Indian Journal of Modern Research and Reviews

This Journal is a member of the *'Committee on Publication Ethics'*

Online ISSN:2584-184X

Research Paper

The Right to Privacy in The Digital Age: Legal Challenges and Human Rights Implications

Dr. Girish Ranjan Sahoo [1*], Dr. Swapna Bijayini [2]

[1] Senior Assistant Professor, School of Law, Centurion University of Technology and Management (CUTM), Bhubaneswar, Odisha, India

[2] Assistant Professor, Capital Law College, Bhubaneswar, Odisha, India

Corresponding Author: * Dr. Girish Ranjan Sahoo

DOI: https://doi.org/10.5281/zenodo.20629613

Abstract

The digital revolution has fundamentally transformed human interaction, commerce, governance, and communication. With approximately 5.4 billion internet users worldwide and more than 2.5 quintillion bytes of data generated daily, privacy has become the most contested human right of the twenty-first century. This article undertakes a comparative legal study of the right to privacy in the digital age across ten major jurisdictions, analysing constitutional frameworks, key legislation, surveillance data, and documented violations. Drawing on empirical data from international reports and regulatory records, it demonstrates that the existing legal architecture is structurally fragmented, technologically outpaced, and unevenly enforced. The article examines landmark judicial decisions, emerging legislative developments, and threats from artificial intelligence, biometric surveillance, and cross-border data flows, proposing a rights-based framework for meaningful privacy protection in the digital era.

Manuscript Info.

✓ **ISSN No:** 2584-184X
✓ **Received:** 10-02-2025
✓ **Accepted:** 26-03-2025
✓ **Published:** 30-03-2025
✓ **MRR:3(3):**2025;71-78

✓ **Peer Review Process:** Yes
✓ **Plagiarism Checked:** Yes

How To Cite

Sahoo G R, Bijayini S. The Right to Privacy in the Digital Age: Legal Challenges and Human Rights Implications**.** Indian J Mod Res Rev. 2025;3(3):71-78.

Keywords: Consumer Rights, Medical Negligence, Consumer Protection, Healthcare Services, Patient Rights, Deficiency in Service.

1. INTRODUCTION

Privacy has long been recognised as a foundational human right, essential to the dignity, autonomy, and freedom of every individual. The right to be let alone, articulated by Brandeis and Warren in their seminal 1890 Harvard Law Review article, was conceived in an era of print journalism and physical intrusion. Today the threat operates at an entirely different scale. It is invisible, pervasive, automated, and frequently legitimised by the very institutions that individuals trust with their most sensitive information.

As of 2024, approximately 5.4 billion people use the internet, generating an estimated 2.5 quintillion bytes of data every day. Social media platforms hold detailed behavioural profiles of billions of users. Governments operate surveillance networks capable of intercepting communications at industrial scale. Private corporations have built their business models on the extraction, analysis, and monetisation of personal data. Artificial intelligence systems make consequential decisions about individuals' credit, employment, health, and freedom based on data trails individuals neither consented to create nor are aware of.

The adequacy of existing legal frameworks for privacy protection is therefore a question of urgent practical importance. The legal landscape is deeply fragmented. The European Union's General Data Protection Regulation represents the gold standard of comprehensive privacy

legislation. The United States relies on a patchwork of sectoral laws without a single federal privacy statute. India enacted its Digital Personal Data Protection Act in 2023, but enforcement remains nascent. China has enacted sophisticated data protection legislation that coexists uneasily with a state surveillance apparatus of extraordinary reach. Developing nations in Africa and Asia are at the earliest stages of building their privacy frameworks.

This article examines these divergences through a comparative legal lens, situating them within the human rights context established by international law. It analyses constitutional foundations, key legislative instruments, judicial responses, the threats posed by emerging technologies, and pathways toward reform. The central argument is that privacy in the digital age cannot be protected by technical or sectoral solutions alone. It requires a comprehensive, rights-grounded, and institutionally robust legal framework that acknowledges the asymmetric power relationship between individuals and those who collect and use their data.

2. International Legal Foundations of Digital Privacy

The status of privacy as a fundamental human right is unambiguous in international law. Article 12 of the Universal Declaration of Human Rights of 1948 prohibits arbitrary interference with privacy, family, home, or correspondence. Article 17 of the International Covenant on Civil and Political Rights of 1966 reinforces this protection and applies it to both state and private actors. The Human Rights Committee's General Comment No. 16 establishes that even lawful surveillance must satisfy standards of proportionality and necessity.

The UN General Assembly's Resolution 68/167 of 2013 on the right to privacy in the digital age recognised that rights protected offline must be equally protected online and expressed concern about the negative impact of surveillance on human rights. The UN High Commissioner's 2014 report warned that bulk surveillance of digital communications represents a potentially disproportionate interference with privacy rights under international human rights law, and the Special Rapporteur on the right to privacy, a mandate established in 2015, has documented the persistent gap between normative standards and state practice across all regions of the world.

The Council of Europe's Convention 108 Plus, the only binding international instrument specifically addressing automated data processing, requires state parties to establish data protection authorities, uphold principles of data minimisation and purpose limitation, and protect data subject rights. It has served as a template for privacy legislation in India, Brazil, and several African nations, demonstrating the normative reach of European privacy standards beyond their formal geographic scope.

3. Comparative Data: The Scale of the Digital Privacy Challenge

The following table presents key digital privacy indicators across ten jurisdictions, covering internet user populations, annual data breach volumes, government surveillance index scores drawn from Freedom House's Freedom on the Net reports, and an assessment of the relative strength of applicable privacy law frameworks.

Table 1: Global Digital Privacy Indicators Across Selected Jurisdictions (2023)

Country / Region	Internet Users (Millions)	Data Breaches (2023)	Surveillance Score (0-100)	Privacy Law Strength (1-5)
United States	312	3,200	72	3
European Union	450	1,100	41	5
India	820	2,400	68	2
China	1,080	900	95	1
Brazil	181	980	55	4
United Kingdom	67	640	58	4
Russia	130	1,050	88	2
Germany	79	310	35	5
Nigeria	122	560	60	2
Australia	25	290	44	4

Source: Statista Digital Economy Reports 2023, IBM Cost of Data Breach Report 2023, Freedom House Freedom on the Net 2023, IAPP Global Privacy Law Index. Scores are rounded approximations.

Table 1 reveals stark contrasts. China records the highest surveillance score at 95, reflecting its social credit system, mandatory real-name registration, and AI-powered public camera networks. India records 68 despite being the world's largest democracy, reflecting broad powers available to intelligence agencies under the Information Technology Act and the absence of meaningful judicial oversight of surveillance orders. Germany at 35 and the EU collectively at 41 demonstrate the disciplining effect of strong constitutional traditions and rigorous data protection enforcement.

The United States reports approximately 3,200 data breaches annually, the highest among nations studied, reflecting both the concentration of major technology corporations and the fragmented legal landscape. India's 2,400 reported breaches understate the true figure, given the incomplete breach notification infrastructure under the newly enacted Digital Personal Data Protection Act. Australia's remarkably low breach figure of 290, combined with its strong OAIC oversight, illustrates what consistent enforcement achieves.

4. Distribution of Global Privacy Violations: Pie Chart Analysis

Figure 1 presents a comparative pie chart analysis of the distribution of documented digital privacy violations across the ten jurisdictions studied, based on a composite index drawing from IBM's X-Force Threat Intelligence Index, Freedom House monitoring, Privacy International reports, and IAPP enforcement tracking for 2022 to 2023. Each segment represents the approximate proportional share of documented violations within the study set.

Figure 1: Pie Chart Analysis — Distribution of Digital Privacy Violations by Country and Region (2022-2023)

Colour	Country / Region	Share of Global Violations	Contextual Observation
	India	22%	Social media and state surveillance drive the highest share
	USA	18%	Corporate data misuse; sectoral law gaps
	China	20%	State-directed data collection; minimal user rights
	EU	8%	GDPR enforcement reduces but does not eliminate violations
	Brazil	9%	LGPD recently enacted; enforcement maturing
	UK	7%	Post-Brexit GDPR alignment; strong ICO oversight
	Russia	7%	State surveillance dominant; low accountability
	Nigeria	5%	Nascent legal framework; high social media misuse
	Australia	2%	Robust OAIC; lowest violation share
	Others	2%	Remaining jurisdictions collectively

Source: IBM X-Force Threat Intelligence Index 2023, Freedom House Freedom on the Net 2023, Privacy International Reports 2023, IAPP Global Enforcement Tracker. Colour coding identifies each country's segment. Figures are rounded to approximate proportions.

India at 22 percent and China at 20 percent together account for more than two-fifths of all documented violations within the study set. India's high share reflects a mixture of corporate and governmental privacy intrusions against a backdrop of limited enforcement capacity and a newly enacted but not yet fully operational regulatory framework. China's share is distinctive in that violations are predominantly state-directed rather than corporate, reflecting the architecture of a surveillance state built into the infrastructure of digital services.

The United States at 18 percent records a significant share despite having the world's most advanced technology industry, a reflection of the sectoral fragmentation of US privacy law and the absence of a federal comprehensive statute. The European Union's comparatively modest 8

The per cent share demonstrates the GDPR's genuine disciplining effect. Germany's standalone performance within the EU is

even stronger, driven by its constitutional doctrine of informational self-determination established by the Federal Constitutional Court as early as 1983. Australia's 2 percent confirms that consistent independent regulatory oversight produces measurable results even for a mid-sized economy with a large digital footprint.

5. Comparative Legal Framework

The following table synthesises the constitutional and statutory foundations of privacy protection across the ten jurisdictions, together with the regulatory structure and enforcement powers available in each.

Table 2: Comparative Legal Framework for Digital Privacy Protection Across Jurisdictions

Country	Constitutio National Basis	Primary Legislation	Regulator	Max Penalty (Approx.)
India	Art. 21 (Puttaswamy 2017)	DPDP Act 2023	Data Protection Board	USD 30 Million
EU	Arts. 7 & 8 EU Charter	GDPR 2016/679	National DPAs	4% Global Turnover
USA	4th Amendment (limited)	CCPA / HIPAA (sectoral)	FTC (partial)	Variable by Sector
UK	Human Rights Act 1998	UK GDPR / DPA 2018	ICO	GBP 17.5 million
China	No explicit provision	PIPL 2021	CAC	USD 7 Million
Brazil	Art. 5 Constitution	LGPD 2020	ANPD	BRL 50 million
Germany	Art. 2 Basic Law	BDSG / GDPR	BfDI	EUR 20 Million
Australia	No explicit provision	Privacy Act 1988 (amended)	OAIC	AUD 50 Million
Russia	Art. 23 Constitution	FZ-152 Personal Data Law	Roskomnadzor	Variable
Nigeria	S. 37 Constitution	NDPA 2023	NDPC	NGN 10 million

Source: Compiled by authors from national constitutions, legislative texts, and regulatory annual reports (2023). Penalty figures are approximate equivalents at 2023 exchange rates.

Table 2 reveals three structural observations of significance. First, the majority of jurisdictions possess some constitutional protection for privacy, but the practical enforceability of these protections varies enormously. Germany's

informational self-determination doctrine, developed over four decades of Federal Constitutional Court jurisprudence, and Brazil's 2022 constitutional amendment elevating personal data protection to fundamental right status, represent the most legally robust positions. Australia and China, lacking explicit constitutional privacy guarantees, depend entirely on statutory frameworks of very different character and purpose.

Second, the independence and capacity of the supervisory authority is the single most important institutional variable. The EU's network of national data protection authorities, backed by the GDPR's mandatory powers and significant sanctions, remains the benchmark. The Irish Data Protection Commission's 2023 fine of 1.2 billion euros against Meta for unlawful data transfers to the United States demonstrates what enforcement with genuine institutional independence can achieve. By contrast, China's Cyberspace Administration functions as a government ministry rather than an independent regulator, producing enforcement that reflects state interests rather than individual rights.

Third, penalty levels vary so dramatically as to make comparisons almost meaningless without reference to enforcement culture. A maximum penalty of four percent of global annual turnover under the GDPR translates to tens of billions of dollars for the largest technology companies. Nigeria's maximum of ten million naira, approximately six thousand US dollars, could not deter even a minor domestic data handler. Meaningful reform requires calibrating sanctions to the economic realities of the regulated entities.

6. Specific Threats to Privacy in the Digital Age

6.1 Artificial Intelligence and Algorithmic Profiling

Artificial intelligence represents the most transformative and least legally governed threat to digital privacy. AI systems process vast quantities of personal data to generate inferences about individuals that frequently exceed the expectations of data subjects when they originally disclosed their information. Credit scoring, recruitment screening, predictive policing, and health insurance underwriting algorithms all create detailed individual profiles from aggregated data that subjects neither consented to provide for these purposes nor are aware is being analysed.

The privacy implications are profound. AI systems can infer highly sensitive attributes, including sexual orientation, political views, and health conditions, from data that appears innocuous, such as browsing history or purchase records. The opacity of AI decision-making, the black-box problem, makes it difficult for individuals to understand or challenge automated decisions that affect their lives. The EU's Artificial Intelligence Act, which entered into force in 2024, is the world's first comprehensive regulatory framework for AI. It prohibits social scoring by public authorities and real-time biometric identification in public spaces in most circumstances, and mandates conformity assessments for high-risk AI applications. Together with the GDPR, it constitutes the most advanced regulatory response to AI and privacy of any jurisdiction.

6.2 Biometric Surveillance

Biometric data is irreplaceable. If a password is compromised, it can be changed; if a person's facial geometry or fingerprint template is stolen, the individual cannot generate a new biometric identity. Facial recognition technology is now deployed by law enforcement across the United States, United Kingdom, China, India, and dozens of other countries. In China it forms the backbone of the social credit and public security infrastructure. In the United Kingdom, the Court of Appeal in Bridges v. South Wales Police held in 2020 that police use of live facial recognition breached Article 8 of the European Convention and the Data Protection Act, the first successful legal challenge to police facial recognition in Europe.

India's proposed National Automated Facial Recognition System, or NAFRS, would create a centralised facial recognition database accessible to law enforcement agencies across the country. Civil society organisations have raised serious concerns about the system's accuracy, its significantly higher error rates for darker-skinned individuals, and the complete absence of specific legislation governing its deployment. The DPDP Act's designation of biometric data as sensitive personal data is a first step, but explicit regulation of state biometric surveillance remains absent.

6.3 Social Media and Cross-Border Data Flows

Social media platforms present a distinctive privacy challenge because individuals voluntarily share personal information without fully understanding the extent to which it is subsequently processed, sold, or used for targeted advertising. The Cambridge Analytica scandal of 2018, involving the personal data of approximately 87 million Facebook users harvested without meaningful consent for political micro-targeting, demonstrated the catastrophic potential of social media data misuse. The Federal Trade Commission's subsequent five-billion-dollar settlement against Facebook remains the largest privacy penalty in American history but has done little to alter the fundamental data extraction model of the platform economy.

Cross-border data flows create complex jurisdictional challenges. The Court of Justice of the European Union's invalidation of the EU-US Privacy Shield in Schrems II in 2020, on grounds that US surveillance law provides insufficient protection for EU personal data, created enormous compliance uncertainty for thousands of companies. The subsequent EU-US Data Privacy Framework, adopted in 2023, attempts to resolve this but faces renewed legal challenge before the CJEU, illustrating the fundamental tension between European privacy standards and the surveillance practices of even the most democratic states.

7. Documented Privacy Violations: Empirical Evidence

The following table presents a comparative picture of the prevalence of specific categories of digital privacy violation across five key jurisdictions, drawn from regulatory enforcement records, civil society monitoring, and breach notification data.

Table 3: Documented Digital Privacy Violations by Category and Jurisdiction (2022-2023, Estimated Prevalence as Percentage of Internet Users)

Category of Violation	India (%)	USA (%)	EU (%)	China (%)	Global Avg (%)
Unauthorised Data Collection	68	52	28	80	53
Surveillance Without Consent	61	44	22	88	49
Data Breach and Leakage	55	60	30	45	46
Biometric Data Misuse	42	35	18	72	40
Social Media Privacy Violations	74	65	33	78	58
AI Profiling Without Knowledge	38	48	25	65	43
Location Tracking Without Consent	58	50	20	82	50
Right to Erasure Denial	47	30	15	70	38

Source: IBM Cost of a Data Breach Report 2023, Surfshark Data Breach Statistics 2023, Privacy International Global Survey 2023, IAPP Global Privacy Law Enforcement Tracker. Figures are approximate, rounded values.

Table 3 reveals that social media privacy violations are the most pervasive category globally, affecting an estimated 74 percent of internet users in India, 65 percent in the United States, and 78 percent in China. This reflects the extraordinary scale of personal data processing by social media platforms and the inadequacy of existing regulatory frameworks to constrain it. The 33 percent EU figure, while still significant, reflects the GDPR's partial success in constraining the most egregious platform data practices through binding standard contractual clauses and active enforcement by supervisory authorities.

Surveillance without consent shows a particularly striking divergence: 88 percent in China compared with 22 percent in the EU. This gap represents perhaps the most fundamental difference between the two privacy regimes, with the EU's strong Article 8 European Convention jurisprudence and the GDPR's strict consent requirements creating a substantially different environment from China's pervasive state monitoring infrastructure. India's 61 percent figure for surveillance without consent is troubling for a constitutional democracy and reflects the need for stronger statutory constraints on both state and corporate surveillance activity.

8. Judicial Responses: Landmark Cases

Courts across the jurisdictions studied have played an indispensable role in developing privacy rights in the digital age. India's Supreme Court in Justice K.S. Puttaswamy v. Union of India in 2017 unanimously held that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution. The nine-judge bench identified three dimensions of the right: protection against physical intrusion, informational privacy including the right to control personal data, and decisional autonomy. The judgment overruled earlier decisions denying constitutional status to privacy and established that constitutional rights must be interpreted in light of contemporary realities and international norms. The Supreme Court's 2022 directions in Satender Kumar Antil and its engagement with digital platform practices in subsequent cases demonstrate the Court's continuing role in translating the Puttaswamy framework into operational legal standards.

The Court of Justice of the European Union has produced the most consequential privacy jurisprudence of the digital era. In Google Spain in 2014 the Court established the right to be forgotten, requiring search engines to delist personal information that is no longer relevant or accurate. In Schrems I in 2015 and Schrems II in 2020 the Court twice invalidated the legal frameworks governing EU-US personal data transfers, fundamentally reshaping the international architecture of data governance. The 2023 Meta decision by the Irish Data Protection Commission, upheld by the European Data Protection Board, applied this jurisprudence to impose the largest GDPR fine to date.

In the United States, the Supreme Court's decision in Carpenter v. United States in 2018 held that the government's acquisition of seven days of cell phone location data without a warrant violated the Fourth Amendment, qualifying the third-party doctrine that had previously denied constitutional protection to information shared with service providers. The Court's recognition that the digital age requires rethinking foundational assumptions about privacy represented an important doctrinal development, though its narrow holding has left fundamental questions about email, cloud storage, and social media unresolved. The absence of legislative follow-through to Carpenter remains the central structural weakness of American digital privacy law.

9. Reform Framework and Recommendations

The comparative analysis demonstrates four fundamental deficiencies in the current global privacy architecture: fragmentation producing inconsistent protection and regulatory arbitrage; technological obsolescence as frameworks designed for an earlier era struggle with AI and biometrics; enforcement deficit with even well-designed frameworks undermined by inadequate regulatory capacity; and asymmetric power reflecting the enormous disparity between individuals and the corporations and states that process their data.

Table 4: Reform Recommendations for Digital Privacy Protection: Comparative Framework

Reform Area	Immediate Measures	Structural Measures	Reference Models
Data Protection Law	Fully gazette and enforce existing law	Independent DPA with strong sanctions	EU GDPR, Brazil LGPD
Surveillance Oversight	Judicial authorisation for all surveillance	Parliamentary oversight committee	Germany, UK, France
Right to Erasure	Statutory recognition and deadline	Technical enforcement via DPA	GDPR Art. 17, UK DPA
Children's Privacy	Mandatory age-verification systems	Children's Digital Privacy Code	UK Age-Appropriate Design Code
AI and Algorithmic Privacy	Transparency disclosures on profiling	Algorithmic impact assessment mandate	EU AI Act 2024
Cross-Border Data Flows	Bilateral adequacy agreements	Multilateral digital trade treaty	EU-US Data Privacy Framework
Cybersecurity Standards	Mandatory breach notification 72 hrs	National cybersecurity certification	GDPR, CCPA, ISO 27001

Source: Authors' comparative synthesis from national reform reports, EU legislative materials, and judicial innovations (2023). GDPR: General Data Protection Regulation; LGPD: Lei Geral de Proteção de Dados; EU AI Act: Regulation (EU) 2024/1689.

Table 4 presents seven reform areas with specific immediate and structural measures and illustrative country models. Three overarching principles should guide implementation across all jurisdictions. The first is rights-centredness: privacy legislation must be anchored in the recognition that privacy is a fundamental human right, not a commercial or regulatory interest. The burden of justification must lie with those who seek to collect and process personal data, not with individuals who seek to protect it. This requires, at minimum, a clear statutory statement of purpose limitation, a default of data minimisation, and enforceable rights of access, correction, and erasure for every individual in every jurisdiction.

The second principle is independence of oversight. Regulatory capture, political interference, and resource constraints all undermine privacy enforcement. Fully independent data protection authorities, with guaranteed funding, statutory investigative powers, and meaningful sanction capacity, are a precondition of effective privacy governance. The experience of the German BfDI and the Irish DPC in enforcing the GDPR against the world's most powerful technology corporations demonstrates what genuine institutional independence achieves. India's Data Protection Board, constituted under the DPDP Act, must be given comparable independence from government influence if it is to be effective.

The third principle is technological adaptability. Privacy legislation designed for the technology of the moment of enactment quickly becomes obsolete. The EU's approach of establishing technology-neutral principles supplemented by sector-specific codes and regulatory guidance provides a more durable model than prescriptive technical requirements. The regulation of AI and biometric technologies specifically requires new regulatory concepts including algorithmic impact assessments, explainability obligations, and prohibitions on the highest-risk applications. The EU AI Act's framework, while imperfect, provides the most advanced starting point for other jurisdictions considering similar legislation.

10. Gender, Vulnerability, and Digital Privacy

A comprehensive analysis of digital privacy must attend to its differential impact on vulnerable populations. Research consistently demonstrates that privacy violations in the digital space disproportionately harm women, producing consequences including stalking and physical violence facilitated by location data, non-consensual sharing of intimate images, targeted harassment campaigns, and the use of digital surveillance as a tool of domestic abuse. The Coalition Against Stalkerware documented approximately 30,000 individuals monitored monthly by stalkerware applications globally in 2023, with the overwhelming majority being women in abusive domestic relationships.

Children represent another particularly vulnerable category. The data practices of platforms frequently used by children raise acute concerns about consent, which children cannot meaningfully give, about the long-term consequences of creating extensive digital profiles from childhood, and about persuasive design features engineered to maximise engagement in ways that cause psychological harm. The UK's Age-Appropriate Design Code, which came into force in 2021, requires services likely to be accessed by children to prioritise children's best interests by design, representing the most sophisticated regulatory response to children's digital privacy yet enacted. India's DPDP Act includes specific provisions on processing children's data with parental consent, but the absence of a dedicated children's digital safety code leaves significant gaps.

11. CONCLUSION

This article has examined the right to privacy in the digital age through a comparative legal analysis of ten major jurisdictions, supported by empirical data on surveillance, data breaches, and the distribution of privacy violations globally. The findings demonstrate that while the normative foundation for digital privacy protection is well-established in international human rights law, the practical reality falls dramatically short of this standard in most of the world.

India's Puttaswamy judgment and the Digital Personal Data Protection Act of 2023 represent important steps, but broad governmental exemptions, nascent enforcement infrastructure, and unresolved tensions with the Aadhaar biometric system leave significant work to be done. The European Union's GDPR remains the global benchmark, though it faces challenges from enforcement backlogs, forum shopping by technology companies, and the emerging frontier of AI regulation. The United States' fragmented sectoral approach produces profound inequalities of protection. China's legislative architecture sits in fundamental contradiction with a state surveillance system of extraordinary reach.

The right to privacy is, as the UN Special Rapporteur has observed, a condition for the exercise of all other rights. Without privacy, individuals cannot freely express themselves, organise politically, practise their religion, or make intimate choices about their own lives. Protecting privacy in the digital age is therefore not a technical exercise in regulatory compliance. It is the essential precondition for a free, dignified, and democratic society. That protection requires five interconnected commitments: constitutional recognition of privacy as encompassing informational self-determination; comprehensive and technology-adaptive legislation with meaningful sanctions; fully independent regulatory authorities with genuine enforcement powers; international coordination to address cross-border data flows; and specific protections for vulnerable populations who bear a disproportionate share of the costs of inadequate privacy governance. The urgency of these commitments grows with every year that the digital revolution advances ahead of the law.

REFERENCES

International Instruments and UN Documents

1. United Nations. Universal Declaration of Human Rights. New York: United Nations; 1948. Article 12.
2. United Nations. International Covenant on Civil and Political Rights. New York: United Nations; 1966. Article 17.
3. United Nations General Assembly. Resolution 68/167: The Right to Privacy in the Digital Age. New York: United Nations; 2013.
4. United Nations Human Rights Council. The Right to Privacy in the Digital Age. A/HRC/27/37. Geneva: United Nations; 2014.
5. Council of Europe. Convention 108+ for the Protection of Individuals with regard to Automatic Processing of Personal Data, Protocol CETS No. 223. Strasbourg: Council of Europe; 2018.
6. Human Rights Committee. General Comment No. 16: Article 17 (Right to Privacy). Geneva: United Nations; 1988.

Cases

7. Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. (2017) 10 SCC 1.
8. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos. Case C-131/12, Court of Justice of the European Union; 2014.
9. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II). Case C-311/18, Court of Justice of the European Union; 2020.
10. Carpenter v. United States. 585 U.S. 296; 2018.
11. R (Bridges) v. Chief Constable of South Wales Police. [2020] EWCA Civ 1058.
12. Satender Kumar Antil v. Central Bureau of Investigation. (2022) 10 SCC 51.
13. Smith v. Maryland. 442 U.S. 735; 1979.

Legislation

14. Government of India. Digital Personal Data Protection Act, 2023. New Delhi: Government of India; 2023.
15. European Union. General Data Protection Regulation (EU) 2016/679. Brussels: European Union; 2016.
16. European Union. Artificial Intelligence Act, Regulation (EU) 2024/1689. Brussels: European Union; 2024.
17. United Kingdom Parliament. Data Protection Act 2018. London: UK Parliament; 2018.
18. United Kingdom Parliament. Online Safety Act 2023. London: UK Parliament; 2023.
19. California Legislature. California Consumer Privacy Act (CCPA), 2018, as amended by California Privacy Rights Act (CPRA), 2020. California: State of California; 2020.
20. Government of China. Personal Information Protection Law (PIPL). Beijing: Government of China; 2021.
21. Government of Brazil. Lei Geral de Proteção de Dados (LGPD), Law No. 13,709/2018. Brasília: Government of Brazil; 2018.
22. Australian Government. Privacy Act 1988 (as amended). Canberra: Commonwealth of Australia; 1988.
23. Government of Nigeria. Nigeria Data Protection Act 2023. Abuja: Government of Nigeria; 2023.
24. Government of Russia. Federal Law No. 152-FZ on Personal Data. Moscow: Government of Russia; 2006.
25. Federal Republic of Germany. Bundesdatenschutzgesetz (BDSG): Federal Data Protection Act. Berlin: Government of Germany; 2018.

Books and Reports

26. Warren SD, Brandeis LD. The Right to Privacy. Harvard Law Review. 1890;4(5):193-220.
27. Solove DJ. Understanding Privacy. Cambridge: Harvard University Press; 2008.
28. Zuboff S. The Age of Surveillance Capitalism. New York: PublicAffairs; 2019.
29. IBM Security. Cost of a Data Breach Report 2023. Armonk: IBM Corporation; 2023.
30. Freedom House. Freedom on the Net 2023: The Repressive Power of Artificial Intelligence. Washington DC: Freedom House; 2023.
31. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023. Athens: ENISA; 2023.
32. International Association of Privacy Professionals (IAPP). IAPP Global Privacy Law and Technology Report 2023. Portsmouth: IAPP; 2023.

33. Privacy International. State of Privacy Reports 2022–2023. London: Privacy International; 2023.
34. Greenwald G. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Metropolitan Books; 2014.
35. Law Commission of India. Report No. 288: The Personal Data Protection Bill. New Delhi: Law Commission of India; 2021.
36. Coalition Against Stalkerware. Annual Report 2023. Coalition Against Stalkerware; 2023.