Page 2889 - 2895

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

A Comparative Analysis of Global Data Protection Regimes and the Quest for Digital Sovereignty

ANKITA JAIN*

ABSTRACT

This paper undertakes a comparative analysis of three legal responses to the challenge of protecting personal data and privacy against state surveillance: the European Union's General Data Protection Regulation, India's Digital Personal Data Protection Act, 2023, and the international standard set by Article 17 of the International Covenant on Civil and Political Rights together with its associated jurisprudence. It argues that each regime contains a structural tension between rules that discipline data collectors and broad exemptions that permit governments to circumvent those rules, illustrated by Article 23 of the GDPR, Section 17 of the DPDPA, and the national-security qualifications recognised under international human rights law. Drawing on the constitutional foundation laid by Justice K.S. Puttaswamy (Retd.) v. Union of India *and the surveillance safeguards articulated in* Big Brother Watch and Others v. the United Kingdom *and* Szabo and Vissy v. Hungary*, the paper contends that the decisive variable is not the text of privacy guarantees but the independence and enforcement capacity of the institutions charged with upholding them. It further examines how the rise of digital sovereignty after 2013 has reshaped cross-border data governance, frequently strengthening domestic surveillance under the guise of protection from foreign interference, and concludes that the principal unfinished task in data protection is the construction of strong, independent oversight institutions.*

Keywords: *Data protection, Privacy, Digital sovereignty, Government surveillance, GDPR, Digital Personal Data Protection Act, ICCPR, Comparative law.*

I. INTRODUCTION

The definition of privacy offered by Samuel D. Warren and Louis D. Brandeis, namely the right to be let alone, was apt for its time, but in the present era of digital transformation it is of limited utility. It does capture the basic intuition, particularly when the state begins to intrude into people's lives. Today, however, the gravest concerns no longer arise from intrusive journalists

* Author is a Research Scholar at Mangalayatan University, Jabalpur, Madhya Pradesh, India.

 [ISSN 2581-5369]

or eavesdropping neighbours. They arise instead from intelligence agencies sifting through metadata, from companies being compelled to surrender decrypted messages, and from the retention of entire populations' records, all in the name of public safety. The underlying problem remains constant: individuals lack control over their own data. In earlier times, solitude and isolation were sufficient to secure privacy; in the present age of modernity, even an isolated person may have his privacy infringed through applications and surveillance devices.

This paper demonstrates how three distinct legal systems attempt to address this problem: the European Union's General Data Protection Regulation (GDPR), India's Digital Personal Data Protection Act, 2023 (DPDPA),[1] and the international standard set by Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and its associated case law.[2] Each adopts a distinctive approach to the problem.

The central questions that arise are these: how do individuals exercise their privacy-related rights, to what extent may the government access citizens' data, and what rules and safeguards has the state established to govern digital surveillance? A further question concerns what digital sovereignty means for the way states approach data control and cybersecurity. To answer these questions, this paper examines the relevant statutes, judicial decisions, policy documents, and scholarly writing on privacy, data protection, and internet governance.

II. PRIVACY AND DATA PROTECTION: THE BASICS

When Alan Westin defined informational privacy as a person's right to determine when, how, and to what extent information about them is communicated to others, he was describing a world that hardly exists any longer. At that time, individuals generally chose what to share. Now, the mere conduct of daily life leaves a continuous data trail, encompassing search terms, shopping habits, and location, all of it tracked and recorded, frequently without the individual's knowledge or control. Daniel Solove's framework is more accurate to present conditions, since it disaggregates privacy into distinct harms, such as surveillance, aggregation, insecurity, and interference with decisions, each of which calls for a different legal response.

Out of these new harms grew the need for data protection law. Unlike older privacy law, which waits until harm occurs and then reacts, data protection law seeks to establish the governing rules in advance: who may collect data, for what purpose, for how long it may be retained, and what obligations processors owe to the persons whose data they hold. At its core, it rests on the conviction that retaining control over personal information is not merely desirable but essential

[1] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).
[2] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

 [ISSN 2581-5369]

to human dignity. That conviction carries significant legal consequences: the state's assertion that it acts in the interest of security does not automatically prevail. It must justify any invasion of privacy and ensure that such invasion is subject to independent oversight.

III. The European Union's General Data Protection Regulation

A. Rights, principles, and accountability

The GDPR came into force in 2018 and within a short time became the most stringent data protection instrument, characterised by strict rules and rigorous regulation. The Regulation is built upon core principles such as transparency, lawfulness, and data minimisation. These are not aspirations but binding legal requirements, and supervisory authorities across Europe possess genuine enforcement powers. Data subjects enjoy an array of rights, ranging from access to information about what is collected and rectification of inaccuracies, to erasure, restriction of processing, and the right to obtain a copy of their data and to port it elsewhere. Organisations that disregard these duties face substantial fines, of up to twenty million euros or four per cent of their global annual turnover, whichever is higher.

The reach of the GDPR is not confined to European borders. In Schrems II, the Court of Justice of the European Union invalidated the Privacy Shield arrangement with the United States, reasoning that United States surveillance law afforded the government broad access and that Europe could not entrust data to a country that failed to constrain its own intelligence gathering.

B. National security exemptions

Article 23 of the GDPR permits member states to restrict data subjects' privacy rights where this is required for national security, defence, or public order. These powers are broad. Intelligence services may obtain exemptions from disclosing the legal basis for their processing, from responding to subject access requests, and even from maintaining records. In practice, the GDPR thus operates with two distinct characters: strict towards private companies, yet considerably more lenient where the state is the entity collecting data. This is not an accident but a feature embedded in the European Union's legal framework, which must always accommodate the prerogatives of its member states, particularly in matters of security.[3]

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 23.

 [ISSN 2581-5369]

IV. India's Digital Personal Data Protection Act, 2023

A. Constitutional setting and core structure

India's DPDPA rests upon a distinctive constitutional foundation. In 2017, the Supreme Court of India declared privacy[4] a fundamental right under Article 21, emphasising the importance of informational privacy, that is, the right to control the dissemination of one's personal details. The DPDPA seeks to give effect to that guarantee. It places considerable emphasis on consent: personal data may be processed only with clear, informed agreement, or where the law requires processing for specified purposes. Organisations must keep data secure, respect the rights of data principals, and notify both the Data Protection Board and affected individuals in the event of a data breach.[5]

The DPDPA fills a significant gap. Before its enactment, India lacked a comprehensive data protection statute and relied instead upon a few piecemeal rules. There is now an actual statutory system in place, complete with its own enforcement body.

B. Section 17: exemptions and structural vulnerabilities

It is here that the difficulties emerge. Section 17 of the DPDPA confers on the government sweeping powers to exempt itself, or any instrumentality of the state, from compliance with the Act on grounds as broad as the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order, and the prevention of incitement to cognisable offences. The language is drawn from the Constitution, but in practice it functions as an open door. There are few meaningful checks on when or how the government invokes these powers; in effect, the executive may simply decide not to follow the privacy law.

That is not the only difficulty. The Data Protection Board, which is meant to scrutinise these exemptions, is composed of government appointees and enjoys little genuine independence. Taken together, these features mean that, while India's law protects individuals adequately against private companies, it offers far weaker protection against the state. The right to privacy, declared fundamental by the courts, does not necessarily receive full statutory support where the government itself is the actor.

[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[5] Vrinda Bhandari & Vasudev Bansal, *India's Digital Personal Data Protection Act, 2023: An Analysis*, 19 INDIAN J.L. & TECH. 1 (2023).

 [ISSN 2581-5369]

V. LAWFUL INTERCEPTION AND THE INTERNATIONAL HUMAN RIGHTS FRAMEWORK

Article 17 of the ICCPR prohibits unlawful or arbitrary interference with privacy,[6] home, and correspondence. States are obliged to establish genuine means of protecting individuals against such interference. The United Nations Human Rights Committee has stated that any governmental surveillance must be authorised by law, must serve the aims of the Covenant, and must be reasonable in the particular circumstances. Reasonable, in this context, means proportionate, genuinely necessary, and, importantly, conducted under laws that are clear and accessible. Secret surveillance founded upon undisclosed rules does not satisfy this standard.

The European Court of Human Rights has built comparable standards into Article 8.[7] In *Big Brother Watch and Others v. the United Kingdom*, the Court held that any bulk interception programme must specify who may be targeted, how long data is retained, how it is accessed, and when it is destroyed. In *Szabo and Vissy v. Hungary*,[8] the Court went further, indicating that surveillance should generally require judicial authorisation before it is undertaken, with ex post facto review serving as a supplementary rather than a primary safeguard. What matters most is not the mere existence of legislation but the presence of robust, independent oversight.

India, by contrast, continues to operate under rules inherited from the pre-digital era. Its principal instrument remains the antiquated Indian Telegraph Act, 1885,[9] supplemented by interception rules made in 2009.[10] The Supreme Court has held that interception orders must be in writing and reasoned, but it has stopped short of requiring prior judicial approval. Review is instead conducted by officials within the executive. Measured against the more exacting standards of the ICCPR and the European Court of Human Rights, India's system falls short.

VI. DIGITAL SOVEREIGNTY CHANGES THE GAME

Following the Snowden disclosures of 2013, digital sovereignty has emerged as a foundational principle. States have become increasingly attentive to the rules governing cross-border data flows and have begun to invest in domestic digital infrastructure. On its face this is sensible;

[6] U.N. Human Rights Comm., General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (Apr. 8, 1988).
[7] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.
[8] *Szabo and Vissy v. Hungary*, App. No. 37138/14, Eur. Ct. H.R. (Jan. 12, 2016).
[9] The Indian Telegraph Act, 1885, No. 13 of 1885, Acts of Parliament, 1885 (India).
[10] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Gazette of India, pt. II sec. 3(i) (India).

 [ISSN 2581-5369]

there is little reason to permit a foreign government to access national data. Yet policies devised in the name of sovereignty frequently prove to be double-edged.

As Julia Pohle and Thorsten Thiel observe,[11] liberal democracies pursue digital sovereignty in order to shield their citizens from both foreign and domestic surveillance, yet many governments invoke it merely as a pretext to expand their own control. Most states now favour this path, imposing local data storage requirements, demanding decryption capabilities, and compelling technology companies to grant law enforcement access. While such measures guard against foreign encroachment, they simultaneously enhance the surveillance capacity of the domestic government. This is rarely acknowledged in official pronouncements, yet the pattern is clear enough: the task of repelling external threats becomes a justification for stronger surveillance at home, and ordinary individuals are left with nowhere to shelter.

This trend troubles internet governance scholars as well. The more vigorously each state pursues an autonomous course, the more difficult it becomes to establish shared global privacy standards. Requirements such as the GDPR's rule that data may be transferred abroad only where the recipient country offers adequate protection are becoming harder to enforce, because each jurisdiction now adopts its own approach.[12] Individuals are not afforded sufficient privacy beyond state borders, and states are unable to constrain one another's privacy norms. Absolute digital sovereignty may present itself as a new gain in security, but ultimately it imperils both safety and freedom.

VII. WHERE THE LAWS MEET AND PART WAYS

A feature common to all three systems is the inherent tension between privacy rules designed to discipline data collectors and exceptions that permit governments to sidestep those rules. There are always carve-outs: Article 23 in the GDPR, Section 17 in the DPDPA,[13] and the national-security qualification under the ICCPR. Each operates differently. India's is the most permissive, the jurisprudence of the European Court of Human Rights is the most demanding, and the GDPR and ICCPR occupy an intermediate position.

The decisive distinction lies in their enforcement structures. The GDPR's independent regulators possess genuine authority to hold companies to account and to exert pressure on foreign governments through the adequacy mechanism.[14] The European Court of Human Rights

[11] Julia Pohle & Thorsten Thiel, *Digital Sovereignty*, 9(4) INTERNET POL'Y REV. 1 (2020).
[12] Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, 145 PRIVACY L. & BUS. INT'L REP. 10 (2018).
[13] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 17, Acts of Parliament, 2023 (India).
[14] Christopher Kuner, Lee A. Bygrave & Christopher Docksey eds., *The EU General Data Protection Regulation (GDPR): A Commentary* (2020).

 [ISSN 2581-5369]

has articulated surveillance safeguards, such as prior judicial approval and continuing oversight,[15] building upon Article 8. By contrast, India's enforcement framework is weak: its Board is not genuinely independent and cannot resist government exemptions. For this reason, strong laws matter in practice only where independent institutions stand behind them. Without real enforcement power, even the best-drafted laws are hollow. The GDPR demonstrates that effective enforcement is achievable, whereas the DPDPA shows that a constitutional promise is insufficient in itself.

VIII. CONCLUSION

The world's patchwork of data protection law has rarely appeared more divided, because at bottom states cannot agree on how much control the state should exercise over the individual. These disagreements are framed in terms of law and philosophy, but they are also driven by politics and by the ascent of digital sovereignty as a rallying cry. If this comparison establishes anything, it is that the principal contest is not over the particulars of consent or data use but over whether enforcement bodies are genuinely independent.

To assert that individuals possess a right to privacy means little in the absence of action. There must be genuinely independent oversight bodies, judicial approval for governmental surveillance, and effective remedies for abuse; otherwise privacy remains words on a page. These are not optional extras. The United Nations Human Rights Committee, the European Court of Human Rights, and the Court of Justice of the European Union all regard them as essential. Where these foundations are absent, as in India's present system, constitutional rights do not translate into everyday reality. The genuine unfinished business in data protection is not merely the enactment of better laws but the construction of strong, independent institutions to enforce them. That is the challenge that remains.

*****

[15] *Big Brother Watch and Others v. the United Kingdom*, App. Nos. 58170/13, 62322/14 & 24960/15, Eur. Ct. H.R. (May 25, 2021).

 [ISSN 2581-5369]