatly, and enforcement is often reactive rather than proactive.

The establishment of a Data Protection Board for enforcement is suggested under India's DPDPA 2023. But questions still surround its autonomy, ability, and readiness to deal with pervasive infractions in a nation with more than a billion internet users.

### 5.4 Impact on Businesses and Consumers

Businesses operating in Europe are subject to stringent compliance requirements, including required data officer appointments and Data Protection Impact Assessments (DPIAs). Strong rights for consumers include access, deletion, and data portability.

Although American companies gain from more freedom, they also face hazards to their image and growing calls for government control. Because of conflicting legislation, consumers often lack clarity and control over their data.

---

[28] Data Protection Authority of India (DPA), "Enforcement and Monitoring of the India Digital Personal Data Protection Act, 2023," Ministry of Electronics and Information Technology, https://meity.gov.in

[29] General Data Protection Regulation (GDPR), European Parliament and Council of the European Union, Regulation (EU) 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj

Although there are obstacles due to a lack of knowledge and inadequate preparation, Indian firms are starting to comply with the new rule. Despite the ongoing development of digital literacy and redressal methods, consumers are increasingly becoming more aware of their rights.

### 5.5 Public Awareness and Digital Literacy

Because of years of lobbying, media attention, and open regulations, public awareness is comparatively high in Europe. The majority of citizens are knowledgeable of their rights and how to use them.
Although awareness is increasing in the United States, especially with regard to corporate spying and data exploitation, it is still uneven because of the complicated legal system.
Public awareness is poor in India, particularly among low-income and rural populations. The digital gap must be closed, and privacy education must be promoted in government initiatives, businesses, and educational institutions[30].
According to this comparative research, India is working to create a fair and inclusive regulatory framework, the United States depends on disjointed sectoral regulations driven by market forces, and Europe leads the world in privacy protection with a rights-based and united approach. In order to shape future international data privacy cooperation and policy harmonisation, it is essential to comprehend these discrepancies.

## 6. CASE LAWS

### Europe

**Google Spain SL v Agencia Española de Protección de Datos[31]**

### Case C-131/12

### Facts

Mario Costeja González, a Spanish resident, filed a complaint with the Spanish Data Protection Agency (AEPD) against Google Spain, "Google Inc., as well as the newspaper La Vanguardia. The citizen was dissatisfied with the websites that appeared in Google search results when his name was entered. Following procedures to retrieve Mr. Costeja González's social security arrears, the pages included a notice for a real estate sale.
Since La Vanguardia had lawfully published the content, the AEPD rejected the accusation against it but upheld the complaint against both Google firms, ordering them to delete the personal data from their indexes. To challenge the AEPD decision, Google Inc. as well as Google Spain took legal action by suing the High Court. The Spanish High Court sent the matter to the CJEU as part of its preliminary determination procedure.

### Issue

1) Are Google's search result compilation operations categorised as activities covered by the Data Protection Directive (Directive 95/46)? In particular:
a) Does Google undertake data processing?
b) Is Google a data controller?
2) Can Google's operations be governed by the Data Protection Directive in terms of territory?
3) Thirdly, may individuals use their right to have search engines delete their personal information?

### Comment

The lawsuit emphasises Google's and other businesses' data protection responsibilities in the EU, which include systems that must respond to requests to delete erroneous or unnecessary data. The court did not, however, provide any instructions on how to strike a balance between individual privacy and the public's right to access all documents. There have been concerns expressed over the effect of aggregating personal data and search engines' decision to choose what the general public may readily access. Because non-EU versions of search engines may be used to get around data removal, its efficacy was also questioned. How the "right to be forgotten" will be implemented globally is still up in the air while new EU legislation are being developed.

### AMERICA

**Riley v. California (2014)[32]**

### 134 S.Ct. 2473

### Case Summary and Outcome

A warrantless search and seizure of digital material from a mobile phone during an arrest violates the 4th Amendment to the US Constitution, according to the US Supreme Court. After pulling a man up for using a vehicle with a registration that had already expired, the arresting officer checked his phone. "Cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person," the court ruled, and as a result, a search warrant is often required.

---

[30] India Digital Personal Data Protection Act, 2023, Ministry of Electronics and Information Technology, Government of India, https://meity.gov.in
[31] Google Spain SL v Agencia Española de Protección de Datos, Case C-131/12
[32] Riley v. California (2014), 134 S.Ct. 2473

### Facts

Riley's mobile phone was confiscated during a normal inventory check of his vehicle, and he was detained during a traffic stop. After examining the phone, police discovered evidence that resulted in accusations of attempted murder and gunshot. Riley moved to suppress the evidence, claiming the search violated his Fourth Amendment rights. The appeals court upheld the trial court's denial of the request.

Police confiscated Wurie's two mobile phones and detained him for narcotics peddling in a different case. After getting a warrant, police used one phone to locate a location, which they then searched, finding guns and narcotics. Wurie attempted to have the evidence suppressed," but the appeals court decided that since mobile phones hold a lot of personal information, a search warrant is necessary.

In both decisions, the U.S. Supreme Court rejected the claim that mobile phones fall within the search consequent to arrest exemption, ruling that a warrant is necessary before searching a cell phone that has been confiscated during an arrest. The Court stressed that while mobile phones are neither a danger to officer safety or a method of escape, they nevertheless carry a considerable amount of personal data.

### INDIA

**K.S. Puttaswamy (Retd.) v. Union of India (2017) (Right to Privacy Case)[33]**
**(2017) 10 SCC 1**

### KEY FACTS:

Justice K.S. Puttaswamy (Retd.), a former judge of the Madras High Court, challenged the legality of the Aadhaar system. He said that the scheme violated individuals' privacy. The right to privacy in India has to be determined by a higher court, says a three-judge panel. A nine-judge panel reached a verdict in this matter.

### ISSUES & DECISION:

It was determined by the Court that the right to privacy must be considered in conjunction with the rights to life and liberty under Article 21 of the Constitution.

### The Rights Framework

In order to protect individual choices and important life decisions, such as sexual orientation, the Court acknowledged that privacy is a fundamental component of human dignity. It said that sexual orientation discrimination erodes one's sense of self-worth and dignity. According to Articles 15 and 21 of the Constitution, the right to privacy is fundamental to one's identity, autonomy, and dignity and is necessary for equality and nondiscrimination.

The Court upheld the idea that privacy is protected by other basic rights in addition to Article 21. It recognised that regardless of gender, class, or economic standing, everyone has the inherent freedom to choose their own sexual orientation.

It demanded that India uphold its human rights obligations, using the UN Declaration of Human Rights and the International Covenant on Civil and Political Rights. Furthermore, the Supreme Court reversed its decision in Suresh Koushal v. Naz Foundation, stating that the foundation of LGBT rights is respect for individual privacy and dignity, and that fundamental rights should not be determined by popular opinion.

The Court ruled that everyone has the right to privacy and autonomy, regardless of socioeconomic background, rejecting the claim that privacy is a benefit enjoyed by a select few. It recognised that laws might restrict privacy as long as they were justifiable, fair, and reasonable.

This ruling was important because it acknowledged the rights of the LGBT community to privacy and self-determination, which prepared the way for the Navtej Singh Johar v. State of India (2017) challenge against Section 377 of the Indian Penal Code.

## 7. CONCLUSION

The legislative traditions, cultural values, political interests, and degrees of digital maturity of Europe, America, and India all influence their unique approaches to digital privacy. The GDPR, which establishes a worldwide standard for the protection of personal data and human liberty, is a prime example of Europe's robust, rights-based framework. In contrast, the United States has a sectoral and market-driven approach, providing disjointed safeguards that differ by state and industry and often putting business interests and innovation ahead of consistent privacy norms. With the recent passage of the DPDPA, 2023, India is forging forward by attempting to strike a balance between the interests of the state, economic expansion, and citizen rights in a society that is increasingly digitizing.

Every system has advantages and disadvantages, but as the digital world becomes more interconnected, there is a need for cooperation that is more international, standardization, and more robust enforcement. In order to guarantee efficient and comprehensive digital privacy protection, it is also crucial to raise public awareness, fortify institutional capacities, and promote privacy-conscious technical advancement. This comparative study

[33] K.S. Puttaswamy (Retd.) v. Union of India (2017) (Right to Privacy Case), (2017) 10 SCC 1

emphasizes the need of a globally consistent but locally flexible framework that protects privacy as a basic right and promotes innovation and technological advancement.

## References


1. Agarwal, A. (2020). Sanctity of Personal Data: a Comparative Study of Data Privacy Laws in Eu, Us and India. *International Journal of Legal Developments and Allied Issues*, *6*(3), 152–189.
2. Bloom-Feshbach, K., Alonso, W. J., Charu, V., Tamerius, J., Simonsen, L., Miller, M. A., & Viboud, C. (2013). Latitudinal Variations in Seasonal Activity of Influenza and Respiratory Syncytial Virus (RSV): A Global Comparative Review. *PLoS ONE*, *8*(2), 3–4. https://doi.org/10.1371/journal.pone.0054445
3. Brain, I. Y., Article, T., Journal, I., Science, L., Journal, I., Science, L., Journal, I., & Science, L. (2024). *INTERNATIONAL JOURNAL OF LEGAL A Comparative Study of the Evaluation on the Right to Privacy in India and the UK , Their Legal Frameworks and Judicial Interpretation : A Cyber Law Perspective*. 600–628.
4. Glenn, E. N. (2015). Settler Colonialism as Structure: A Framework for Comparative Studies of U.S. Race and Gender Formation. *Sociology of Race and Ethnicity*, *1*(1), 52–72. https://doi.org/10.1177/2332649214560440
5. Guess, A. M., Lerner, M., Lyons, B., Montgomery, J. M., Nyhan, B., Reifler, J., & Sircar, N. (2020). A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. *Proceedings of the National Academy of Sciences of the United States of America*, *117*(27), 15536–15545. https://doi.org/10.1073/pnas.1920498117
6. Hanafizadeh, P., Keating, B. W., & Khedmatgozar, H. R. (2014). A systematic review of Internet banking adoption. *Telematics and Informatics*, *31*(3), 492–510. https://doi.org/10.1016/j.tele.2013.04.003
7. Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. *International Journal of Press/Politics*, *25*(3), 493–516. https://doi.org/10.1177/1940161219900126
8. Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., & Gill, P. (2018). Apps, Trackers, Privacy, and Regulators A Global Study of the Mobile Tracking Ecosystem. *25th Annual Network and Distributed System Security Symposium, NDSS 2018*, *February*. https://doi.org/10.14722/ndss.2018.23353
9. Sharon, T. (2021). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, *23*(s1), 45–57. https://doi.org/10.1007/s10676-020-09547-x
10. Sheth, S., Kaiser, G., & Maalej, W. (2014). Us and them: A study of privacy requirements across north america, asia, and Europe. *Proceedings - International Conference on Software Engineering*, *1*, 859–870. https://doi.org/10.1145/2568225.2568244
11. Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the internet of things: Threats and challenges. *Security and Communication Networks*, *7*(12), 2728–2742. https://doi.org/10.1002/sec.795
12. European Union, *General Data Protection Regulation (EU) 2016/679*, Official Journal of the European Union, L 119, 4 May 2016, pp. 1–88.
13. Government of India, *The Digital Personal Data Protection Act, 2023*, Act No. 22 of 2023, Ministry of Law and Justice (Legislative Department), 11 August 2023.
14. Solove, Daniel J., *Understanding Privacy*, Harvard University Press, 2008, p. 1–25.
15. Schneier, Bruce, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company, 2015, pp. 35–72.
16. European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016* on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
17. European Commission, "Guidelines on Data Protection Officers ('DPOs')" (2017) WP243 rev.01, Article 29 Data Protection Working Party https://ec.europa.eu/newsroom/article29/items/612048
18. United States Congress, *California Consumer Privacy Act of 2018*, Cal. Civ. Code §§ 1798.100–1798.199 (as amended by the California Privacy Rights Act of 2020), enforced by the California Privacy Protection Agency, https://oag.ca.gov/privacy/ccpa
19. United States Senate, *American Privacy Rights Act of 2024*, Draft Bill, introduced April 2024, available at https://www.commerce.senate.gov/services/files/72F6FA9D-FEC5-47D3-9C95-23276CFA09B5
20. California State Legislature, *California Consumer Privacy Act of 2018*, Cal. Civ. Code §§ 1798.100–1798.199 (amended by the California Privacy Rights Act of 2020), enforced by the California Privacy Protection Agency, https://cppa.ca.gov/regulations/
21. California State Legislature, *Senate Bill 362 (Delete Act)*, Chapter 393, Statutes of 2023, codified at Cal. Civ. Code § 1798.99.82, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB362
22. United States District Court for the Northern District of California, *NetChoice, LLC v. Bonta*, No. 5:22-cv-08861-BLF, Preliminary Injunction Order dated 18 September 2023,

https://www.courtlistener.com/docket/66677606/netchoice-llc-v-bonta/
23. Washington State Legislature, *My Health My Data Act*, Chapter 19.373 RCW, Laws of 2023, https://app.leg.wa.gov/rcw/default.aspx?cite=19.373
24. Nevada Legislature, *Senate Bill No. 370 (Consumer Health Data Privacy Law)*, 82nd Session (2023), effective 31 March 2024, https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10838/Overview
25. Illinois Biometric Privacy Act, 740 ILCS 14/1, https://www.illinois.gov/
26. India Digital Personal Data Protection Act, 2023, Ministry of Electronics and Information Technology, Government of India, https://meity.gov.in
27. India Digital Personal Data Protection Act, 2023, Ministry of Electronics and Information Technology, Government of India, https://meity.gov.in
28. Data Protection Authority of India (DPA), "Enforcement and Monitoring of the India Digital Personal Data Protection Act, 2023," Ministry of Electronics and Information Technology, https://meity.gov.in
29. General Data Protection Regulation (GDPR), European Parliament and Council of the European Union, Regulation (EU) 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj
30. India Digital Personal Data Protection Act, 2023, Ministry of Electronics and Information Technology, Government of India, https://meity.gov.in
31. Google Spain SL v Agencia Española de Protección de Datos, Case C-131/12
32. Riley v. California (2014), 134 S.Ct. 2473
33. K.S. Puttaswamy (Retd.) v. Union of India (2017) (Right to Privacy Case), (2017) 10 SCC 1