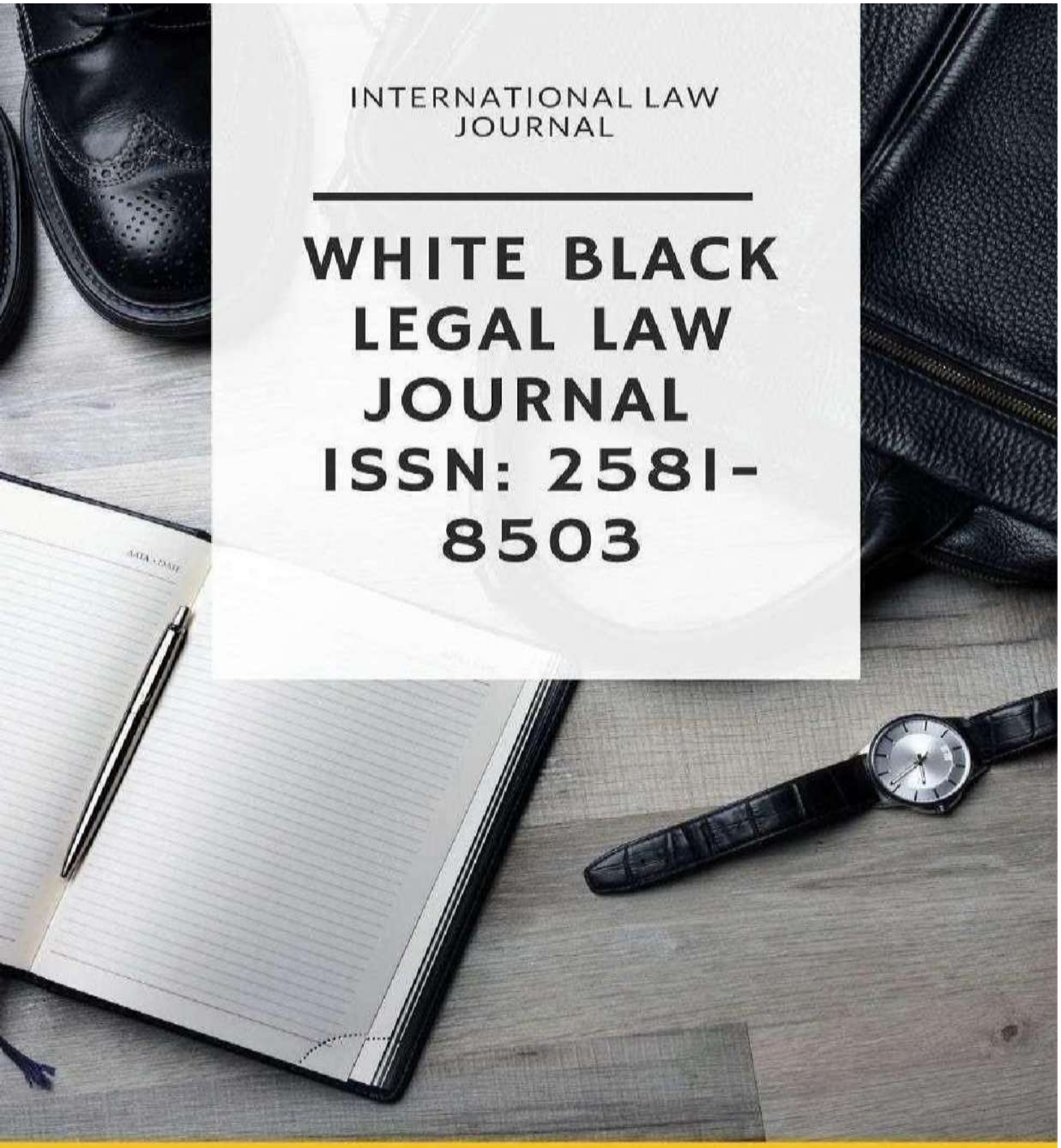

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 6 | April 2026 ISSN: 2581-8503

MASS SURVEILLANCE, FACIAL RECOGNITION, AND DATA GOVERNANCE IN INDIA: ASSESSING COMPLIANCE WITH ICCPR STANDARDS

AUTHORED BY - DISHA SHARMA

Abstract

The rapid expansion of digital governance in India has fundamentally altered the relationship between the State and the individual, particularly through the deployment of surveillance technologies, data-driven administrative systems, and platform regulation mechanisms. While these developments have enhanced administrative efficiency and national security capabilities, they have simultaneously generated significant concerns regarding their compatibility with constitutional guarantees and international human rights obligations. This paper examines India's compliance with the standards established under the International Covenant on Civil and Political Rights (ICCPR), particularly Articles 17, 19, 26, and 2(3), in the context of mass surveillance, facial recognition technologies, and contemporary data governance frameworks.

Adopting a doctrinal and comparative methodology, the study analyses statutory instruments such as the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and subordinate regulatory frameworks alongside judicial precedents and international human rights standards. It argues that while India has made partial progress in recognising privacy and digital rights—most notably through judicial interpretation—its regulatory architecture continues to fall short of ICCPR requirements relating to legality, necessity, proportionality, and effective remedy. The absence of a comprehensive surveillance law, broad executive discretion, algorithmic opacity, and weak institutional accountability mechanisms collectively undermine compliance.

The paper concludes that India's digital governance framework reflects an imbalance between technological expansion and rights-based safeguards. It proposes doctrinal, legislative, and institutional reforms, including the adoption of a comprehensive surveillance law, strengthening of data protection oversight, and the development of a cumulative proportionality framework, to align India's digital governance practices with its international human rights commitments.

1. Introduction

The digital transformation of governance has emerged as one of the most defining features of contemporary states, fundamentally reshaping the structure, reach, and modalities of public administration. India represents a particularly significant case in this regard, having developed one of the world's most expansive and integrated digital public infrastructures over the past two decades (Kshetri, 2019; Aronson, 2021). This transformation is reflected in the widespread deployment of biometric identification systems such as Aadhaar, real-time financial platforms like the Unified Payments Interface (UPI), data-driven welfare delivery mechanisms, and increasingly sophisticated surveillance technologies. Together, these developments signify not merely technological advancement but a structural reconfiguration of governance, where data becomes central to state functioning and decision-making.

At the same time, the expansion of digital governance has been accompanied by the growing use of algorithmic decision-making, platform regulation, and large-scale data extraction practices. Scholars have argued that such developments reflect a broader global shift toward "datafied governance," where the exercise of state power is increasingly mediated through digital infrastructures and predictive analytics (Lyon, 2018; Zuboff, 2019). In the Indian context, this shift has led to an unprecedented enhancement of the State's capacity to collect, process, and analyse personal data across multiple domains, including welfare distribution, law enforcement, and public administration (Aronson, 2021). While these capabilities have improved efficiency, inclusion, and service delivery, they have simultaneously raised complex constitutional and human rights concerns.

Technologies such as facial recognition systems, centralized monitoring networks, and mandatory data retention frameworks operate at a scale and intensity that fundamentally alter the balance between individual autonomy and state authority. Unlike traditional forms of governance, which were constrained by administrative and logistical limitations, digital systems enable continuous, real-time monitoring and profiling of individuals, often without their knowledge or meaningful consent (Solove, 2021). This expansion of surveillance capacity has led scholars to characterise modern governance as increasingly "surveillance-oriented," where the boundaries between security, administration, and control become blurred (Lyon, 2018). In such a framework, the absence of clear legal safeguards and institutional accountability mechanisms creates significant risks of arbitrary and disproportionate interference with fundamental rights.

India's obligations under international human rights law provide a critical normative framework for assessing these developments. Having ratified the International Covenant on Civil and Political Rights (ICCPR) in 1979, India is bound by a comprehensive set of obligations that include the protection of privacy under Article 17, freedom of expression under Article 19, equality before the law under Article 26, and the right to an effective remedy under Article 2(3) (United Nations, 1966; Joseph & Castan, 2013). Importantly, these obligations are not external impositions on India's constitutional order but commitments voluntarily undertaken by the State and reinforced through constitutional principles such as Article 51, which directs the State to foster respect for international law and treaty obligations (Baxi, 2007). Furthermore, Indian constitutional jurisprudence has consistently recognised the interpretive value of international human rights norms in expanding the scope of fundamental rights, particularly in areas where domestic law is evolving.

Against this backdrop, the central question that arises is whether India's contemporary digital governance framework is capable of meeting these international standards. This paper examines the extent to which surveillance practices, facial recognition technologies, and data governance laws in India align with the principles of legality, necessity, proportionality, and accountability embedded within the ICCPR framework. These principles constitute the core normative criteria against which any interference with fundamental rights must be assessed in international human rights law (Human Rights Committee, 1988; 2011).

The study adopts a doctrinal legal methodology, focusing on the analysis of statutory frameworks, judicial precedents, and international legal instruments, while also incorporating comparative insights from jurisdictions such as the United Kingdom and the European Union, where more developed regulatory approaches to digital governance have emerged (De Hert & Papakonstantinou, 2016). This combined approach allows for a nuanced evaluation of both the normative adequacy and institutional implementation of India's digital governance regime.

The central argument advanced in this paper is that, despite significant progress in recognising digital rights at the constitutional level—most notably through judicial decisions expanding the scope of privacy and dignity—India's legislative and institutional frameworks remain structurally inadequate in ensuring compliance with international human rights standards. The absence of a comprehensive surveillance law, the persistence of broad executive discretion, the lack of algorithmic accountability, and the weakness of remedial mechanisms collectively

produce a regulatory environment that falls short of ICCPR requirements. This gap between constitutional aspiration and regulatory reality is not merely incidental but reflects deeper structural tensions within India's evolving digital governance architecture.

2. Constitutional and International Law Framework

India's engagement with international human rights law is formally structured around a dualist constitutional approach, under which international treaties do not automatically acquire the force of domestic law unless they are expressly incorporated through legislative enactment (Seervai, 1996; Aust, 2013). This doctrinal position was authoritatively articulated in Gramophone Company of India Ltd. v. Birendra Bahadur Pandey, where the Supreme Court held that treaty obligations, even when binding at the international level, require legislative transformation before they can be directly enforced within the domestic legal system. This reflects a classical understanding of sovereignty, where the legislature retains primacy in determining the internal applicability of international norms.

However, this formal dualism is neither absolute nor exhaustive of India's constitutional practice. It is significantly qualified by a robust and evolving interpretive tradition through which international law informs the content and scope of fundamental rights. In Vishaka v. State of Rajasthan, the Supreme Court departed from strict dualism by holding that international conventions and norms, particularly those consistent with constitutional guarantees, may be relied upon in the absence of domestic legislation. This decision marked a decisive shift toward what scholars describe as an **"interpretive incorporation"** model, where international human rights standards function as persuasive and, at times, normative guides in constitutional adjudication (Baxi, 2007).

This approach was further consolidated in Justice K.S. Puttaswamy v. Union of India, where the Court drew extensively upon international human rights jurisprudence, including provisions of the ICCPR and comparative constitutional law, to recognise the right to privacy as intrinsic to life and personal liberty under Article 21 (Chandrachud, 2017). The judgment underscored that fundamental rights must be interpreted in a manner consistent with global human rights standards, particularly in areas where technological developments generate new forms of state power and potential rights infringements.

This interpretive praxis represents a critical bridge between international obligations and domestic constitutional law. Rather than treating international law as external or supplementary, the Indian judiciary has embedded it within the interpretive process, especially in contexts where constitutional rights are dynamic and evolving (Baxi, 2007; Joseph & Castan, 2013). Such an approach not only enhances the normative depth of constitutional rights but also aligns domestic jurisprudence with India's international commitments.

The constitutional foundation for this interpretive engagement is further strengthened by Article 51 of the Constitution, which directs the State to foster respect for international law and treaty obligations. Although placed within the Directive Principles and therefore non-justiciable, Article 51 reflects a constitutional orientation toward internationalism and provides normative legitimacy to the judiciary's reliance on international human rights instruments (Austin, 1999). In practice, this has enabled courts to treat international norms not merely as optional references but as integral components of constitutional reasoning, particularly in rights-expanding contexts.

The significance of this framework becomes especially pronounced in the domain of digital governance. Emerging technologies such as mass surveillance systems, biometric identification infrastructures, and algorithmic decision-making mechanisms create forms of state power that extend beyond the anticipatory scope of traditional constitutional provisions. In such circumstances, international human rights standards—particularly those articulated under the ICCPR—offer a structured and principled benchmark for evaluating the adequacy of domestic legal frameworks (De Hert & Papakonstantinou, 2016). The ICCPR's emphasis on legality, necessity, proportionality, and accountability provides a coherent normative framework for assessing state actions in areas such as surveillance, data processing, and regulation of digital expression.

The interpretive use of international law thus transforms the ICCPR from a merely aspirational instrument into a substantive constitutional resource. It enables courts to bridge normative gaps in domestic law and to respond to the challenges posed by rapidly evolving technological landscapes. However, this interpretive commitment remains uneven in its application. While landmark judgments have demonstrated a willingness to engage with international norms, there is a discernible lack of consistent application in regulatory and legislative contexts, particularly in areas such as surveillance governance and data protection.

This inconsistency raises a critical concern: the risk that international human rights norms may remain confined to judicial rhetoric rather than being systematically integrated into the design and operation of digital governance frameworks. For India to fully realise its constitutional and international commitments, it is necessary to move beyond episodic reliance on international law toward a more coherent and institutionalised incorporation of ICCPR standards into legislative and regulatory practices.

3. ICCPR Standards on Digital Rights

The ICCPR establishes a comprehensive framework for the protection of civil and political rights, which has been progressively interpreted to apply to digital environments (United Nations, 1966; Joseph & Castan, 2013). Four provisions are particularly relevant in assessing digital governance: Article 17 (privacy), Article 19 (freedom of expression), Article 26 (equality), and Article 2(3) (effective remedy).

Article 17 prohibits arbitrary or unlawful interference with privacy, family, home, or correspondence. The Human Rights Committee, through General Comment No. 16, has clarified that any interference with privacy must satisfy three key requirements: legality, necessity, and proportionality (Human Rights Committee, 1988). The requirement of legality demands that surveillance and data collection be authorised by clear, accessible, and foreseeable law (Kuner, 2017). Necessity requires that such measures pursue a legitimate aim and be strictly required to achieve that aim, particularly in contexts such as national security or public order (Privacy International, 2019). Proportionality mandates that the least intrusive means be employed and that safeguards be in place to prevent abuse (De Hert & Papakonstantinou, 2016).

Article 19 protects freedom of expression, including the right to seek, receive, and impart information. Restrictions on this right must meet a strict three-part test: they must be provided by law, pursue a legitimate aim, and be necessary and proportionate (Human Rights Committee, 2011). The Human Rights Committee has emphasised that vague or overly broad regulations can create a chilling effect, discouraging lawful expression and undermining democratic participation (Balkin, 2018; Human Rights Committee, 2011).

Article 26 guarantees equality before the law and protection against discrimination. In the context of digital governance, this provision is particularly relevant in addressing algorithmic

bias and discriminatory outcomes arising from automated decision-making systems (Barocas & Selbst, 2016). The increasing use of artificial intelligence in governance raises the risk of reproducing existing social inequalities in new technological forms, particularly when systems rely on historically biased datasets (Eubanks, 2018).

Article 2(3) establishes the right to an effective remedy for violations of rights. This requires not only the existence of legal rights but also accessible, independent, and effective mechanisms for their enforcement (Joseph & Castan, 2013). In the digital context, this includes remedies for data breaches, unlawful surveillance, and violations of informational privacy, which must be supported by institutional mechanisms capable of providing timely and meaningful redress (Kuner, 2017).

These provisions collectively create a normative framework that places strict limits on state power in the digital sphere. They require that digital governance systems be designed and implemented in a manner that respects individual autonomy, ensures accountability, and prevents arbitrary or discriminatory interference with rights (Solove, 2021; De Hert & Papakonstantinou, 2016).

4. India's Digital Governance Architecture

India's digital governance framework has evolved through a layered and incremental process, combining statutory enactments, executive rule-making, and large-scale technological infrastructures. Rather than emerging from a single comprehensive legislative vision, this architecture reflects a gradual expansion of regulatory mechanisms in response to technological change and administrative demands (Aronson, 2021; Kshetri, 2019). As a result, it is best understood not as a unified system but as a multi-nodal governance structure, where different legal instruments and institutions operate simultaneously, often with overlapping mandates and varying degrees of accountability.

At the statutory level, the Information Technology Act, 2000 constitutes the foundational legal framework for digital governance in India. Initially enacted to provide legal recognition to electronic transactions and facilitate e-commerce, the Act has, over time, expanded in scope to regulate a wide range of digital activities, including surveillance, intermediary liability, and cybersecurity (Singh, 2019). Amendments to the Act, particularly in 2008, introduced provisions such as Section 69, which authorises the interception, monitoring, and decryption

of digital communications on grounds including national security and public order. While these provisions were designed to address emerging security concerns, scholars have argued that their broad phrasing and reliance on executive authorisation raise significant concerns regarding proportionality and oversight (Kuner, 2017; Privacy International, 2019).

The regulatory framework governing intermediaries has similarly undergone substantial expansion. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose extensive due diligence obligations on digital platforms, including requirements related to content takedown, grievance redressal, and traceability of communications. While these measures aim to enhance accountability and address online harms, they have also been criticised for potentially incentivising over-censorship and creating chilling effects on freedom of expression (Balkin, 2018; Singh, 2021). The increasing regulatory burden placed on intermediaries reflects a broader shift toward platform governance, where private actors are effectively enlisted as agents of state regulation.

A significant recent development in India's digital governance architecture is the enactment of the Digital Personal Data Protection Act, 2023. The Act introduces a consent-based framework for the processing of personal data, recognising individuals as "data principals" and imposing obligations on "data fiduciaries" to ensure lawful and secure data processing (Greenleaf, 2023). It also establishes the Data Protection Board of India as an enforcement authority with the power to investigate breaches and impose penalties. However, despite these advances, the Act has attracted considerable scholarly critique, particularly in relation to its broad exemptions for state agencies under Section 17, which allow the government to bypass key data protection obligations on grounds such as national security and public order (Greenleaf, 2023; De Hert & Papakonstantinou, 2016). These exemptions raise fundamental questions about whether the framework adequately protects individuals against state surveillance and data misuse.

Beyond statutory regulation, India's digital governance framework is increasingly defined by the deployment of large-scale technological systems that enable extensive data collection and monitoring. The Central Monitoring System (CMS) facilitates real-time interception of communications across telecommunications networks, while Network Traffic Analysis (NETRA) enables the monitoring of internet traffic through keyword-based filtering and pattern recognition (Privacy International, 2019). The National Automated Facial Recognition System (NAFRS) represents a further expansion of surveillance capabilities, enabling

biometric identification across public spaces through integration with law enforcement databases. These systems collectively signify a transition from targeted surveillance to data-intensive, continuous monitoring architectures, where the scope of state observation extends across the digital and physical domains (Lyon, 2018).

These technological infrastructures operate alongside platform regulation mechanisms under the Information Technology Rules, 2021, which impose obligations on intermediaries to monitor and regulate online content. This convergence of surveillance technologies and platform governance creates a complex regulatory ecosystem in which state authority is exercised both directly, through surveillance systems, and indirectly, through obligations imposed on private entities (Balkin, 2018). The resulting model has been described as a form of "hybrid governance," where public and private actors jointly participate in the regulation of digital spaces.

While this architecture reflects a comprehensive and rapidly evolving approach to digital governance, it is characterised by significant structural limitations. One of the most prominent concerns is fragmentation, with multiple regulatory bodies—including the Ministry of Electronics and Information Technology (MeitY), CERT-In, sectoral regulators, and the Data Protection Board—operating within overlapping jurisdictions without a clear coordination mechanism (Aronson, 2021). This institutional fragmentation creates ambiguity regarding accountability and complicates the enforcement of rights.

Equally significant is the system's reliance on executive discretion. Many key regulatory powers, particularly in the areas of surveillance and data processing, are exercised through executive orders and delegated legislation rather than primary statutes. This raises concerns about the adequacy of procedural safeguards and the potential for arbitrary use of power, particularly in the absence of independent oversight mechanisms (Kuner, 2017; Privacy International, 2019).

The absence of a unified legislative framework governing surveillance and data processing further exacerbates these challenges. Unlike jurisdictions that have enacted comprehensive data protection and surveillance laws with clearly defined safeguards, India's framework remains dispersed across multiple statutes and rules, resulting in gaps and inconsistencies in regulation (De Hert & Papakonstantinou, 2016). These structural deficiencies raise important

questions about the framework's ability to meet constitutional standards and comply with international human rights obligations, particularly in relation to legality, proportionality, and accountability.

5. Compliance Analysis: India and ICCPR Standards

The evaluation of India's digital governance framework against ICCPR standards reveals a pattern of partial compliance accompanied by significant gaps. These gaps are most evident in relation to the principles of legality, proportionality, and accountability.

The practice of mass surveillance in India illustrates a fundamental tension between state objectives and individual rights. Surveillance systems such as the Central Monitoring System and NETRA operate without a comprehensive statutory framework that clearly defines their scope, limits, and oversight mechanisms. This absence of specific legislation undermines the requirement of legality under Article 17 of the ICCPR, as individuals cannot reasonably foresee the circumstances under which their data may be collected or monitored. Moreover, the reliance on executive authorisation, rather than independent judicial oversight, raises concerns about arbitrariness and lack of accountability.

Facial recognition technologies present an additional layer of complexity. The deployment of systems such as the National Automated Facial Recognition System occurs in the absence of a dedicated legal framework governing their use. These technologies inherently involve the processing of biometric data on a large scale, often without individualised suspicion. Comparative jurisprudence, such as R (Bridges) v Chief Constable of South Wales Police, has emphasised the need for clear legal standards, impact assessments, and safeguards against bias. In the Indian context, the absence of such safeguards raises concerns under both Article 17 and Article 26 of the ICCPR, particularly in relation to the risk of discriminatory outcomes.

The Digital Personal Data Protection Act, 2023 represents a significant step towards establishing a data protection framework, but it falls short in several respects. The broad exemptions granted to the State under Section 17 allow for the exclusion of government agencies from key provisions of the Act, potentially undermining the very purpose of data protection. Additionally, questions regarding the independence of the Data Protection Board and the absence of robust remedies for individuals limit the effectiveness of the framework.

Platform regulation under the Information Technology Rules, 2021 further highlights the tension between regulation and freedom of expression. Requirements such as traceability and proactive content monitoring impose significant obligations on intermediaries, which may lead to over-censorship and chilling effects. The Supreme Court's decision in Shreya Singhal v. Union of India underscores the importance of protecting free expression from vague and overbroad restrictions, a principle that is equally relevant under Article 19 of the ICCPR.

Finally, the absence of effective remedies remains a critical gap. While legal frameworks exist in principle, their practical accessibility and effectiveness are limited. Individuals affected by data breaches, surveillance, or algorithmic decisions often lack clear avenues for redress, undermining the guarantees of Article 2(3) of the ICCPR.

6. Comparative and Normative Insights

Comparative analysis provides valuable insights into how different jurisdictions have responded to the challenges posed by digital governance, particularly in reconciling state interests with the protection of fundamental rights. In the United Kingdom, the enactment of the Human Rights Act, 1998 represents a significant institutional development, as it incorporates key provisions of the European Convention on Human Rights (ECHR) into domestic law. This framework requires all public authorities to act in a manner compatible with rights such as privacy and freedom of expression, thereby embedding international human rights standards directly into administrative decision-making (Fenwick & Phillipson, 2017). In practice, this has enabled courts to subject surveillance practices and data processing activities to rigorous proportionality review, ensuring that state action is both justified and legally constrained.

The United Kingdom has also developed a more structured approach to surveillance oversight through legislation such as the Investigatory Powers Act, 2016, which introduces mechanisms including judicial authorisation and independent oversight bodies. These safeguards reflect an institutional recognition that surveillance powers, if left unchecked, may lead to disproportionate interference with privacy rights (Murray, 2018). Judicial decisions such as R (Bridges) v Chief Constable of South Wales Police further demonstrate the willingness of courts to scrutinise emerging technologies, particularly where issues of legality, proportionality, and algorithmic bias are implicated.

At the supranational level, the European Union has adopted a comprehensive regulatory framework through instruments such as the General Data Protection Regulation (GDPR). The GDPR establishes detailed obligations relating to consent, purpose limitation, data minimisation, and accountability, and is widely regarded as one of the most robust data protection regimes globally (De Hert & Papakonstantinou, 2016; Kuner, 2017). Importantly, it also introduces enforceable rights for individuals, including the right to access, rectification, erasure, and protection against automated decision-making, thereby operationalising the concept of informational self-determination (Wachter, Mittelstadt, & Floridi, 2017). The existence of independent supervisory authorities further ensures that these rights are not merely declaratory but are supported by effective enforcement mechanisms.

These comparative frameworks highlight three critical elements necessary for aligning digital governance with human rights standards: first, the presence of clear and specific legislation that defines the scope and limits of state power; second, the establishment of independent oversight institutions capable of enforcing compliance; and third, the availability of effective remedies for individuals whose rights have been violated (De Hert & Papakonstantinou, 2016; Kuner, 2017). Together, these elements demonstrate how institutional design plays a crucial role in translating abstract normative principles into practical safeguards.

In contrast, India's approach to digital governance remains characterised by fragmentation and a heavy reliance on executive discretion. While constitutional jurisprudence—particularly in the recognition of privacy as a fundamental right—provides a strong normative foundation, the absence of corresponding legislative clarity and institutional independence limits its practical effectiveness (Baxi, 2007; Aronson, 2021). Regulatory authority is dispersed across multiple bodies without a coherent coordination framework, and key areas such as surveillance continue to be governed primarily through executive rules rather than comprehensive legislation.

This divergence between normative commitment and institutional design creates what may be described as a "compliance gap," where constitutional and international standards are acknowledged in principle but insufficiently realised in practice. Unlike jurisdictions such as the United Kingdom and the European Union, where legal frameworks are structured to ensure ex ante safeguards and ex post accountability, India's system often relies on post-hoc judicial intervention, which is inherently limited in addressing systemic issues (Murray, 2018). As a result, the gap between principle and practice emerges as a central challenge for India's digital

governance framework, raising fundamental questions about its ability to meet both constitutional and international human rights obligations.

7. Findings

The analysis conducted in this study reveals that India's digital governance framework demonstrates partial and uneven alignment with the standards established under the International Covenant on Civil and Political Rights (ICCPR). While constitutional jurisprudence—particularly the recognition of privacy as a fundamental right—reflects a progressive interpretive approach, the broader regulatory and institutional landscape remains insufficiently developed to ensure full compliance with international human rights norms (Human Rights Committee, 1988; Joseph & Castan, 2013).

A primary finding of this study is the absence of a comprehensive and specific legislative framework governing surveillance activities. Existing surveillance powers are dispersed across multiple statutes and executive instruments, lacking the clarity and foreseeability required under the principle of legality. This creates a structural gap in compliance with Article 17 of the ICCPR, as individuals are unable to anticipate the scope and conditions under which their personal data may be accessed or monitored (Kuner, 2017; Privacy International, 2019).

The study further finds that India's digital governance architecture is characterised by a high degree of executive discretion and limited independent oversight. Surveillance authorisation processes are predominantly administrative rather than judicial, raising concerns regarding arbitrariness and lack of accountability. This institutional design weakens the safeguards necessary to ensure proportionality and necessity in state action (De Hert & Papakonstantinou, 2016).

Another significant finding relates to the regulatory limitations of the Digital Personal Data Protection Act, 2023, particularly the broad exemptions granted to state agencies. These exemptions undermine the universality of data protection principles by placing the State outside the scope of regulatory scrutiny in key areas, thereby weakening accountability mechanisms and raising concerns regarding compliance with privacy standards (Greenleaf, 2023).

The analysis also highlights the risk of discriminatory outcomes arising from algorithmic and data-driven governance systems, particularly in the absence of transparency, audit mechanisms, and regulatory oversight. This creates potential inconsistencies with Article 26 of the ICCPR, as automated systems may reproduce or amplify existing social inequalities (Barocas & Selbst, 2016; Eubanks, 2018).

Finally, the study identifies a critical gap in the form of limited access to effective remedies. Although rights are recognised at the constitutional level, institutional mechanisms for enforcement remain fragmented and often inaccessible. The absence of clear compensation frameworks and independent adjudicatory processes undermines compliance with Article 2(3) of the ICCPR, which requires effective and enforceable remedies for rights violations (Joseph & Castan, 2013).

Taken together, these findings indicate that India's digital governance framework, while normatively aligned in principle, exhibits significant structural and operational deficiencies that limit its ability to fully realise international human rights standards.

8. Conclusion and Recommendations

The findings of this study underscore a fundamental tension within India's digital governance framework: the rapid expansion of technological capabilities has not been matched by a corresponding evolution of legal safeguards and institutional accountability mechanisms. While India has made important strides in recognising digital rights through constitutional interpretation, particularly in the domain of privacy, these advances remain insufficient in the absence of coherent legislative design and effective enforcement structures (Baxi, 2007; Solove, 2021).

Addressing these challenges requires a comprehensive and multi-layered reform strategy. At the legislative level, there is an urgent need to enact a comprehensive surveillance law that clearly defines the scope, limits, and permissible grounds for surveillance, while incorporating safeguards such as prior judicial authorisation, necessity thresholds, and proportionality requirements. Such a framework would ensure compliance with the legality requirement under international human rights law and provide greater clarity and predictability in the exercise of state power (De Hert & Papakonstantinou, 2016).

In parallel, the Digital Personal Data Protection Act, 2023 must be strengthened, particularly by narrowing the scope of state exemptions and ensuring that government agencies remain subject to meaningful data protection obligations. Enhancing the independence, transparency, and functional autonomy of the Data Protection Board is essential to prevent regulatory capture and to ensure effective enforcement (Greenleaf, 2023; Kuner, 2017).

At the institutional level, the establishment of independent oversight mechanisms is critical. This includes the introduction of judicial or quasi-judicial authorisation processes for surveillance activities, as well as the development of specialised regulatory bodies equipped with technical expertise in areas such as data governance and algorithmic accountability (Murray, 2018). Strengthening grievance redressal systems and introducing clear compensation frameworks would further operationalise the right to an effective remedy.

From a doctrinal perspective, the development of a framework of cumulative proportionality is necessary to address the systemic nature of digital governance. Rather than evaluating individual measures in isolation, this approach would assess the combined impact of overlapping regulatory interventions on fundamental rights, thereby providing a more holistic and realistic understanding of rights infringement in digital contexts (Barak, 2012).

In conclusion, aligning India's digital governance framework with ICCPR standards is not merely a matter of international compliance but a constitutional imperative. The preservation of fundamental values such as liberty, dignity, and equality in a data-driven society depends on the ability of legal and institutional frameworks to keep pace with technological change. Without such alignment, the expansion of digital governance risks entrenching forms of state power that operate beyond effective legal control. The future of digital governance in India will therefore depend on its capacity to reconcile innovation with a robust, rights-oriented regulatory framework that is both principled and enforceable.

References

1. Aronson, B. (2021). Data governance in India: The evolving regulatory framework. *Asian Journal of Law and Society, 8*(2), 1–20.
2. Aust, A. (2013). *Modern treaty law and practice* (3rd ed.). Cambridge University Press.
3. Austin, G. (1999). *Working a democratic constitution: The Indian experience*. Oxford University Press.

4. Balkin, J. M. (2018). Free speech in the algorithmic society: Big data, private governance, and new school speech regulation. *UC Davis Law Review, 51*(3), 1149–1210.
5. Barak, A. (2012). *Proportionality: Constitutional rights and their limitations*. Cambridge University Press.
6. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732.
7. Baxi, U. (2007). *The future of human rights* (3rd ed.). Oxford University Press.
8. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 1–15.
9. De Hert, P., & Papakonstantinou, V. (2016). The General Data Protection Regulation (GDPR): A sound system for the protection of individuals. *Computer Law & Security Review, 32*(2), 179–194.
10. Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
11. Fenwick, H., & Phillipson, G. (2017). *Media freedom under the Human Rights Act*. Oxford University Press.
12. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines, 28*(4), 689–707.
13. Greenleaf, G. (2023). India's Digital Personal Data Protection Act 2023: A preliminary analysis. *Privacy Laws & Business International Report*.
14. Human Rights Committee. (1988). *General Comment No. 16: Article 17 (Right to Privacy)*. United Nations.
15. Human Rights Committee. (2011). *General Comment No. 34: Article 19 (Freedom of Expression)*. United Nations.
16. Joseph, S., & Castan, M. (2013). *The International Covenant on Civil and Political Rights: Cases, materials, and commentary* (3rd ed.). Oxford University Press.
17. Kshetri, N. (2019). The role of the state in developing a digital economy: Evidence from India. *Telecommunications Policy, 43*(10), 101845.
18. Kuner, C. (2017). *Transborder data flows and data privacy law*. Oxford University Press.
19. Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

20. Murray, A. D. (2018). *Information technology law: The law and society* (4th ed.). Oxford University Press.
21. Privacy International. (2019). *State of surveillance: India report*. Privacy International.
22. Seervai, H. M. (1996). *Constitutional law of India* (4th ed.). Universal Law Publishing.
23. Singh, P. (2019). The Information Technology Act and digital regulation in India. *Indian Journal of Law and Technology*.
24. Singh, P. (2021). Intermediary liability and digital regulation in India: A critical analysis. *Journal of Cyber Law Studies*.
25. Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.
26. United Nations. (1966). *International Covenant on Civil and Political Rights*.
27. United Nations General Assembly. (2013). *The right to privacy in the digital age*.
28. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99.
29. Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.