LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 3 | Issue 1

2025

DIGITAL SOVEREIGNTY AND STATE RESPONSIBILITY: NAVIGATING CYBERSECURITY CHALLENGES IN INDIA'S LEGAL LANDSCAPE

Amal Singh Patel[1] & Dr. Axita Shrivastava[2]

I. ABSTRACT

This research paper explores the evolving dynamics of digital sovereignty and state responsibility within India's cybersecurity landscape. It critically examines India's legal and regulatory framework, focusing on the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and sector-specific cybersecurity mandates. The study highlights the role of Indian institutions like CERT-In, NCIIPC, and regulatory bodies including TRAI, RBI, and SEBI in shaping compliance mechanisms. Landmark judicial pronouncements, including K.S. Puttaswamy v. Union of India and Shreya Singhal v. Union of India, are analyzed to understand constitutional safeguards in cyberspace governance. The paper delves into India's assertion of sovereignty through data localization, extraterritorial jurisdiction, and blocking powers under Section 69A of the IT Act. It discusses India's strategic position in global digital governance, balancing territorial and data-centric sovereignty models. The research also examines India's stance on international legal norms, including its engagement with UNGGE, OEWG, and resistance to the Budapest Convention. By integrating legal doctrines, regulatory structures, and global frameworks, this paper offers a comprehensive analysis of India's approach to navigating cybersecurity challenges while asserting digital sovereignty and fulfilling its responsibilities in cyberspace.

[1] 10th Semester B.A.LL.B Student, Amity Law School, Amity University Uttar Pradesh.
[2] Assistant Professor, Amity Law School, Amity University Uttar Pradesh.

 (ISSN: 2583-7753)

II. KEYWORDS

Digital sovereignty, State responsibility, Cybersecurity compliance, Data protection, International cyber law.

III. INTRODUCTION

A. Contextualizing Digital Sovereignty in the Indian Framework

Digital sovereignty embodies a nation's authority to regulate its digital infrastructure, data flows, and cyberspace activities within its jurisdiction. In India, this notion intersects with constitutional mandates, cyber laws, and international norms. The interplay between Article 19(1)(a) of the Indian Constitution, ensuring freedom of speech and expression, and the regulatory oversight under the Information Technology Act, 2000 (IT Act), sets the tone for India's assertion over its digital domain. This relationship grows complex as cross-border data flows and foreign digital entities operating in India challenge the state's regulatory autonomy. The Supreme Court's verdict in *K.S. Puttaswamy v. Union of India*, recognized privacy as a fundamental right, shaping India's data governance and anchoring digital sovereignty in the constitutional framework.[3]

India's data localization policies reflect its pursuit of digital sovereignty. The Reserve Bank of India mandated payment system operators to store data locally under the *Storage of Payment System Data Circular*, 2018, ensuring that critical financial data remains within the national territory.[4] Similarly, the *Draft Data Protection Bill*, 2021, requires certain sensitive personal data to be stored locally, underscoring India's claim over its digital infrastructure. These measures reveal India's strategic approach to safeguard national security, privacy, and economic interests in cyberspace.

The global reliance on digital platforms controlled by transnational corporations has exposed India's vulnerabilities. The Cambridge Analytica scandal involving Facebook underscored the need for stricter data governance laws to protect Indian citizens from

[3] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[4] Reserve Bank of India, *Storage of Payment System Data Circular*, 2018.

foreign influence.[5] The government's move to ban Chinese apps under Section 69A of the IT Act, citing national security concerns, exemplifies India's attempt to assert digital sovereignty amidst geopolitical tensions. This aligns with the National Cyber Security Policy, 2013, which emphasizes securing cyberspace from external threats.[6]

International law influences India's stance on digital sovereignty. The Tallinn Manual on the International Law Applicable to Cyber Warfare suggests that states possess sovereignty over their cyberspace, similar to their land, sea, and air domains.[7] However, India's adherence to such frameworks remains cautious. The country actively participates in dialogues under the United Nations Group of Governmental Experts (UNGGE) on responsible state behavior in cyberspace, balancing its interests against global standards. This balancing act becomes crucial as India advocates for a multilateral approach to Internet governance through bodies like the International Telecommunication Union (ITU), resisting a Western-dominated multi-stakeholder model.[8]

India's legislative apparatus struggles to keep pace with the evolving digital landscape. The IT Act, primarily enacted to address e-commerce and cybercrimes, fails to comprehensively cover issues like data sovereignty, cross-border data transfers, and cybersecurity. The Personal Data Protection Bill, modeled partly on the EU's General Data Protection Regulation (GDPR), aims to fill this gap. It introduces concepts of data fiduciary and data principal, establishing a consent-driven framework for data processing.[9] Yet, its provisions on data localization have sparked debates on protectionism and international trade implications.

India's judiciary plays a pivotal role in shaping digital sovereignty. In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the IT Act, affirming the

[5] David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 91 (2010).
[6] Ministry of Electronics and Information Technology, *National Cyber Security Policy*, 2013 (India).
[7] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* 22-24 (Cambridge Univ. Press 2013).
[8] United Nations Group of Governmental Experts (UNGGE), *Reports on the Developments in the Field of Information and Telecommunications in the Context of International Security*, 2021.
[9] Personal Data Protection Bill, 2021, No. 17, Acts of Parliament, 2021 (India).

precedence of free speech over arbitrary state control. However, the judgment also upheld intermediary liability under Section 79, which mandates digital platforms to comply with lawful orders. This duality captures the tension between individual rights and state sovereignty in digital governance.[10]

Telecommunications laws contribute to India's digital sovereignty narrative. The *Telecom Regulatory Authority of India (TRAI)* governs spectrum allocation, licensing, and foreign investment in telecom infrastructure, crucial for securing digital borders. Recent discussions on introducing net neutrality rules and regulating Over-The-Top (OTT) services under TRAI's jurisdiction reflect India's efforts to assert control over digital service providers.[11] The convergence of telecom and digital regulations signifies India's intent to comprehensively govern cyberspace.

India's approach to digital sovereignty also extends to cybersecurity. The *Indian Computer Emergency Response Team (CERT-In)* operates under Section 70B of the IT Act, coordinating responses to cyber threats. Recent guidelines issued by CERT-In in April 2022 mandate organizations to report cybersecurity incidents within six hours, a move to strengthen national cyber defenses.[12] This framework aims to enhance India's cyber resilience, reinforcing its sovereignty over digital infrastructure.

B. Research Objectives

1. To examine the legal and regulatory frameworks governing digital sovereignty and cybersecurity compliance in India.
2. To analyze the role of Indian judicial interpretations in shaping state responsibility within cyberspace.

[10] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[11] Telecom Regulatory Authority of India (TRAI), *Consultation Paper on Regulatory Framework for OTT Communication Services*, 2022.
[12] Indian Computer Emergency Response Team (CERT-In), *Cybersecurity Directions*, April 2022.

3. To evaluate India's position in global digital governance and its approach to international cybersecurity norms and cooperation.

C. Research Questions

1. How do India's existing laws, including the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, assert and protect digital sovereignty in the context of cybersecurity?
2. What impact have landmark judgments, such as *K.S. Puttaswamy v. Union of India* and *Shreya Singhal v. Union of India*, had on defining the balance between state control and individual rights in India's digital governance?
3. How does India's stance on international frameworks like the UNGGE, OEWG, and its opposition to the Budapest Convention reflect its broader strategy for maintaining digital sovereignty while engaging in global cyber law discourses?

D. Research Methodology

This research adopts a doctrinal legal research methodology, focusing on the systematic analysis of statutory provisions, judicial pronouncements, policy documents, and international legal instruments relevant to India's digital sovereignty and cybersecurity framework. Primary sources include the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and key Supreme Court rulings such as K.S. Puttaswamy v. Union of India and Shreya Singhal v. Union of India. Secondary sources comprise scholarly articles, government reports, cybersecurity guidelines, and international law manuals like the Tallinn Manual 2.0. The research employs comparative analysis to evaluate India's legal framework in relation to international standards, particularly the European Union's GDPR and global cybersecurity norms established by bodies like UNGGE and OEWG. Qualitative content analysis is used to interpret legal texts, policies, and case law, ensuring a comprehensive understanding of India's cybersecurity governance. The methodology critically assesses the balance between state

responsibility, individual rights, and national security, contributing to the evolving discourse on digital sovereignty in the Indian context.

IV. THEORETICAL FOUNDATIONS OF DIGITAL SOVEREIGNTY

A. Evolution of Sovereignty in Digital Domains

Traditional sovereignty centered on physical borders and state authority over land, air, and maritime zones. But digital space is fluid. Unlike physical territory, cyberspace lacks defined boundaries. This change forced a rethinking of classical Westphalian sovereignty. Sovereignty today must account for non-territorial, virtual structures.

States originally had limited say in internet infrastructure. Transnational corporations like Google, Meta, and Amazon own a vast majority of global data servers. This undermines local jurisdiction. International norms evolved to meet this gap. The Tallinn Manual 2.0 reaffirms that states hold sovereignty in cyberspace, just as in the physical realm. Yet, implementation is ambiguous. Enforcement is harder. The global nature of cyberspace blurs state control. The United Nations Group of Governmental Experts (UNGGE) supports the view that international law applies to cyber operations. But it offers no enforcement mechanism. Sovereignty becomes more aspirational than enforceable. State responses vary. China has codified its digital control in the Cybersecurity Law of 2017. Russia passed the Sovereign Internet Law in 2019. These models illustrate how states now treat cyberspace as a domain of sovereignty regulated and segmented.

India’s journey reflects an evolving assertion. Initially, India had a minimalist internet governance approach. Over time, concerns about surveillance, data misuse, and foreign dominance forced a shift. The Supreme Court in K.S. Puttaswamy v. Union of India, declared privacy a fundamental right, laying the constitutional foundation for India's digital sovereignty. The judgment linked data to dignity, autonomy, and freedom.

Post-2017, sovereignty included control over data collection, storage, and transfer. The banning of Chinese apps under Section 69A of the Information Technology Act, 2000,

shows an aggressive assertion of sovereign control over foreign digital platforms.13 The CERT-In Directions, 2022, reinforced this trend by mandating quick breach reporting. Sovereignty now means active defense, proactive governance, and secure digital infrastructure.

B. Territorial vs. Data-Centric Sovereignty Models

Two major frameworks shape state authority over cyberspace. One focuses on territorial control, the other on the control of data regardless of where it resides. Territorial sovereignty applies when a server or data processor is within national borders. States claim jurisdiction based on physical presence. This aligns with traditional legal doctrines. Data-centric sovereignty is newer. It is based on the principle that states have authority over their citizens' data, even if stored abroad. This principle is key to laws like the European Union's General Data Protection Regulation (GDPR). Article 3 of GDPR allows the EU to regulate any entity that processes the personal data of EU residents even outside the EU.

India is adopting a hybrid model. The Digital Personal Data Protection Act, 2023 (DPDP Act), enforces data protection based on both territorial and extraterritorial jurisdiction. Section 3(b) of the Act applies the law to data processing done outside India, if the data pertains to goods or services offered to Indian residents. It empowers India to regulate offshore digital services, asserting a data-centric approach. India's earlier push for data localization reflected a tilt toward territoriality. The Reserve Bank of India's 2018 directive required payment data to be stored only in India. The proposed e-commerce policy also echoed these localization demands. Critics argue this harms startups and invites retaliatory trade measures. Supporters claim it strengthens digital sovereignty and national security.

[13] Ministry of Electronics and Information Technology (MeitY), Press Release on Blocking of 59 Apps, June 2020.

The dual model reflects India's balancing act. In Shreya Singhal v. Union of India, the Supreme Court upheld intermediary liability under Section 79 while striking down Section 66A as unconstitutional. The judgment acknowledged a sovereign's right to regulate but also emphasized fundamental freedoms. This highlights India's effort to create sovereign control that still aligns with democratic values. Data sovereignty also emerges in public procurement. India's preference for indigenous data storage providers under the Public Procurement (Preference to Make in India) Order, 2017, promotes national digital control. The National Cyber Security Strategy, still in draft, proposes indigenous cyber capabilities and governance, reinforcing this model.

C. India's Unique Position in Global Digital Governance

India does not mirror any one global model. The United States champions a market-driven, multi-stakeholder internet. China advocates state-centric governance. The EU focuses on strong privacy frameworks. India situates itself uniquely, drawing selectively from all three.

India supports multilateralism in cyberspace. It calls for a larger state role in global digital governance. The Indian stance at the International Telecommunication Union (ITU) supports rules made by sovereign states, not tech giants. This seeks to counterbalance the dominance of Western private corporations in internet architecture.

India also plays a leading role in South-South cooperation. Its digital public infrastructure model, through platforms like Aadhaar and UPI, is being exported to countries in Africa and South-East Asia. This bolsters India's diplomatic footprint and redefines digital sovereignty as a form of technological diplomacy.

India's internal digital policy landscape further asserts sovereignty. The DPDP Act introduces the Data Protection Board of India under Section 18. It allows the state to enforce accountability through penalties up to ₹250 crore for non-compliance. The Act also provides for blocking access to digital services under Section 37. These provisions reflect sovereignty in enforcement, regulation, and deterrence.

International negotiations reflect India's sovereign assertions. At the WTO, India resists e-commerce liberalization without data rights guarantees. It maintains a firm position against permanent moratoriums on customs duties for electronic transmissions. This protects India's right to tax and regulate digital flows.

India's jurisprudence also reflects its nuanced approach. In Anuradha Bhasin v. Union of India, the Supreme Court held that access to the internet is part of the right to freedom of speech under Article 19(1)(a). Yet it allowed restrictions on grounds of national security under Article 19(2). The Court upheld a sovereign's right to disconnect digital access if justified. This reinforces the dual responsibility securing rights while exercising sovereign control.

V. REGULATORY FRAMEWORK AND LEGAL JURISDICTION

A. The Information Technology Act Framework

The Information Technology Act, 2000, constitutes the principal legislative framework governing digital activities within India. Its enactment responded to the growing necessity for a legal structure that could recognize electronic records and facilitate electronic commerce. Initially, the Act focused on legitimizing electronic contracts and digital signatures. However, subsequent amendments expanded its ambit to encompass cybersecurity, cybercrime, data privacy, and intermediary liability.

Section 66 of the Act criminalizes hacking and imposes penalties for unauthorized access to computer systems. This provision equips India with statutory tools to regulate unlawful intrusions into digital spaces. The scope of Section 66A, which penalized offensive online messages, was curtailed by the Supreme Court in *Shreya Singhal v. Union of India*, The Court struck down Section 66A, citing its violation of Article 19(1)(a) of the Constitution. Despite this, the judgment upheld intermediary liability rules, reinforcing the state's regulatory role over digital intermediaries.[14]

[14] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

Section 69, a cornerstone of the Act, authorizes the interception, monitoring, or decryption of digital information by government agencies in the interest of sovereignty, integrity, defense, or public order. In *PUCL v. Union of India*, the Supreme Court laid down procedural safeguards for telephone tapping. These safeguards now inform the interpretation of Section 69, ensuring that surveillance powers are not abused without proper oversight.[15] Section 69A empowers the government to block public access to online content. This provision gained prominence when India banned 59 Chinese mobile applications, including TikTok and WeChat, citing national security concerns in 2020.[16]

The Act establishes the Indian Computer Emergency Response Team (CERT-In) under Section 70B. CERT-In plays a critical role in coordinating responses to cybersecurity incidents. The CERT-In Directions, issued in 2022, mandate that cybersecurity incidents must be reported within six hours. This reporting requirement reinforces India's cyber defense mechanism and underpins digital sovereignty by ensuring timely government intervention in cyber incidents.[17]

Section 70 extends sovereign control over Critical Information Infrastructure (CII), designating systems vital for national security, economic stability, and public health. Unauthorized access to CII attracts severe penalties, including life imprisonment if it results in death or severe harm. This provision aligns with the global understanding of cybersecurity as a domain of national defense.

Intermediary liability is another essential aspect of the IT Act. Section 79 provides conditional immunity to intermediaries, such as social media platforms and internet service providers, shielding them from liability for user-generated content if they observe due diligence. The *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, further detail this obligation. Intermediaries must act on government

[15] PUCL v. Union of India, (1997) 1 SCC 301.
[16] Ministry of Electronics and Information Technology (MeitY), Press Release on Blocking of 59 Apps, June 2020.
[17] Indian Computer Emergency Response Team (CERT-In), *Cybersecurity Directions*, April 2022.

orders to remove unlawful content within stipulated timelines. This framework enables India to exercise jurisdiction over global digital platforms operating in its territory.

The IT Act's extraterritorial jurisdiction is enshrined in Section 75. It allows the prosecution of offenses committed outside India if the affected computer system is located within India. This provision underpins India's digital sovereignty by asserting legal authority over cyberspace activities that impact Indian citizens or systems.

The Act was amended post the Supreme Court's ruling in *Anuradha Bhasin v. Union of India*, The Court recognized access to the internet as an integral part of the right to freedom of speech under Article 19(1)(a). However, it also affirmed the state's right to impose restrictions under Article 19(2), including internet shutdowns when necessary for national security or public order.[18] This dual recognition cements the role of the IT Act in balancing individual rights with sovereign control.

B. Personal Data Protection Legislation

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant milestone in India's digital governance landscape. The Act provides a comprehensive framework for personal data processing, balancing the individual's right to privacy with the legitimate needs of data processing entities. The DPDP Act replaces Section 43A of the IT Act, which previously offered limited redress for data breaches. Section 3 defines the scope of the Act. It applies to the processing of digital personal data within India and extraterritorially if the data relates to goods or services offered to Indian residents. This provision aligns with the principle of data-centric sovereignty, ensuring India's jurisdiction extends to global data controllers handling Indian citizens' data.[19]

Section 4 mandates that data processing must occur for lawful purposes, either with the consent of the Data Principal or under certain legitimate uses. Section 7 details these legitimate uses, which include compliance with legal obligations, emergencies, public

[18] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[19] Digital Personal Data Protection Act, 2023, § 3, No. 22, Acts of Parliament, 2023 (India).

health, and state functions. This structure mirrors the EU's GDPR while tailoring the obligations to India's unique socio-political context.[20] The rights of the Data Principal, defined under Section 11, include access to data, correction, completion, updating, and erasure. These rights empower individuals, reinforcing privacy as articulated in *K.S. Puttaswamy v. Union of India*, where the Supreme Court recognized privacy as a fundamental right.[21]

Section 10 introduces the concept of Significant Data Fiduciaries (SDFs). The government may designate data fiduciaries as significant based on the volume and sensitivity of data processed, risk to sovereignty, and public order. SDFs must appoint Data Protection Officers and conduct regular Data Protection Impact Assessments. This requirement strengthens compliance and accountability.

Section 33 prescribes penalties for non-compliance, with fines extending up to ₹250 crore. This reflects India's commitment to enforcing data protection rigorously. Section 37 empowers the government to block access to digital services that repeatedly breach data protection norms. These provisions enhance India's enforcement capacity, enabling it to assert digital sovereignty over foreign entities.

The Act establishes the Data Protection Board of India under Section 18. The Board functions as an independent regulator, adjudicating disputes and imposing penalties. Its structure mirrors global regulatory bodies like the UK's Information Commissioner's Office (ICO), ensuring checks and balances in enforcement. The DPDP Act embodies India's hybrid regulatory approach. It incorporates data localization elements, allowing the government to restrict cross-border data transfers under Section 16. This provision ensures critical personal data remains within national borders, supporting digital sovereignty.

[20] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), art. 6.
[21] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

Section 9 addresses the processing of children's data, mandating verifiable parental consent and prohibiting behavioral monitoring or targeted advertising directed at children. This provision safeguards vulnerable groups, aligning with international best practices. Exemptions under Section 17 provide flexibility. Data processing for national security, research, or archiving purposes may bypass certain obligations. These carve-outs ensure the law remains adaptable without compromising state interests.

C. Critical Information Infrastructure Protection Norms

Critical Information Infrastructure (CII) refers to systems essential for the security, economy, public health, or safety of a nation. The Information Technology Act, 2000 (IT Act) lays the foundational framework for the protection of CII in India. Section 70 of the IT Act defines CII as any computer resource whose incapacitation or destruction would have a debilitating impact on national security, the economy, public health, or safety.[22] This provision grants the Indian government powers to declare any sector or system as CII and to prescribe necessary safeguards.

The National Critical Information Infrastructure Protection Centre (NCIIPC), established in 2014 under the National Technical Research Organisation (NTRO), is the designated nodal agency for protecting CII. The NCIIPC operates under a legal mandate provided by Section 70A of the IT Act. Its role includes identifying critical sectors, issuing advisories, coordinating with stakeholders, and monitoring threats to CII. The agency prioritizes sectors like energy, banking and financial services, transportation, government services, strategic manufacturing, and telecom.[23]

The CERT-In (Indian Computer Emergency Response Team) complements NCIIPC's mandate by coordinating responses to cybersecurity incidents across sectors. Under Section 70B of the IT Act, CERT-In mandates incident reporting, particularly involving CII. The Cybersecurity Directions of 2022 issued by CERT-In require the reporting of

[22] Information Technology Act, 2000, § 70, No. 21, Acts of Parliament, 2000 (India).
[23] National Critical Information Infrastructure Protection Centre (NCIIPC), *Guidelines for the Protection of Critical Information Infrastructure*, 2022.

cybersecurity incidents within six hours. This rapid reporting framework enhances the state's ability to contain breaches and reinforces sovereign oversight over digital infrastructure.[24]

Penalties under Section 70(3) of the IT Act are stringent. Unauthorized access to CII attracts imprisonment up to ten years and a fine. If such access endangers life or causes death, the penalty extends to life imprisonment. These legal consequences reflect the critical importance of CII for national defense and economic stability.

International cooperation shapes India's CII protection norms. India engages bilaterally with countries like the United States, Japan, and Israel for cybersecurity collaboration. These partnerships facilitate information sharing, joint exercises, and capacity-building. The US-India Cyber Framework Agreement (2016) emphasizes cooperation on protecting critical infrastructure and countering cyber threats.[25]

The National Cyber Security Policy, 2013, outlines India's broader cybersecurity posture. It highlights the need to secure CII, foster public-private partnerships, and promote indigenous cybersecurity technologies. The draft National Cyber Security Strategy further builds on this, proposing sector-specific guidelines, periodic audits, and mandatory incident reporting to strengthen CII defenses.

Judicial precedents affirm the state's duty to secure CII. In *RBI v. Jayantilal N. Mistry*, the Supreme Court upheld the public's right to access information involving regulatory bodies like the Reserve Bank of India. This ruling underscores the balance between transparency and security, ensuring that regulatory oversight over CII remains accountable without compromising sensitive infrastructure.[26]

The NCIIPC also conducts regular threat assessments. It categorizes CII entities based on risk and ensures they implement baseline security controls. These include network

[24] Indian Computer Emergency Response Team (CERT-In), *Cybersecurity Directions*, April 2022.
[25] US-India Cyber Framework Agreement, 2016.
[26] RBI v. Jayantilal N. Mistry, (2016) 3 SCC 525.

segmentation, encryption standards, access controls, and real-time monitoring. The Guidelines for the Protection of Critical Information Infrastructure, 2022, issued by NCIIPC, mandate sector-specific cybersecurity practices. They recommend regular vulnerability assessments, red teaming exercises, and compliance with global standards like ISO 27001 and NIST frameworks.

D. Extraterritorial Application of Indian Cyber Laws

The principle of extraterritorial jurisdiction extends India's legal authority beyond its borders. This is essential in cyberspace, where data flows and cybercrimes transcend national boundaries. Section 75 of the IT Act asserts extraterritorial jurisdiction. It applies to offenses committed outside India if the act involves a computer, system, or network located in India.[27] This provision equips Indian authorities to prosecute foreign cybercriminals whose actions impact Indian systems.

The Digital Personal Data Protection Act, 2023 (DPDP Act) further reinforces extraterritoriality. Section 3(b) applies the Act to data processing outside India if the data relates to goods or services offered to individuals within India. This mirrors global standards, such as the EU's GDPR, which asserts jurisdiction based on the location of the data subject, not the processor.[28]

Enforcement of extraterritorial jurisdiction hinges on mutual legal assistance treaties (MLATs). India has signed MLATs with several countries, enabling legal cooperation in cybercrime investigations. These treaties facilitate data sharing, evidence collection, and extradition. However, the absence of MLATs with certain jurisdictions poses challenges. To address this, India has been negotiating bilateral frameworks, such as the India-US CLOUD Act Agreement, to streamline cross-border data access for law enforcement.

In *Facebook Inc. v. Union of India*, the Supreme Court examined data-sharing obligations of global social media platforms with Indian authorities. The Court underscored that

[27] Information Technology Act, 2000, § 75, No. 21, Acts of Parliament, 2000 (India).
[28] Digital Personal Data Protection Act, 2023, § 3(b), No. 22, Acts of Parliament, 2023 (India).

foreign entities operating in India must comply with domestic laws, reinforcing jurisdictional reach over cross-border data flows.[29] This case reflects India's assertive approach to extraterritoriality in regulating digital platforms.

India's regulatory tools include blocking powers under Section 69A of the IT Act and Section 37 of the DPDP Act. These sections empower the government to block access to digital services that breach Indian laws, even if operated from outside India. The blocking of Chinese apps like TikTok exemplifies this. India cited national security concerns and enforced compliance through territorial enforcement mechanisms.

The Telecom Regulatory Authority of India (TRAI) imposes foreign investment restrictions and security conditions on telecom infrastructure. These regulations ensure that critical digital networks remain under Indian jurisdiction, even when involving foreign entities. The National Security Directive on Telecommunication Sector (2021) mandates the sourcing of telecom equipment from trusted vendors, reinforcing sovereign control over digital infrastructure.

Internationally, India resists frameworks that dilute state sovereignty in cyberspace. It has not signed the Budapest Convention on Cybercrime, citing concerns over its sovereignty. Instead, India supports a UN-led framework for cybercrime cooperation. The United Nations Group of Governmental Experts (UNGGE) and Open-Ended Working Group (OEWG) platforms reflect India's preference for multilateralism that respects sovereign interests.

The WTO debates on e-commerce and cross-border data flows present another dimension of extraterritoriality. India opposes permanent moratoriums on customs duties for electronic transmissions, arguing that such measures undermine its regulatory sovereignty. India maintains that data governance must remain within the purview of sovereign nations. The CERT-In Directions of 2022 impose compliance obligations on global service providers offering services in India. These include mandatory breach

[29] Facebook Inc. v. Union of India, 2020 SCC OnLine SC 845.

reporting and data retention, even for offshore entities. Non-compliance may lead to penalties or blocking orders, reinforcing India's extraterritorial regulatory stance.

VI. STATE RESPONSIBILITY IN CYBERSPACE

State responsibility in cyberspace emerges from the intersection of international law, national security, and digital sovereignty. The doctrine derives from foundational principles in public international law, particularly the law of state responsibility codified by the International Law Commission (ILC). The Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), 2001 provide the baseline. Under Article 2 of ARSIWA, a state commits an internationally wrongful act when its conduct is attributable to it and constitutes a breach of an international obligation.[30]

The principle of due diligence remains central. States are obligated to prevent their territories from being used to harm other states. This applies in cyberspace too. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations elaborates on this. Rule 6 of the Manual imposes a duty on states to prevent cyber operations emanating from their territory that cause serious harm to other states.[31] However, this obligation is subject to the knowledge of the state and its capability to prevent such acts.

India has consistently affirmed the applicability of international law to cyberspace. In its submissions to the United Nations Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG), India has endorsed the due diligence principle but also argued for flexibility in its application. Given the asymmetric capabilities of states, India maintains that capacity-building must accompany legal obligations.[32]

Attribution is a complex issue in cyberspace. Cyber operations are often cloaked in anonymity, routed through multiple jurisdictions, and employ false flag tactics. Under

[30] International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts*, 2001, art. 2.
[31] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 19-22 (Cambridge Univ. Press 2017).
[32] United Nations Open-Ended Working Group (OEWG), *Final Report on the Developments in the Field of Information and Telecommunications in the Context of International Security*, 2021.

ARSIWA, attribution requires that the cyber operation is conducted by state organs or entities under the effective control of the state (Article 4 and 8). The Tallinn Manual 2.0, Rule 15, reflects this but acknowledges the technical difficulties in proving such control.[33] India's legal framework under the Information Technology Act, 2000, particularly Section 66F on cyber terrorism, criminalizes attacks that threaten national security. Yet, attributing such attacks to state actors remains diplomatically and technically challenging.

India's engagement in multilateral platforms reinforces its stance on state responsibility. India has pushed for the development of global norms that respect state sovereignty in cyberspace. In doing so, it aligns with the UN Charter, which under Article 2(4) prohibits the threat or use of force against the territorial integrity or political independence of states. Cyber operations that cause physical damage or loss of life may qualify as use of force. However, non-destructive operations like espionage or economic disruption often fall in a grey zone.

The Budapest Convention on Cybercrime, 2001, though not signed by India, influences global legal standards. India's reluctance stems from sovereignty concerns, particularly the potential for foreign law enforcement to access Indian data without local oversight. Nevertheless, India engages bilaterally and regionally on cybercrime issues, advocating for cooperation frameworks that respect sovereign jurisdictions.

The Digital Personal Data Protection Act, 2023 (DPDP Act) embodies India's domestic obligations to protect individuals' data, asserting responsibility over personal data governance. Section 3(b) applies extraterritorially, ensuring that data related to Indian citizens, even if processed outside India, falls under Indian jurisdiction.[34] This reflects India's commitment to uphold digital sovereignty and fulfill its obligations to its citizens in cyberspace.

[33] Tallinn Manual 2.0, Rule 15.
[34] Digital Personal Data Protection Act, 2023, § 3(b), No. 22, Acts of Parliament, 2023 (India).

India's military doctrine also integrates cyber responsibilities. The Integrated Defence Staff's Cyber Doctrine, 2019, articulates offensive and defensive cyber capabilities. It recognizes the state's responsibility to defend its cyberspace while respecting international law. The doctrine aligns with the National Cyber Security Policy, 2013, which envisions a secure cyberspace to safeguard national interests. This dual framework ensures that India fulfills its duty of care, a core aspect of state responsibility.

The CERT-In Directions, 2022, impose mandatory breach reporting, enhancing state oversight over cybersecurity incidents. By mandating rapid incident disclosures, the government ensures that private entities contribute to national cyber defense. This reflects the multi-stakeholder approach endorsed by India, wherein state responsibility in cyberspace is shared with private sector actors.

The judiciary plays a role in shaping state responsibility. In *K.S. Puttaswamy v. Union of India*, the Supreme Court recognized privacy as a fundamental right, obligating the state to protect individuals' data against both state and non-state actors.[35] This constitutional mandate intersects with international obligations, reinforcing the state's duty to secure cyberspace as a realm of individual rights.

India's use of blocking powers under Section 69A of the IT Act further underscores state responsibility. By banning apps and platforms that threaten national security, India exercises its sovereign right to regulate cyberspace. The state bears responsibility for ensuring that such regulatory actions comply with constitutional guarantees and international norms.

In *Anuradha Bhasin v. Union of India*, the Supreme Court affirmed the state's responsibility to justify internet shutdowns under constitutional scrutiny. The Court held that freedom of speech under Article 19(1)(a) includes the right to access the internet, though it may be

[35] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

restricted in the interest of national security or public order.[36] This ruling ensures that the state remains accountable for its actions in cyberspace.

India advocates for capacity-building as an integral part of state responsibility. In its submissions to international forums, India emphasizes that developing countries require technical and financial support to fulfill their cyber obligations. Without adequate capabilities, expecting uniform compliance across nations becomes inequitable. The OEWG Final Report, 2021, reflects this. It acknowledges the differing capacities of states and calls for assistance mechanisms. India's participation in global cybersecurity exercises and training programs, such as those under the Global Forum on Cyber Expertise (GFCE), reinforces its commitment to responsible state behavior.

India's public-private partnerships in cybersecurity also demonstrate the evolving nature of state responsibility. The Data Security Council of India (DSCI), established by NASSCOM, collaborates with government agencies, ensuring industry participation in national cyber defense. This shared responsibility model aligns with India's multi-stakeholder governance approach. The Telecom Regulatory Authority of India (TRAI) imposes cybersecurity obligations on telecom providers, ensuring the security of national digital infrastructure. The National Security Directive on Telecommunication Sector, 2021, mandates sourcing telecom equipment from trusted vendors, reflecting sovereign responsibility over supply chain security.

India's International Cybersecurity Cooperation Agreements with countries like the United States, Japan, and Israel further manifest state responsibility. These agreements promote information sharing, joint incident response, and capacity-building, ensuring that India remains aligned with global norms while safeguarding national interests.

[36] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

VII. CASE ANALYSIS: LANDMARK LEGAL DEVELOPMENTS

K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, stands as the cornerstone of privacy jurisprudence in India. The nine-judge bench unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution. This ruling transformed India's approach to data protection and digital rights. The Court connected privacy with dignity, autonomy, and liberty. It recognized informational privacy as part of this right. The judgment compelled the state to draft comprehensive data protection legislation. It also positioned India within the global discourse on digital sovereignty by emphasizing the role of the state in safeguarding citizens' data.[37]

Shreya Singhal v. Union of India, reshaped the contours of online speech regulation in India. The Supreme Court struck down Section 66A of the Information Technology Act, 2000. This provision criminalized the sending of offensive messages through communication devices. The Court ruled that Section 66A violated the right to freedom of speech under Article 19(1)(a) and failed the test of reasonable restrictions under Article 19(2). However, the Court upheld Section 69A and intermediary liability under Section 79 of the IT Act. This balance reflected the Court's acknowledgment of state responsibility in cyberspace. It protected free speech but allowed the state regulatory oversight over digital platforms, reinforcing India's digital sovereignty.[38]

Anuradha Bhasin v. Union of India, examined internet shutdowns in the context of constitutional freedoms. The Court held that freedom of speech under Article 19(1)(a) includes the right to access the internet. Restrictions on this right must meet the standards of legality, necessity, and proportionality under Article 19(2). The Court ruled that indefinite internet shutdowns are impermissible. However, it allowed reasonable restrictions on internet access in the interest of national security and public order. This

[37] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[38] *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*

judgment clarified the extent of state power over digital infrastructure, making the state accountable in cyberspace governance.[39]

In *PUCL v. Union of India,* the Supreme Court dealt with telephone tapping, laying down procedural safeguards. Although the case predated the digital age, its principles extend to electronic surveillance under Section 69 of the IT Act. The Court emphasized that surveillance must be authorized, necessary, and proportionate. These safeguards inform the state's exercise of surveillance powers in cyberspace, balancing security needs with constitutional rights.[40]

Justice K.S. Puttaswamy (Retd.) v. Union of India,commonly known as the Aadhaar judgment, further refined data protection principles. The Court upheld the constitutional validity of the Aadhaar scheme but limited its mandatory use to welfare schemes and tax filings. It struck down provisions allowing private entities to demand Aadhaar details, recognizing the risk to privacy. This judgment reaffirmed the state's duty to regulate digital identification systems while protecting individual rights. It emphasized data minimization and purpose limitation, reinforcing state responsibility over digital ecosystems.[41]

In Facebook Inc. v. Union of India, the Supreme Court deliberated on the issue of data sharing between global digital platforms and Indian law enforcement. The case arose from concerns about traceability of originators of messages on encrypted platforms like WhatsApp. The Court underscored that foreign entities operating in India must comply with Indian laws. It highlighted the tension between encryption, privacy, and law enforcement needs. This case demonstrates how state responsibility in cyberspace intersects with transnational digital services, affirming the sovereign authority of Indian laws over global platforms.[42]

[39] *Anuradha Bhasin v. Union of India.*
[40] *PUCL v. Union of India.*
[41] *Justice K.S. Puttaswamy (Retd.) v. Union of India.*
[42] *Facebook Inc. v. Union of India.*

The Google India Private Ltd. v. Visaka Industries Ltd., case addressed intermediary liability under Section 79 of the IT Act. The Supreme Court held that intermediaries enjoy safe harbor protection but must act upon receiving actual knowledge of unlawful content. This case underscored the state's role in regulating digital platforms and ensuring that intermediaries do not become conduits for illegal activities. It also reinforced the due diligence obligations of intermediaries, supporting India's digital regulatory framework.[43]

In *Avnish Bajaj v. State (NCT of Delhi),* the Delhi High Court addressed the liability of the CEO of Baazee.com (later eBay India) in a cyber pornography case. The Court held that intermediaries are not automatically liable for user-generated content but must act upon knowledge of illegality. This case laid the groundwork for intermediary liability jurisprudence in India, influencing later amendments to the IT Act and rules governing digital platforms.[44]

Sabu Mathew George v. Union of India, concerned the regulation of online content under the Pre-Conception and Pre-Natal Diagnostic Techniques (PCPNDT) Act, 1994. The Supreme Court directed search engines like Google, Yahoo, and Microsoft to prevent advertisements violating the PCPNDT Act. This case extended the state's regulatory reach into cyberspace, compelling global platforms to comply with Indian laws. It reinforced state responsibility to ensure that cyberspace remains aligned with national legal frameworks.[45]

VIII. CYBERSECURITY ARCHITECTURE AND COMPLIANCE

India's cybersecurity architecture operates through a multi-tiered institutional and regulatory framework. The Information Technology Act, 2000 (IT Act) serves as the foundational legislation, outlining offenses, penalties, and compliance mandates for securing cyberspace. Section 70B of the IT Act establishes the Indian Computer

[43] *Google India Private Ltd. v. Visaka Industries Ltd.*
[44] *Avnish Bajaj v. State (NCT of Delhi).*
[45] *Sabu Mathew George v. Union of India.*

Emergency Response Team (CERT-In) as the national nodal agency for cybersecurity incident response. CERT-In's Cybersecurity Directions, 2022, mandate mandatory breach reporting within six hours. This reporting obligation applies to service providers, intermediaries, data centers, and government organizations, ensuring real-time state intervention in cyber incidents.[46]

The National Critical Information Infrastructure Protection Centre (NCIIPC), formed under Section 70A of the IT Act, complements CERT-In by safeguarding critical sectors like power, telecom, and banking. The NCIIPC Guidelines for the Protection of Critical Information Infrastructure, 2022, prescribe sector-specific compliance measures. These include real-time monitoring, access controls, periodic audits, and adherence to global cybersecurity standards like ISO 27001 and NIST frameworks.[47] NCIIPC ensures that critical infrastructure entities remain resilient against sophisticated cyber threats, reinforcing India's sovereign control over its digital backbone.

The National Cyber Security Policy, 2013, articulates India's broader cybersecurity strategy. It emphasizes creating a secure computing environment, fostering public-private partnerships, and building indigenous cybersecurity capabilities. The policy calls for establishing a National Cyber Coordination Centre (NCCC), which operationalizes cyber threat intelligence sharing among government agencies, defense establishments, and critical sectors. The draft National Cyber Security Strategy, awaiting finalization, proposes enhanced measures including offensive cyber capabilities, legal frameworks for cybersecurity governance, and capacity-building initiatives.[48]

The Digital Personal Data Protection Act, 2023 (DPDP Act) introduces compliance obligations for data fiduciaries. Section 10 mandates the designation of Significant Data Fiduciaries (SDFs) based on the volume and sensitivity of data processed. SDFs must

[46] Indian Computer Emergency Response Team (CERT-In), *Cybersecurity Directions*, April 2022.
[47] National Critical Information Infrastructure Protection Centre (NCIIPC), *Guidelines for the Protection of Critical Information Infrastructure*, 2022.
[48] Ministry of Electronics and Information Technology, *National Cyber Security Policy*, 2013.

appoint Data Protection Officers, conduct Data Protection Impact Assessments (DPIAs), and undergo periodic audits. Section 33 of the Act imposes penalties up to ₹250 crore for non-compliance, ensuring robust enforcement.[49] The Data Protection Board of India, established under Section 18, adjudicates data breach disputes and enforces compliance.

The CERT-In Cybersecurity Directions, 2022, also impose compliance obligations on global service providers offering services in India. These include maintaining logs for 180 days, mandatory breach reporting, and cooperation with law enforcement. The Directions extend India's jurisdiction over offshore entities, ensuring that the global digital ecosystem respects India's regulatory mandates.[50]

India's Telecom Regulatory Authority (TRAI) regulates cybersecurity compliance in the telecom sector. The National Security Directive on Telecommunication Sector, 2021, mandates telecom providers to source equipment from trusted vendors. The directive ensures supply chain security, preventing potential foreign surveillance or sabotage. TRAI also enforces network security obligations, including periodic audits and threat assessments.

The Defence Cyber Agency, formed in 2019 under the Integrated Defence Staff, operationalizes India's military cyber capabilities. It coordinates offensive and defensive cyber operations, ensuring that India's defense infrastructure remains secure against state-sponsored cyber threats. The Ministry of Defence Guidelines for Cybersecurity in Defence Sector, 2019, prescribe additional security measures, including air-gapped networks, encryption, and red-teaming exercises. The Data Security Council of India (DSCI), established by NASSCOM, plays a pivotal role in promoting cybersecurity best practices across the private sector. DSCI conducts capacity-building, certification programs, and industry-specific cybersecurity initiatives, complementing government efforts.

[49] Digital Personal Data Protection Act, 2023, §§ 10, 18, 33, No. 22, Acts of Parliament, 2023 (India).
[50] CERT-In Cybersecurity Directions, 2022.

Compliance frameworks extend to the financial sector. The Reserve Bank of India (RBI) mandates cybersecurity frameworks for banks and payment systems. The RBI's Cybersecurity Framework for Banks, 2016, requires banks to implement robust IT governance, incident response mechanisms, and periodic risk assessments. The Storage of Payment System Data Circular, 2018, enforces data localization for payment data, ensuring sovereign control over financial data.[51] The Securities and Exchange Board of India (SEBI) enforces cybersecurity obligations on stock exchanges, clearing corporations, and depositories. The SEBI Cybersecurity Framework for Market Infrastructure Institutions, 2015, mandates cybersecurity audits, incident reporting, and disaster recovery mechanisms. SEBI ensures that the financial market infrastructure remains resilient against cyberattacks, preserving market integrity.

The Insurance Regulatory and Development Authority of India (IRDAI) imposes cybersecurity requirements on insurers. The IRDAI Guidelines on Information and Cyber Security, 2017, mandate information security governance, cyber incident reporting, and data protection measures. This multi-sectoral approach ensures comprehensive cybersecurity compliance across the economy.

India's judiciary reinforces compliance through landmark rulings. In K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, the Supreme Court recognized privacy as a fundamental right, compelling compliance frameworks to align with constitutional mandates.[52] In *Anuradha Bhasin v. Union of India,* the Court emphasized proportionality in internet shutdowns, ensuring state actions align with constitutional freedoms while maintaining cybersecurity.

The blocking powers under Section 69A of the IT Act allow the government to direct intermediaries to block unlawful content. This enforcement mechanism complements cybersecurity compliance, ensuring that digital platforms operate within legal bounds. India's participation in international cybersecurity initiatives enhances compliance

[51] Reserve Bank of India, *Storage of Payment System Data Circular*, 2018.
[52] *K.S. Puttaswamy v. Union of India.*

mechanisms. India collaborates with global entities like the Global Forum on Cyber Expertise (GFCE) and engages in bilateral cybersecurity agreements with the United States, Japan, and Israel. These collaborations promote information sharing, joint exercises, and harmonization of cybersecurity standards.

India's WTO stance on e-commerce and data flows reflects its emphasis on sovereign cybersecurity regulation. India opposes permanent moratoriums on customs duties for electronic transmissions, arguing for the need to retain policy space for cybersecurity and digital regulation. The Budapest Convention on Cybercrime, 2001, although not ratified by India, influences India's cybersecurity compliance landscape. India prefers a UN-led cybercrime framework that respects state sovereignty, ensuring that compliance mechanisms align with national interests.

IX. CONCLUSION

India's digital sovereignty intertwines constitutional guarantees with national security imperatives. The Information Technology Act, 2000, anchors India's legislative control over cyberspace. Sections 69, 69A, 70, and 70B empower the government to regulate, intercept, block, and secure digital ecosystems. These provisions ensure that India retains control over its cyberspace, safeguarding sovereignty while balancing individual rights.[53] The architecture reflects sovereign autonomy but raises compliance demands across sectors.

Judicial pronouncements shape this sovereignty. The Supreme Court in *K.S. Puttaswamy v. Union of India,* recognized privacy as a fundamental right. This decision redefined the balance between state regulation and individual freedoms. Sovereignty could no longer be asserted without constitutional justification. The Court mandated that state actions in cyberspace must respect privacy, proportionality, and due process. Digital governance became constitutionally bound.[54]

[53] Information Technology Act, 2000, §§ 69, 69A, 70, 70B, No. 21, Acts of Parliament, 2000 (India).
[54] *K.S. Puttaswamy v. Union of India.*

India's cybersecurity framework, led by CERT-In, NCIIPC, and sectoral regulators like TRAI, RBI, and SEBI, establishes compliance norms. The Cybersecurity Directions, 2022, require mandatory breach reporting and security audits, reinforcing state oversight.[55] The National Cyber Security Policy, 2013, further integrates resilience and capacity-building. Compliance ensures that private entities align with national security goals, supporting sovereign digital infrastructure.

The Digital Personal Data Protection Act, 2023, introduces data sovereignty by imposing extraterritorial jurisdiction under Section 3(b). It applies to global entities processing Indian citizens' data. This provision ensures sovereign control over personal data, reflecting global norms like the GDPR. Section 33 prescribes penalties up to ₹250 crore for non-compliance. The Data Protection Board of India, created under Section 18, ensures enforcement. This framework empowers the state to govern data ecosystems while protecting citizen rights.[56]

Judicial oversight continues to reinforce compliance. *Shreya Singhal v. Union of India,* struck down Section 66A of the IT Act but upheld intermediary liability under Section 79. The Court balanced free speech with sovereign regulation over digital platforms. This equilibrium remains central to India's digital sovereignty.[57]

In *Anuradha Bhasin v. Union of India,* the Court asserted that access to the internet forms part of the right to freedom of speech under Article 19(1)(a). Yet, it allowed reasonable restrictions under Article 19(2) for national security. The state's regulatory actions, like internet shutdowns, must meet legality, necessity, and proportionality tests. Sovereignty thus remains subject to judicial review.[58]

International law shapes India's sovereign posture. The United Nations Group of Governmental Experts (UNGGE) and Open-Ended Working Group (OEWG) emphasize

[55] Indian Computer Emergency Response Team (CERT-In), *Cybersecurity Directions*, April 2022.
[56] Digital Personal Data Protection Act, 2023, §§ 3(b), 18, 33, No. 22, Acts of Parliament, 2023 (India).
[57] *Shreya Singhal v. Union of India*.
[58] *Anuradha Bhasin v. Union of India.*

state responsibility in cyberspace. India supports due diligence obligations but calls for capacity-building for developing nations. Attribution remains a challenge due to the anonymity of cyber operations. Tallinn Manual 2.0 articulates these complexities. India aligns its cyber strategies with these frameworks, emphasizing sovereignty and non-interference.[59]

India's resistance to the Budapest Convention on Cybercrime, 2001, reflects its sovereign stance. India prefers a UN-led cybercrime treaty to avoid potential foreign interference in domestic cyber matters. This ensures that India retains jurisdiction over its digital space. Sovereignty remains central to India's global negotiations on digital governance.

India's blocking powers under Section 69A of the IT Act reinforce sovereignty. The government's ban on apps like TikTok exemplifies this. The state exercises territorial enforcement to assert national security priorities. Compliance mechanisms ensure that foreign digital platforms adhere to Indian laws. Public-private partnerships enhance India's cybersecurity compliance. The Data Security Council of India (DSCI) collaborates with government agencies, strengthening threat intelligence sharing and compliance audits. This model reinforces India's multi-stakeholder governance.

India's trade policy aligns with digital sovereignty. At the WTO, India resists permanent moratoriums on customs duties for electronic transmissions, retaining policy space for data governance. Sovereignty extends to economic domains, allowing regulation of cross-border data flows.

India's cyber military capabilities underscore defensive and offensive strategies. The Defence Cyber Agency, under the Integrated Defence Staff, operationalizes cyber defense. The Ministry of Defence Guidelines for Cybersecurity in Defence Sector, 2019, mandate security protocols for military networks. This ensures that cyber defense remains integral to national security. Telecom infrastructure remains a critical aspect of

[59] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 19-22 (Cambridge Univ. Press 2017).

sovereignty. The National Security Directive on Telecommunication Sector, 2021, mandates sourcing from trusted vendors. The TRAI enforces security standards across telecom networks. Supply chain security ensures sovereign control over digital communication channels.

X. REFERENCES

1. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
2. *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
3. Indian Computer Emergency Response Team (CERT-In), *Cybersecurity Directions*, April 2022.
4. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
5. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
6. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
7. Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).
8. Ministry of Electronics and Information Technology, *National Cyber Security Policy*, 2013 (India).
9. National Critical Information Infrastructure Protection Centre (NCIIPC), *Guidelines for the Protection of Critical Information Infrastructure*, 2022.
10. Reserve Bank of India, *Storage of Payment System Data Circular*, 2018.
11. US-India Cyber Framework Agreement, 2016.
12. United Nations Open-Ended Working Group (OEWG), *Final Report on the Developments in the Field of Information and Telecommunications in the Context of International Security*, 2021.
13. Defence Cyber Agency, *Cyber Doctrine*, Integrated Defence Staff, 2019 (India).

14. Telecom Regulatory Authority of India (TRAI), *National Security Directive on Telecommunication Sector*, 2021.

15. United Nations General Assembly, *Charter of the United Nations*, 24 October 1945.