

National Security, Human Rights and AI Regulation in India: Balancing Liberty and Security in the Digital Age

Madhavi

Examiner of Trademark, Copyright & GI

Abstract

India's democratic framework faces a profound transformation at the intersection of national security imperatives, constitutional human rights, and the digital revolution. The emergence of artificial intelligence (AI) and social media as tools of communication, surveillance, and influence has redefined the relationship between the state and its citizens. This paper examines India's evolving legal architecture in the domains of national security and human rights, focusing particularly on the governance of AI and digital platforms. It argues that while the Indian state's efforts to safeguard sovereignty and public order are constitutionally legitimate, the expansive scope of security legislation and digital regulation presents risks to civil liberties and democratic accountability. Through historical and doctrinal analysis, this paper explores how India's constitutional and statutory frameworks have evolved from colonial preventive-detention laws to the digital-era governance of information ecosystems, highlighting the urgent need for a rights-based approach to security in the age of artificial intelligence.

INTRODUCTION

In the twenty-first century, the concept of national security has expanded far beyond territorial defense and military preparedness. Technological advancement—particularly the rapid development of artificial intelligence (AI), big-data analytic, and social media—has created new domains of risk and contestation. National security today encompasses cyber security, information integrity, and the resilience of digital infrastructures. In India, these transformations coincide with the world's largest experiment in democratic digitization: the Aadhaar biometric identity system, Digital India initiative, and rapid growth of AI-driven governance and commerce.

While digital technologies have enhanced transparency and efficiency, they have simultaneously created vulnerabilities. State and non-state actors now possess unprecedented power to manipulate information, conduct cyber attacks, and influence public discourse. Social media platforms have become instruments of both democratic engagement and political polarization. AI technologies enable predictive policing, facial recognition, and mass surveillance—tools that, if misused, may compromise privacy, expression, and due process (Baxi, 2008). The challenge for India, therefore, lies in reconciling **national security** with **human rights**, ensuring that security imperatives do not erode constitutional guarantees.

The constitutional foundation of India's security governance rests on two pillars: **the state's duty to protect sovereignty and integrity**, and **the citizen's right to life and liberty**. Articles 19 and 21 of the Constitution guarantee freedom of speech and personal liberty, while Article 22 allows preventive detention under specific circumstances. This duality—freedom and restraint—defines India's ongoing

struggle to balance liberty and order in both physical and digital domains.

As AI and social media reshape India's public sphere, traditional legal frameworks such as the **National Security Act (1980)**, **Unlawful Activities (Prevention) Act (1967, amended 2019)**, and **Information Technology Act (2000)** are being reinterpreted to address emerging threats. However, critics argue that these statutes, often applied with limited oversight, risk expanding executive power at the expense of individual freedoms. The recent **Digital Personal Data Protection Act (2023)**, while marking a milestone in data-privacy law, grants broad exemptions to government agencies, raising questions about proportionality and necessity in state surveillance practices (Kumar, 2023).

This paper situates India's national-security and digital-rights regime within a historical and constitutional context. It traces the evolution from colonial-era preventive detention to contemporary data governance and algorithmic regulation. It contends that the constitutional vision of India as a democratic republic—grounded in dignity, equality, and freedom—must remain central as the state navigates the complexities of technological sovereignty.

Historical Context: From Colonial Control to Digital Constitutionalism

India's approach to national security and human rights cannot be understood without reference to its colonial past. The **British Raj** governed through a system of exceptional powers designed to maintain political control rather than public welfare. The **Rowlatt Act of 1919** authorized preventive detention without trial, sparking nationwide protests led by Mahatma Gandhi. This legacy of emergency governance profoundly influenced India's post-independence legal architecture (Singh, 2015).

After independence in 1947, the framers of the **Constitution of India (1950)** sought to establish a democratic republic that would prevent the arbitrary exercise of power while allowing the state to preserve order and security. **Dr. B.R. Ambedkar**, in the Constituent Assembly Debates, acknowledged that freedom without security could lead to anarchy, while excessive security could erode democracy. Thus, the Constitution embedded both **fundamental rights** (Part III) and **emergency powers** (Part XVIII), balancing liberty with stability.

Preventive Detention and Early Security Laws

Preventive detention—arguably the most controversial legacy of colonial rule—was incorporated into the Constitution under **Article 22**, which permits detention without trial for specified periods. The **Preventive Detention Act, 1950**, enacted soon after independence, allowed the state to detain individuals suspected of threatening public order or national security. Although the Act expired in 1969, its principles resurfaced in later legislation such as the **Maintenance of Internal Security Act (MISA)¹, 1971**, and the **National Security Act (NSA), 1980**.

The **Supreme Court of India** initially adopted a deferential approach toward preventive detention. In *A.K. Gopalan v. State of Madras* [(1950) SCR 88], the Court upheld the Preventive Detention Act, emphasizing legislative supremacy in matters of security. However, in *Maneka Gandhi v. Union of India* [(1978) 1 SCC 248], the Court revolutionized rights jurisprudence by interpreting “procedure established by law” under Article 21 to mean “**just, fair, and reasonable**”, thereby extending constitutional scrutiny to administrative and legislative actions affecting liberty.

¹ The **MISA (1971)** was extensively used during the **Emergency period (1975–77)** to detain political opponents without trial, leading to widespread condemnation and its eventual repeal.

The Evolution of Security Governance

The post-Emergency era witnessed growing awareness of the need to reconcile state security with civil liberties. The **National Security Act (1980)** authorized preventive detention to maintain public order but mandated periodic review by advisory boards. Despite procedural safeguards, the Act has been criticized for its vagueness and potential misuse against dissenters (Austin, 1999).

Parallelly, India's participation in international human-rights regimes—such as ratifying the **International Covenant on Civil and Political Rights (ICCPR)** in 1979—expanded the normative framework for evaluating national laws. However, the incorporation of these standards into domestic practice remained uneven, constrained by national-security priorities and limited institutional capacity (Rajagopal, 2000).

From Analog to Digital Security

The liberalization of India's economy in the 1990s and the subsequent information-technology revolution redefined the meaning of security. The **Information Technology Act (2000)** marked India's first comprehensive attempt to regulate cyberspace, granting the government authority to block content, intercept communications, and investigate cybercrimes. While justified on grounds of cybersecurity and sovereignty, these powers raised new constitutional questions concerning privacy and free expression.

In *Justice K.S. Puttaswamy (Retd.) v. Union of India* [(2017) 10 SCC 1], the Supreme Court unanimously recognized the **right to privacy** as a fundamental right under Article 21, reshaping the discourse on digital rights. The Court held that any restriction on privacy must meet tests of legality, necessity, and proportionality. This landmark ruling laid the groundwork for data-protection and AI-governance discourse in India, though practical enforcement remains inconsistent.

India's National-Security Legal Framework

India's national-security architecture comprises several overlapping statutes aimed at combating terrorism, preserving public order, and protecting sovereignty. Among these, the **Unlawful Activities (Prevention) Act (UAPA), 1967**, the **National Investigation Agency Act (2008)**, and the **National Security Act (1980)** form the core.

The **UAPA**, originally designed to curb secessionist movements, has evolved into India's primary counter-terrorism law. The **2019 amendment** empowered the central government to designate individuals—not merely organizations—as terrorists, without prior judicial determination. Critics argue this contravenes the presumption of innocence and enables pre-trial stigmatization (Baxi, 2008). The **National Investigation Agency (NIA) Act** centralized the investigation of such offenses, expanding federal control over internal security.

The **National Security Act (1980)**, invoked frequently in cases of communal unrest or perceived threats to sovereignty, authorizes preventive detention for up to twelve months. While intended as an emergency tool, the Act's subjective language ("acting in a manner prejudicial to the security of the state") has allowed wide administrative discretion².

In addition, the **Armed Forces (Special Powers) Act (AFSPA), 1958**, grants sweeping powers to security forces in "disturbed areas," including the use of lethal force and immunity from prosecution without central sanction. Though justified as essential to counter-insurgency, it has drawn criticism from the UN

² The **Advisory Board mechanism** under Section 9 of the NSA offers procedural review, but it rarely overturns detentions, leading scholars to describe the process as "symbolic rather than substantive oversight."

Human Rights Council for enabling impunity.

Human-Rights Jurisprudence and Constitutional Safeguards

India's constitutional architecture enshrines an expansive catalogue of fundamental rights—Articles 14 (equality), 19 (freedoms), 20–22 (protection of life and liberty). Yet, in practice, these rights have often been subordinated to security exigencies. Judicial interpretation has oscillated between deference and activism.

The **Supreme Court's post-Maneka era** saw the emergence of “**substantive due process**” as a constraint on state power. Landmark decisions—*Sunil Batra v. Delhi Administration* [(1978) 4 SCC 494], *Francis Coralie Mullin v. Administrator, Union Territory of Delhi* [(1981) 1 SCC 608]—expanded the meaning of liberty to include dignity and humane conditions of detention.

In the digital context, *Puttaswamy* (2017) became the cornerstone of India's human-rights jurisprudence, affirming that privacy is intrinsic to autonomy and dignity. Subsequent cases—such as *Anuradha Bhasin v. Union of India* [(2020) 3 SCC 637]—extended this reasoning to online freedoms, holding that indefinite internet shutdowns violate proportionality and due process.

Nevertheless, tensions persist between judicial pronouncements and executive practice. The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** impose obligations on social-media intermediaries to trace “originators” of information, raising concerns about end-to-end encryption and surveillance (Kumar, 2023). Courts have yet to fully delineate the boundaries of such obligations vis-à-vis Articles 19(1)(a) and 21.

AI, Social Media, and Digital Regulation

AI and algorithmic governance have introduced new dimensions to national security. India's **National Strategy for Artificial Intelligence (NITI Aayog, 2018)** envisions “AI for All,” emphasizing inclusivity and growth. However, regulatory frameworks remain fragmented. The **Digital Personal Data Protection Act (2023)**, replacing earlier drafts of a privacy bill, seeks to safeguard personal data but exempts government processing “in the interests of sovereignty and integrity of India.” This broad exception undermines the rule of proportionality established in *Puttaswamy*.

Social-media regulation presents parallel challenges. The **IT Rules (2021)** require platforms to remove content within tight timelines and appoint compliance officers. While intended to curb misinformation, these provisions risk chilling effect on expression, particularly when combined with penal laws such as Sections 66A and 69A of the IT Act. Although Section 66A was struck down in *Shreya Singhal v. Union of India* [(2015) 5 SCC 1], instances of its continued invocation by lower authorities persist³.

AI applications in policing and national-security surveillance—such as predictive analytics, facial recognition, and social-media monitoring—pose fresh ethical dilemmas. The absence of comprehensive AI legislation leaves governance dependent on executive discretion. Without transparency requirements or algorithmic-impact assessments, citizens face difficulty contesting automated decisions that affect liberty or access to services.

Ethical and Constitutional Challenges

The interplay between national security, human rights, and AI highlights core ethical tensions. On one

³ In 2022, the Supreme Court in *Peoples Union for Civil Liberties v. Union of India* directed that police refrain from using Section 66A, reaffirming its invalidation.

hand, the state bears an obligation to protect citizens from terrorism, cybercrime, and disinformation. On the other, unrestrained surveillance and data collection can erode democratic trust. The challenge lies in ensuring **proportionality, necessity, and accountability**.

From an ethical standpoint, AI-driven governance risks entrenching bias. Predictive-policing algorithms trained on biased data may disproportionately target marginalized communities, replicating structural inequalities. Similarly, social-media moderation driven by opaque algorithms raises questions about fairness and freedom of expression. Ethical AI frameworks, such as those proposed by the European Union and the OECD, emphasize transparency and human oversight—principles that India has yet to codify. Constitutionally, unchecked digital surveillance may infringe Article 21. The Supreme Court in *Puttaswamy* mandated that state intrusion into privacy must satisfy three criteria: legality, necessity, and proportionality. Yet, programs like the **Central Monitoring System (CMS)** and **NATGRID** operate with limited statutory backing and minimal judicial review⁴.

Policy Recommendations

1. **Codify AI Governance Principles.** India should enact a dedicated **Artificial Intelligence Regulation Act** incorporating transparency, accountability, and non-discrimination.
2. **Strengthen Judicial Oversight.** Establish a **Digital Rights Tribunal** to review surveillance and data-processing orders.
3. **Limit Preventive Detention.** Amend the **NSA** and **UAPA** to incorporate stricter evidentiary standards and periodic judicial review.
4. **Enhance Data-Protection Safeguards.** Narrow governmental exemptions in the **DPDP Act (2023)** to align with proportionality principles.
5. **Promote Digital Literacy.** Civic education on AI ethics and privacy can foster participatory oversight.
6. **Encourage Multi-Stakeholder Regulation.** Include civil-society actors and independent experts in oversight committees for AI deployment in policing or governance.

Conclusion

India's trajectory from colonial emergency powers to digital governance reveals a persistent tension between liberty and security. Each technological epoch—from print censorship to algorithmic regulation—has tested the resilience of constitutional democracy. As the world's largest democracy enters the age of artificial intelligence, its credibility will depend on embedding transparency, accountability, and constitutionalism within its national-security apparatus.

Balancing security with human rights is not a zero-sum equation but a question of institutional design. A rights-respecting security state, grounded in judicial oversight and ethical technology governance, can protect both sovereignty and dignity. India's constitutional promise—of liberty under law—must remain the guiding principle in regulating AI, social media, and the national-security state.

References

1. Austin, G. (1999). *The Indian Constitution: Cornerstone of a Nation*. Oxford University Press.
2. Baxi, U. (2008). *Human Rights in a Posthuman World: Critical Essays*. Oxford University Press.
3. Bradshaw, S., & Howard, P. N. (2019). *The Global Disinformation Order: 2019 Global Inventory of*

⁴ NATGRID integrates data from multiple agencies, including immigration, banking, and telecom, for national-security analysis—raising significant data-protection concerns.

Organised Social Media Manipulation. Oxford Internet Institute.

4. Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review of Law, Computers & Technology*, 33(2), 76–99.
5. Kumar, R. (2023). Digital sovereignty and data governance in India: A policy perspective. *Centre for Internet and Society*.
6. Rajagopal, B. (2000). Human rights and development: Law, policy and practice in postcolonial India. *Human Rights Quarterly*, 22(4), 925–958.
7. Singh, M. (2015). Colonial governance and the origins of India's security state. *Modern Asian Studies*, 49(6), 1849–1873.
8. Supreme Court of India. A.K. Gopalan v. State of Madras, (1950) SCR 88.
Supreme Court of India. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
9. Supreme Court of India. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
10. Supreme Court of India. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
11. Supreme Court of India. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
12. Supreme Court of India. Sunil Batra v. Delhi Administration, (1978) 4 SCC 494.
13. Supreme Court of India. *Francis Coralie Mull