International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 26-02-2026, Accepted: 29-03-2026, Published: 13-04-2026
Volume 12, Issue 2, 2026, Page No. 84-87

Right To Privacy As A Human Right In The Digital Age comparative models, Ai Governance and International Human Rights

Sheela Kumari
Assistant Professor, Law, Maa Ambe K.P. Sanghvi Govt Law College, Sirohi, Rajasthan, India

Abstract
Building on the recognition of privacy as a fundamental right in Indian constitutional law, this second part examines how different constitutional systems and international regimes conceptualise and protect privacy in an era of digital transformation. It analyses the European Union's strong regulatory framework under the GDPR and the Artificial Intelligence Act, and compares this with privacy protections developed in Canada, Australia, the United Kingdom, and South Africa, with particular focus on the central role of proportionality and independent oversight of surveillance powers. The article then turns to emerging privacy risks generated by artificial intelligence and algorithmic governance, including large-scale profiling, systemic opacity, discriminatory outcomes, and automated decision-making, and evaluates how far current Indian law responds to these challenges. Finally, it surveys international human rights law, especially Article 17 of the ICCPR and the work of UN bodies, to argue for deeper harmonisation between India's domestic framework and global privacy norms. It contends that India must develop comprehensive legislative regimes, robust algorithmic accountability mechanisms, and independent supervisory institutions if privacy is to function as a structural guarantee of democracy in the digital age.

Keywords: Right to privacy, human right, digital age, constitutional law, comparative models

Introduction

Part I of this study examined the theoretical foundations of the right to privacy, its close relationship with human dignity, and the evolution of Indian constitutional doctrine from early formalist decisions to the landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India. It showed how Puttaswamy recognised privacy as a fundamental right flowing from Articles 14, 19, and 21 and adopted proportionality as the core standard for assessing state interference in privacy, before applying this framework to concrete controversies such as Aadhaar and Pegasus.

Part II moves from doctrinal consolidation to comparative and forward-looking analysis. First, it surveys constitutional and statutory models of privacy and data protection in the European Union, Canada, Australia, the United Kingdom, and South Africa, highlighting common principles, institutional safeguards, and different ways of embedding proportionality into law. Secondly, it addresses the specific challenges posed by artificial intelligence and algorithmic governance, including how profiling, bias, opacity, and automated decision-making generate new forms of privacy and equality harm. Thirdly, it situates privacy within the framework of international human rights law and considers how India, already a party to core human rights treaties, can align its domestic legal order with emerging global standards and best practices. The concluding section draws these strands together to identify key reform priorities for Indian law.

Comparative Constitutional Models of Privacy

a. European Union: GDPR and Strong Regulation

The European Union adopts perhaps the most comprehensive and rights-oriented approach to privacy and data protection in contemporary constitutional practice. Articles 7 and 8 of the Charter of Fundamental Rights distinguish between respect for private and family life and the right to protection of personal data, thereby treating data protection as an autonomous fundamental right rather than a mere extension of privacy. This dual recognition reflects the understanding that modern threats arise not only from invasions of spatial or decisional privacy but from systemic data processing itself.

The General Data Protection Regulation operationalises these guarantees through a detailed, directly applicable legislative framework built around key principles such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability. Controllers and processors must identify a lawful basis for processing, such as consent, contractual necessity, legal obligation, vital interests, public task, or legitimate interests, and they bear the burden of demonstrating compliance. The GDPR grants individuals a suite of enforceable rights: access, rectification, erasure (the "right to be forgotten"), restriction of processing, data portability, and the right to object to both processing and certain forms of automated decision-making. National supervisory authorities are empowered to investigate infringements, order corrective measures, and impose substantial administrative fines, providing the regime with real teeth.

The Court of Justice of the European Union has reinforced this rights-centred model through jurisprudence such as Schrems II, where it invalidated the EU–US Privacy Shield mechanism for transatlantic data transfers. The Court held that third-country surveillance regimes must provide "essentially equivalent" protection to EU fundamental rights and that indiscriminate or bulk access to data by foreign intelligence agencies violates the principle of proportionality. In effect, the EU model links data protection not only to domestic constitutional law but also to international data flows, exporting its privacy standards globally.

b. Canada: Charter Rights and the Oakes Test

Canadian constitutional law integrates privacy primarily through Section 8 of the Canadian Charter of Rights and

Freedoms, which protects individuals against unreasonable search and seizure. Any limitation on Charter rights must be justified under Section 1, with courts applying the structured proportionality analysis developed in R. v. Oakes. Under the Oakes test, the state must demonstrate that the measure pursues a pressing and substantial objective, is rationally connected to that objective, impairs the right as little as reasonably possible, and maintains a proportionate balance between the beneficial and deleterious effects.

In privacy cases, Canadian courts have progressively recognised strong expectations of privacy in digital contexts. In R. v. Spencer, the Supreme Court held that police requests for subscriber information from internet service providers without prior judicial authorisation violated Section 8, recognising that anonymity and control over identifying information are integral to informational privacy. Similarly, in R. v. Marakah, the Court found a reasonable expectation of privacy in text messages stored on a recipient's device, acknowledging that digital communication cannot be treated as automatically "exposed" to third parties. These decisions illustrate technologically sensitive, evidence-based application of proportionality principles, and they highlight the central role of judicial warrants and independent review in safeguarding privacy.

c. Australia: Statutory and Proportionality Hybrid

Australia presents a hybrid model in which privacy is primarily protected through legislation rather than a constitutional bill of rights. The Privacy Act 1988 establishes Australian Privacy Principles that regulate the collection, use, disclosure, and security of personal information by government agencies and certain private sector entities. In parallel, the Telecommunications (Interception and Access) Act 1979 governs interception of communications and access to stored communications, including metadata retention schemes.

At the constitutional level, the High Court has increasingly used structured proportionality to review burdens on the implied freedom of political communication, particularly in cases like McCloy v. New South Wales. Although this implied freedom is not a general privacy right, the Court's adoption of suitability, necessity, and balancing tests indicates a broader judicial willingness to use proportionality as a tool for evaluating rights limitations. Oversight over surveillance and interception is largely administered through bureaucratic and ombudsman mechanisms, leading to ongoing debates about whether statutory safeguards are sufficient in the absence of explicit constitutional rights.

d. United Kingdom: Article 8 and Investigatory Powers

In the United Kingdom, privacy protection is grounded in Article 8 of the European Convention on Human Rights, which has been incorporated into domestic law through the Human Rights Act 1998. Article 8 guarantees the right to respect for private and family life, home, and correspondence, but allows interference where it is in accordance with law and "necessary in a democratic society" for specified aims. UK courts therefore apply a four-stage proportionality analysis: the importance of the objective, rational connection between measure and objective, availability of less intrusive means, and whether the measure strikes a fair balance between individual rights and community interests.

The Investigatory Powers Act 2016 consolidates and updates the legal framework for surveillance, including interception, equipment interference (hacking), and retention of communications data. While the Act expands certain powers, it simultaneously introduces institutional safeguards such as the "double-lock" mechanism, under which warrants must be approved by both a Secretary of State and an independent Judicial Commissioner. An Investigatory Powers Commissioner provides systemic oversight, and individuals may challenge unlawful surveillance before the Investigatory Powers Tribunal. This structure reflects an attempt to reconcile extensive security powers with meaningful legal and institutional checks.

e. South Africa: Explicit Constitutional Protection

South Africa offers one of the clearest examples of explicit constitutional protection for privacy. Section 14 of the Constitution guarantees the right to privacy, including freedom from searches, seizures, and interception of communications. Any limitation of this right must comply with Section 36, which sets out a structured limitations clause requiring that restrictions be reasonable and justifiable in an open and democratic society based on dignity, equality, and freedom. In practice, this operates similarly to proportionality analysis.

In AmaBhungane Centre for Investigative Journalism v. Minister of Justice, the Constitutional Court examined the Regulation of Interception of Communications Act (RICA) and held several provisions unconstitutional. The Court found that the absence of post-surveillance notification, inadequate protection for journalistic sources, and insufficient independent oversight rendered the statutory scheme inconsistent with the right to privacy. It mandated reforms, including judicial authorisation requirements and safeguards for privileged communications. South Africa thus illustrates how explicit constitutional rights, combined with a robust limitations clause, can empower courts to reshape surveillance law in favour of greater transparency and accountability.

f. Comparative Reflections

Despite significant institutional and textual differences, these jurisdictions exhibit convergence on several core principles. First, privacy and data protection are increasingly treated as fundamental rights rather than mere policy interests. Secondly, structured proportionality— whether articulated through the GDPR, the Oakes test, Section 36, or Article 8 ECHR—has become the dominant methodology for evaluating restrictions on privacy. Thirdly, independent oversight mechanisms, including data protection authorities, judicial commissioners, constitutional courts, and ombudsmen, are recognised as indispensable to regulating surveillance powers.

For India, these comparative experiences suggest that effective privacy protection requires more than a doctrinal declaration of rights. It demands clear and detailed legislative frameworks, specialised and independent regulators with real powers, and a consistent judicial practice of applying proportionality in a rigorous, evidence-based manner. Such measures would strengthen the structural role of privacy within India's constitutional democracy.

Artificial Intelligence, Algorithmic Governance and Future Privacy Risks

a. Algorithmic Profiling and Informational Power

Artificial intelligence systems depend on vast quantities of data—biometric identifiers, behavioural logs, geolocation histories, financial records, social media activity, and more—to generate probabilistic profiles of individuals and groups. Machine learning algorithms detect patterns and correlations that may not be apparent to human observers, enabling targeted predictions about behaviour, preferences, and risk. While this can increase efficiency in areas such as credit scoring or welfare targeting, it simultaneously amplifies informational power in the hands of both state and corporate actors.

Aggregation of disparate data points can reveal highly sensitive information about health, political beliefs, or religious affiliation, even if none of the data sets individually appears intrusive. Profiling technologies can be used for predictive surveillance, where individuals are subjected to heightened monitoring or intervention not because of proven wrongdoing but because an algorithm predicts that they belong to a "high-risk" category. These developments undermine informational self-determination, as individuals often lack both knowledge of how they are being profiled and effective means to resist or correct these inferences.

b. Bias, Discrimination and Equality

AI systems are only as fair as the data and design choices that underpin them. When training data reflects historical patterns of discrimination or structural inequality, algorithms may reproduce and even amplify these biases. For instance, in welfare allocation, predictive policing, creditworthiness assessments, or hiring tools, models may disproportionately classify already marginalised groups as high-risk or low-value, leading to systematic exclusion or greater scrutiny.

In such contexts, privacy and equality concerns intersect. Excessive data extraction from vulnerable communities, combined with opaque profiling, can entrench disadvantage and convert social prejudice into seemingly objective "risk scores." From a constitutional perspective, automated systems that affect access to state benefits or expose individuals to heightened surveillance must be scrutinised not only for privacy intrusions but also for discriminatory impact under equality guarantees.

c. Opacity and the Black Box Problem

A central challenge in AI governance is the opacity of complex machine learning systems, especially deep neural networks. These models may operate as "black boxes," producing outputs that even their designers struggle to fully explain. Individuals subject to adverse decisions, such as denial of welfare benefits, credit, employment, or immigration status, are often unable to ascertain what data was used, how variables were weighted, whether errors occurred, or how to challenge the outcome.

This opacity has both privacy and due process implications. It undermines informational self-determination by obscuring how personal data is transformed into decisions, and it threatens procedural fairness by denying affected persons meaningful opportunities to understand and contest state action. In constitutional terms, automated decision-making that significantly affects rights or entitlements cannot be reconciled with principles of natural justice if individuals are kept in ignorance of the basis of such decisions.

d. Automated Decision-Making and Human Oversight

The GDPR directly addresses the risks of fully automated decision-making in Article 22, which grants individuals the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects. It further requires appropriate safeguards, including the right to obtain human intervention, to express one's point of view, and to contest the decision. These provisions reflect the view that certain decisions, particularly those

affecting rights, obligations, or significant opportunities, should not be left entirely to opaque algorithmic systems.

Building on these principles, the proposed EU Artificial Intelligence Act adopts a risk-based regulatory model. High-risk AI systems (for example, those used in critical infrastructure, employment, law enforcement, and migration control) must comply with stringent requirements relating to risk assessment, quality of data sets, transparency, documentation, human oversight, and robustness. Certain practices, such as real-time remote biometric identification in public spaces, are subject to strict restrictions or near-bans due to their profound implications for privacy and civil liberties. The EU's approach thus situates AI regulation firmly within a fundamental rights framework.

e. Indian Legal Context and Algorithmic Accountability

India's digital governance architecture, spanning Aadhaar-linked welfare schemes, digital payment systems, and emerging smart city and policing projects, increasingly relies on automated or algorithmic processing. Yet the existing legal framework provides only fragmentary regulation of AI deployment and does not comprehensively address automated decision-making, explainability, or human oversight. The Digital Personal Data Protection Act focuses primarily on data processing obligations and individual rights but does not establish a full-fledged algorithmic accountability regime.

In light of Puttaswamy's recognition of informational privacy as part of Article 21, algorithmic governance must satisfy constitutional requirements of legality, legitimate aim, necessity, and proportionality, including data minimisation, transparency, independent supervision, and meaningful human review in high-stakes contexts. Without these safeguards, AI-driven systems risk normalising opaque surveillance and automated discrimination, thereby infringing both privacy and equality protections under Articles 14 and 21. Future Indian privacy jurisprudence will therefore need to expand its focus beyond traditional surveillance to encompass AI ethics and algorithmic accountability.

International Human Rights Law and Global Harmonisation

a. Article 17 ICCPR

Privacy protection is deeply embedded in international human rights law. Article 17 of the International Covenant on Civil and Political Rights provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence. The provision imposes both negative and positive obligations on States:

they must refrain from unlawful interference and must also adopt legislative and other measures to protect individuals from arbitrary interference, including by private actors.

In General Comment No. 16, the UN Human Rights Committee clarified that interferences with privacy must not only be authorised by law but must also be reasonable and necessary in the particular circumstances. Laws permitting surveillance must specify the precise circumstances in which such measures may be taken, the competent authorities, and the

safeguards available. The Committee has emphasised that "arbitrary" interference can include actions that are lawful under domestic law but incompatible with the Covenant's aims and proportionality requirements.

b. Surveillance and Proportionality in International Law

Recent communications, concluding observations, and thematic reports by UN bodies have developed a more detailed proportionality framework for surveillance. The Human Rights Committee has criticised mass, indiscriminate surveillance programmes that lack adequate safeguards and targeted justification, and has stressed that generic invocations of national security cannot justify unrestricted data collection. The UN Special Rapporteur on the right to privacy has expressed particular concern about the proliferation of sophisticated spyware, such as Pegasus, and "bulk" interception capabilities that enable pervasive monitoring of individuals across borders.

These bodies have consistently called for stringent safeguards: prior judicial authorisation based on probable cause or similar standards, genuinely independent supervisory authorities, transparency reporting by states and companies, effective remedies for victims of unlawful surveillance, and clear rules governing the export and use of surveillance technologies. A central theme is that technological advances do not reduce state obligations under human rights law; rather, they heighten the need for robust legal controls.

c. Cross-Border Data Governance

In a globalised digital environment, personal data frequently flows across national borders, creating complex issues of jurisdiction, adequacy, and extraterritorial responsibility. International human rights law increasingly informs debates about cross-border data transfers and the standards that receiving countries must meet to protect privacy. The CJEU's Schrems II decision exemplifies this trend: it held that EU data could be transferred to third countries only if those countries ensure protection essentially equivalent to EU standards, including effective remedies and limitations on state access for surveillance purposes.

Although Schrems II is not binding on India, it exerts normative influence by setting a high benchmark for adequacy assessments. As India seeks to participate in global digital trade and data-driven services, the robustness of its privacy and surveillance safeguards will increasingly affect its ability to enter into data transfer arrangements with other jurisdictions. Moreover, as a State Party to the ICCPR, India must ensure that its domestic interception and data retention laws conform to Article 17's requirements of legality, necessity, and proportionality.

d. Harmonisation and Constitutional Convergence

Global practice reveals a gradual convergence around certain core elements of privacy protection: recognition of privacy as a fundamental right, use of structured proportionality review, establishment of independent oversight and accountability mechanisms, and insistence on transparency and remedies in surveillance regimes. Harmonisation does not require countries to adopt identical statutory schemes, but it does demand adherence to these basic human rights principles.

For India, aligning domestic law with international standards would serve multiple functions. It would reinforce the legitimacy of its constitutional jurisprudence, enhance trust in its digital regulatory environment, and facilitate cross-border data cooperation with key economic partners. It would also signal a substantive commitment to the rule of law and to protecting individuals against the abuse of technological power by both state and private actors.

Conclusion

The comparative and international analysis in this second part shows that privacy and data protection have moved to the centre of constitutional democracies worldwide. Jurisdictions such as the European Union, South Africa, and Canada illustrate how strong regulatory frameworks, explicit constitutional guarantees, and rigorous proportionality review can be used to craft rights-sensitive responses to digital surveillance and data processing.

At the same time, rapid advances in artificial intelligence and algorithmic governance introduce novel and complex privacy risks that traditional legal tools did not anticipate. Profiling, predictive analytics, opaque decision-making, and automated systems can generate structural harms that intersect privacy, dignity, and equality. For India, building on Puttaswamy, the central challenge is to translate constitutional commitments into detailed legislative regimes, effective independent oversight, and robust algorithmic accountability mechanisms. Sustaining privacy as a structural guarantee of democracy in the digital age will require continuous doctrinal vigilance, institutional reform, and active engagement with evolving international human rights standards.

References

1. Regulation (EU) 2016/679 (GDPR).
2. Regulation (EU) 2024/1689 (AI Act).
3. Data Protection Comm'r v. Facebook Ireland (Schrems II), Case C-311/18 (CJEU, 2020).
4. Google Spain SL v. AEPD, Case C-131/12 (CJEU, 2014).
5. R. v. Oakes, 1 S.C.R. 103 (Can.).
6. R. v. Spencer, 2014 SCC 43 (Can.).
7. R. v. Marakah, 2017 SCC 59 (Can.).
8. McCloy v. New South Wales, HCA 34 (Austl.).
9. Investigatory Powers Act 2016 (UK).
10. AmaBhungane v. Minister of Justice, ZACC 15 (S. Afr.).
11. International Covenant on Civil and Political Rights, Art. 17.
12. U.N. Human Rights Comm., General Comment No. 16 (1988).
13. U.N. Special Rapporteur on Privacy, Surveillance and Human Rights, U.N. Doc. A/HRC/46/37 (2021).
14. Digital Personal Data Protection Act, No. of 2023 (India).