INDIA'S CYBERSECURITY ARCHITECTURE UNDER THE LENS: LEGAL ADEQUACY, INSTITUTIONAL GAPS, AND REFORM IMPERATIVES

Adarsh Vaibhav, BBA LLB, National University of Study and Research in Law, Ranchi

ABSTRACT

The process of digital transformation in India has been so immense that it has transformed the sphere of governance, business, as well as the provision of national services, and now with almost 850 million internet users, cybersecurity has become an essential pillar of national security, economic stability, and constitutional governance. The spread of digital infrastructure, such as e-governance systems, e-payment systems, and critical information networks, has also increased vulnerability to multipolar cyber threats, such as ransomware attacks, data breaches, state-sponsored efforts, and disruption of critical infrastructure.

The Indian cybersecurity environment is only mainly based on the Information Technology Act, 2000 (IT Act) amended in 2008, and with the Digital Personal Data Protection Act, 2023 (DPDP Act), alongside sector-specific subsidiary legislation. The Indian Computer Emergency Response Team (CERT -In), National Critical Information Infrastructure Protection Centre (NCIIPC), and Indian Cybercrime Coordination Centre (I4C) have been established, as institutional mechanisms that can facilitate the response of an incident and secure critical infrastructure. However, there are still certain issues of institutional fragmentation, limited enforcement capacity, jurisdictional ambiguities, and lack of number of sector-specific standards.

This framework falls under constitutional requirements of protection of fundamental rights under Articles 14,19, and 21. Rulings of the court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, *Shreya Singhal v. Union of India* have emphatically underscored the necessity to balance national security with privacy, expression, and proportionality.

By conducting a thorough review of historical changes in the legislation, institutional ecosystems, landmark court cases, and high-profile incidents, including AIIMS ransomware attack, CoWIN breach claims, and Aadhaar vulnerabilities, this paper critically analyses the Indian readiness on cybersecurity. It pinpoints flaws in systems of enforcement, coordination, and foreign collaboration and reveals an urgent need of overall omnibus laws, unified command system, capacity-building measures, and enhanced

cooperation between the citizens and business organizations.

This paper hypothesizes that cybersecurity needs to be radically reimagined as a multidimensional governance problem at the nexus of law, technology, national security, and human rights - as a strategically indispensable necessity to India becoming a leading digital powerhouse in the world.

Keywords: Cybersecurity governance, Information Technology Act, Digital transformation, Data protection, Constitutional rights, Institutional reform, Cyber resilience, Critical infrastructure protection.

Objective and Scope of the Study

This paper critically analyses the cybersecurity system in India in terms of the legal sufficiency, institutional performance and governance issues. Its ultimate goal is to examine whether the current legal framework in India, i.e. the Information Technology Act, 2000 (amended 2008), sector-specific laws and the constitution is sufficient to deal with the modern cyber threats.[1] The areas targeted include a review of the institutional capabilities and solutions, such as the Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), and law-enforcement agencies, and locating systemic weaknesses that hinder successful cybersecurity governance. [2]

This study also examines the constitutional foundations of the digital rights specifically the interplay between the needs of national security and the basic rights guaranteed by Articles 14, 19 and 21 of the Constitution.[3] This article suggests reform imperatives needed to enhance cyber resilience in India through the analysis of landmark cases, and actual-world cyber incidences, which are expected to transform the economy to US trillion by 2028, which is highly digitalised.[4]

Introduction

The process of digital transformation in India takes place at a scale and pace that, to many people, seems to be unprecedented. The country has over 850 million internet users[5] and a fast-

[1] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2008 (India).
[2] National Critical Information Infrastructure Protection Centre Gazette Notification (Jan. 16, 2014).
[3] India Const. art. 14, 19, 21.
[4] Ministry of Electronics & Info. Tech., India's Trillion-Dollar Digital Opportunity (2023), *https://www.meity.gov.in*
[5] Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators Report (Oct.-Dec. 2023).

growing digital economy that has seen an exponential growth in the number of digital transactions, e-governments as well as the adoption of technologies in the various sectors. However, it is this same acceleration, which has been increasing the attack surface of cyber adversaries by a relative margin, which includes state-sponsored activities, ransomware attacks, data breaches, and critical-infrastructure attacks.[6]

The cybersecurity situation in India has three overlapping problems. To begin with, the existing legal system, which is mainly grounded in the Information Technology Act of 2000, has not yet adapted to the new threats of artificial-intelligence-based attacks, deepfakes, vulnerabilities to quantum-computing, and supply-chain attacks. Second, there is institutional diffusion between various agencies; such as, CERT-In, NCIIPC, the National Cyber Security Coordinator, the Defence Cyber Agency, and a myriad of state police cyber-crime cells, which introduce gaps in coordination and jurisdiction. Third, the absence of detailed data-protection laws until recently has created great gaps in both privacy protection and data regulation across borders.

These vulnerabilities have been highlighted by recent incidents. The health-related services of the All-India Institute of Medical Sciences (AIIMS) were interrupted in November 2022 by ransomware that revealed the vulnerability of critical infrastructure.[7] The COVID-19 vaccination database hack revealed sensitive information of millions of people posing significant questions regarding the quality of cybersecurity measures by the government. The advanced persistent threats on power grids, defence facilities, and research facilities that are sponsored by states also shed some light on the strategic levels of cyber warfare that India needs to address.

It is urgent on this basis that India embarks on a massive legal reforming process, institutional restructuring and greater public-private partnerships, to develop a cyber resilience profile that matches its digital aspirations and geopolitical importance.

Evolution of India's Cybersecurity Framework

Legislative Genesis: The Information Technology Act, 2000

The commencement of the process of establishing cybersecurity governance in India started

[6] National Cyber Security Coordinator, Annual Cybersecurity Threat Assessment Report 2023 (2023).
[7] Press Trust of India, AIIMS Server Down for Nearly 3 Weeks After Cyber Attack, The Hindu (Nov. 23, 2022).

with the enactment of the Information Technology Act of 2000, which sought to provide legal protection to the electronic transactions and the computer-related crime.[8] India had in the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, responded with the Act. Nonetheless, its earlier form was mostly transactional and concerned itself with digital signatures, electronic records and simple cybercrimes as provided in Section 43 and 66.

The 2000 Act presented essential clauses such as the section 43 (damage to computer systems) and Section 66 (computer related offences), Section 67 (publishing obscene information) and Section 70 (protected systems). It, nevertheless, did not include specifications on data protection, privacy rights, and organizational accountability as part of cybersecurity practices.[9]

The 2008 Amendment: Expanding Scope and Penalties

The IT (Amendment) Act of 2008 was an important development, which included a number of major provisions. Section 66A made illegal communication service messages that disseminated offensive content--a point that the Supreme Court some years later invalidated in Shreya Singhal v. Union of India (2015) on the ground of breaching Article 19(1)(a).[10] Section 66B dealt with the dishonest acceptance of stolen computer resources, Section 66C, 66D and 66E dealt with identity theft, personation by fraud and breach of privacy, respectively. Section 66F brought in the provisions of cyber-terrorism that comes with harsh penalties. Section 43A was also an addition to the amendment, making corporations liable in the protection of data as well as making body corporates to practice reasonable security measures. Section 72A made it a crime to reveal the information that has been gained in violation of the valid contract. All these provisions were a paradigm shift in terms of organizational responsibility in cybersecurity.

Institutional Architecture Development

CERT-In (2004): The Indian Computer Emergency Response Team, which was constituted as per the 70B of the IT Act, is the central node in responding to cybersecurity attacks. CERT-In also issues advisories, conducts security audits as well as emergency responses. Its

[8] U.N. Comm'n on Int'l Trade Law, UNCITRAL Model Law on Electronic Commerce (1996).
[9] Pavan Duggal, Cyber Law in India: Law on Internet 45-62 (2016).
[10] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

efficiency is, however, limited by less powers of enforcement and lack of resources.

NCIIPC (2014): Established under Section 70A, the National Critical Information Infrastructure Protection Centre provides security of critical information infrastructure within power, telecommunications, transport, banking and defence sectors. Although mandated to do so, NCIIPC currently experiences a problem with thorough coverage of the sector and the incorporation of real-time threat intelligence.[11]

National Cyber Security Policy (2013): This policy document captured the vision of India to develop a secure and resilient cyberspace to the citizens, businesses and government.[12] Some of the goals that it identified included developing a confident cybersecurity ecosystem, reinforcing regulatory frameworks, and improving cybersecurity awareness. However, the application has been disjointed.[13]

Cybercrime Coordination Centre (I4C, 2020): I4C is the coordination and cooperation among the law enforcement agencies in the fight against cybercrime and offers forensic assistance to the organizations involved in combating cybercrime and manages the National Cybercrime Reporting Portal.[14]

Regulatory Evolution: The Information Technology Rules

A number of rules have been added into the IT Act to deal with certain issues:

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: The concept of sensitive personal data is defined and security practices that are required by body corporations working with sensitive data.[15]

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Enforced due diligence of social media platforms, major social media intermediaries, and digital news publishers, such as content moderation, traceability of information source, and

[11] Latha Jishnu, Critical Infrastructure: Time to Worry About Cybersecurity, Bus. Standard (Nov. 2, 2020).
[12] Ministry of Electronics & Info. Tech., National Cyber Security Policy 2013 (July 2, 2013).
[13] Venkatesh Nayak, National Cyber Security Policy: *Ambition Without Resources?* Commonwealth Human Rights Initiative (2014).
[14] Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C) Scheme (2018).
[15] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).

redressal mechanisms of grievances.[16]

Information Technology (Directions for Information Security Practices) Rules, 2022: The service providers, intermediaries, data centres, and VPN providers of mandated parties are required to report cybersecurity incidents to CERT -In within 6 hours and keep logs of the same within 180 days.[17]

Digital Personal Data Protection Act, 2023

India introduced the Digital Personal Data Protection Act of 2023 that creates the detailed framework of the personal data processing. The Act presents the principles of consent-based processing of data, limitation of its purpose, minimisation of data, and individual rights, such as the right to access, correction and erasure. It forms the Data Protection Board of India to be the regulatory authority. Nevertheless, general exemptions of government agencies have left the question of the possibility of excessive surveillance.[18]

Rights and Responsibilities: Constitutional and Legal Framework

Constitutional Foundations

Article 21 - Right to Privacy: The famous case in Justice K.S. Puttaswamy (Retd.). v. Union of India (2017) confirmed that privacy is an inherent right in Article 21.[19] The nine-judges court ruled that confidentiality also includes informational confidentiality, thus requiring that personal information should not be violated by any unauthorized intruder. This declaration by the constitution compels cybersecurity to tune the security imperatives in a manner that they are consistent with the sanctity of the privacy rights.[20]

Article 19(1)(a) - Freedom of Speech and Expression: In Shreya Singhal v. In Union of India 2015, the Supreme Court overturned Section 66A of the IT Act, which barred offensive messages, as it had been determined that, because of its ambiguity, it was unconstitutional, and as it had the effect of fostering a culture of intimidating speech.[21] The ruling highlights that

[16] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[17] Information Technology (Directions for Information Security Practices and Procedures and Cyber Incident Response) Rules, 2022 (India).
[18] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[19] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[20] Gautam Bhatia, The Transformative Constitution: A Radical Biography in Nine Acts 289-312 (2019).
[21] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

legislation on cybersecurity may not place excessive restrictions on people that infringe upon the right to communicate.

Article 14 - Equality Before Law: Cybersecurity laws need to be applied in a consistent and arbitrary freeway.[22] In Anuradha Bhasin v. The Court in Union of India (2020) stated that the internet access is part of Article 19(1)(a);[23] therefore, any ban, e.g., an internet one, should meet the proportionality requirements and be confined to the minimum necessary to achieve an alleged purpose.

Article 21A - Right to Education: The digital gap that is pervasive in the area of cybersecurity awareness and access to safe digital platforms involves educational rights.[24] In this age of online education, these differences bring plight to access to secure digital learning standards.

Organizational Responsibility

Section 43A Liability: Any corporate organ responsible for the custody, processing, or handling of sensitive personal information is required to put in place reasonable security practices.[25] Wrongful loss or gain which leads to failure causes the body corporate to become liable to compensations. Information security praxis rules, 2011, promote the standards set by IS/ISO/IEC 27001 as these reasonable practices.

Section 70 Protected Systems: The government can identify specific computer resources as secure systems.[26] Access to such systems though unauthorized makes the perpetrator subject to up to ten years imprisonment a provision that is meant to protect critical infrastructure of the country.

Section 84A Disclosure Obligations: The middlemen will be obligated to store information within a given time and release the details to the government agencies to aid investigations, prevention, or cybersecurity, thus creating conflicts between safeguarding data and granting law-enforcement agencies access.[27]

[22] India Const. art. 14.
[23] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[24] India Const. art. 21A.
[25] Information Technology Act, 2000, 43A, No. 21 of 2000, INDIA CODE (2000).
[26] Information Technology Act, 2000, 70, No. 21 of 2000, INDIA CODE (2000).
[27] Information Technology Act, 2000, 84A, No. 21 of 2000, INDIA CODE (2000) (as amended by Information Technology (Amendment) Act, 2008).

Individual Rights and Corporate Accountability

The Digital personal data protection act, 2023, presents the clear rights of data principals, such as the right to access, data rectification, data erasure, and data rights appointment.[28] Data fiduciaries have a duty to act by the law, have limited purpose, minimize data, reasonableness security protection, and report breaches.

Section 17 of the Act gives exemption to government agencies regarding some of the obligations in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or incitement to any cognisable offence. This exception brings plausible arguments concerning the possibility of surveillance in the absence of proper protection.

Authorities and Restraints of Law Enforcement

Section 69 of the IT Act gives the government the ability to give directions of interception, surveillance, or decryption of information where there is a need to do so in the interests of sovereignty, security, order in the society, or investigation. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, provide procedures safeguards but critics state that they are inadequate.[29]

Section 69B gives more powers to monitor and gather traffic information or other data by authorities towards cybersecurity. Although these powers are essential in terms of threat detection, when the exercise is done without effective mechanisms of judicial control, there is a high chance of abuse.[30]

Case Studies: Lessons from Indian Cyber Incidents

Case Study 1: AIIMS Ransomware Attack (November 2022)

In November 2022, the All-India Institute of Medical Sciences, Delhi, was a victim of a ransomware attack that took down its digital infrastructure and left the school virtually

[28] Digital Personal Data Protection Act, 2023, 11-14, No. 22 of 2023, INDIA CODE (2023).
[29] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Ministry of Communications and Information Technology Notification (Oct. 27, 2009).
[30] *See* Chinmayi Arun, *On Privacy Standards for Intermediaries*, 3 INDIAN J.L. & TECH. 36 (2007).

inoperable in almost three weeks.[31] The data breach encrypted essential servers, affected patient services, stopped outpatient department appointments, and breached seven servers and about 1.3 terabytes of vulnerable data.

Legal and Institutional Failures: The case revealed glaring healthcare cybersecurity governance gaps. Even though AIIMS was considered important infrastructure, it did not have well-developed backup plans, all-encompassing incident-response guidelines, and regular cybersecurity audits.[32] Defensive strategies as part of the National Critical Information Infrastructure Protection Centre (NCIIPC) had not, in reality, been applied to the medical field. The slow recovery process was a pointer on the lack of an effective business continuity framework.

Lessons: The case highlights the necessity to establish strict cybersecurity requirements of critical infrastructure, to conduct regular security audits, to insist on the cyber insurance of public institutions, and to introduce the industry-specific CERT mechanisms to meet healthcare cybersecurity needs.

Case Study 2: CoWIN Data Breach Allegation (2021)

In April 2021, it was claimed that the CoWIN immunisation database was leaked to the dark web and claimed to have revealed personal and biometric data of over 150 million citizens such as names, mobile numbers, Aadhar credentials and vaccination status.[33]

Legal Implications: Although the government did not acknowledge any substantive violation, the incident led to the suspicion of the inefficiency of the data security protocols of the state-affiliated digital platforms. A lack of a codified data protection law then created no statutory obligation in breach notification; thus, allowing a lack of transparency and accountability.[34] The incident demonstrated the inadequacy of current security audit procedures in digital services by governments.

Lessons: This incident enhanced a case to require that public platforms are audited by the office of security; mandatory breach-notification requirements; mandatory third-party security

[31] *AIIMS Server Down: Ransomware Attack Suspected, Services Hit*, HINDUSTAN TIMES (Nov. 23, 2022).
[32] Ministry of Health & Family Welfare, Report on AIIMS Cybersecurity Incident (2023) (on file with author).
[33] *CoWIN Data of 15 Crore Indians Up for Sale on Dark Web, Claims Researcher*, INDIA TODAY (Apr. 29, 2021).
[34] Arindrajit Basu, *India's Data Breach Notification Vacuum*, 9 NUJS L. REV. 287 (2021).

audits, and encryption of sensitive data transmitted and at rest.[35]

Case Study 3: Domino's India Data Breach (2021)

In May 2021, a massive data breach of Domino Pizza India revealed the personal and payment data of about 18 million orders.[36] The offender posted an indexable catalogue in the dark web.

Legal Response: Section 43(A) of the Information Technology Act would have provided Domino with the potential blame of compensating victims of negligent security practices.[37] But this was not strictly followed and no major punitive measures were taken. The absence of a fully developed privacy law limited the actions of regulation and no obligatory disclosure of breach to customers was made.

Lessons: The episode depicts the loopholes in the enforcement of Section 43(A), the need to have specific laws on breach-notification, high fines on careless data management and the existence of mandatory insurance cover on cyber-management.

Case Study 4: Maharashtra State Electricity Distribution Company Cyber Attack (October 2020)

In October 2020, a cyber-attack was reportedly aimed at the power distribution network of Maharashtra, making load dispatch unavailable and causing a massive outage in Mumbai. Chinese state-sponsored actors were implicated in reports as well, which is a strong critical-infrastructure threat.

Strategic Implications: This attack revealed weaknesses in SCADA systems used to control power distribution, lack of threat intelligence on high-end persistent threat (APT) organizations, poor coordination between NCIIPC and utility operators, and none of the operational-technology security.

Lessons: The incident highlights the geopolitical aspect of cybersecurity, the need of sector-specific standards of critical infrastructure, the improvement in the exchange of threat-intelligence between governments and utilities, and the need of compulsory OT/ICS security

[35] Centre for Internet & Society, Towards Mandatory Data Breach Notifications in India (Policy Brief, 2021).
[36] *Domino's India Data Breach Exposes Details of 18 Crore Orders*, ECONOMIC TIMES (May 19, 2021).
[37] Information Technology Act, 2000, 43A, No. 21 of 2000, INDIA CODE (2000).

testing.

Case Study 5: Aadhaar Data Vulnerabilities (2017-2018)

In 2017 to 2018, there were several reports exposing that journalists were able to access the Aadhaar database at nominal fee to show that there were severe security vulnerabilities in the ecosystem, even though the database was safe.[38]

Legal Developments: Justice K.S. Puttaswamy v. the Supreme Court, 1987. The constitutional validity of Aadhaar in Union of India (the Aadhaar judgment, 2018) was upheld, but the non-constitutionality of Section 57 was proven, which limited the possibility of accessing biometric data to the private side, as well as the duration of data retention and the necessity to provide more effective protection of privacy.[39] In the judgment, it was noted that biometric enrolment inspired by states should adhere to the principles of proportionality.

Lessons: The Aadhaar case provided underlying principles in terms of the scope of state surveillance, the need to restrict access points to data, the need to have compulsory security audits of authentication systems, and the need to make technologic design based on privacy by default.[40]

Institutional Gaps and Challenges

Fragmented Institutional Architecture

The existing governance framework of Indian cyber security is typified by a high instance of institutional fragmentation, which has no integrated coordination frameworks.[41] Coordination gaps, long incident-response times and unnecessary resource allocation are all products of overlapping mandates and limited information-sharing protocols by CERT-In and NCIIPC, I4C, the National Cyber Security Coordinator, the Defence Cyber Agency, the National Security Council Secretariat, and state police cybercrime cells, which coordinate poorly.

[38] *Aadhaar Data Breach: Personal Details Available for Just Rs 500*, THE TRIBUNE (Jan. 4, 2018).
[39] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (India)
[40] Vrinda Bhandari & Renuka Sane, *Aadhaar and the Right to Privacy: The Supreme Court's Verdict*, 53 ECON. & POL. WKLY. 11 (2018).
[41] CERT-In, Annual Report 2021-22, at 12-15 (2022).

Incompetence of resources and capacity

Police departments have confidence issues with deep capacity limits in investigating cybercrimes. The majority of state police departments have no dedicated cybercrime unit, forensic infrastructure and sufficient number of trained personnel thus, the ratio between investigator and cybercrime is pathetically low.[42] Courts also lack the capacity to adjudicate complex cybercrimes and few judges have the technical know-how of analysing digital evidence and computer jurisprudence.[43]

Lack of Sector-Specific Standards

Although the Information Technology Act provides general statutory coverage, the specifics of cybersecurity standards are still underdeveloped in sectors.[44] The most critical, which include healthcare, education, transportation, and manufacturing, do not have forceful, specialized systems that consider their unique threat environments and operational demands.

Weak Private Sector Interaction.

The Indian cyber security policy does not fully leverage on the expertise and resources of the private sector.[45] Compared to the United States and the European Union where the predominant model of public-private alliances is anticipated, the current model practiced by India is mainly government-centric and the threat-intelligence sharing between industry stakeholders and the government is meager.[46]

Data Localization Debates

The debate around policy issues of data localisation which require the storage of data on Indian soil is the extreme of the conflict between data sovereignty, cyber security and economic efficiency.[47] Although localisation would increase access to law-enforcement, reduce foreign

[42] Bureau of Police Research & Development, Cybercrime Investigation: A Study of Capacity and Capabilities 34-38 (2022).
[43] Karnika Seth, *Judicial Capacity Building for Cyber Crimes in India*, 15 J. INT'L COM. L. & TECH. 177 (2020).
[44] Information Technology Act, 2000, No. 21 of 2000, INDIA CODE (2000).
[45] National Cyber Security Policy 2013, Ministry of Electronics and Information Technology (July 2, 2013).
[46] Elonnai Hickok & Aditya Singh Chawla, *Public-Private Partnerships in Cybersecurity: Lessons for India from Other Jurisdictions*, CTR. FOR INTERNET & SOC'Y (2020).
[47] Reserve Bank of India, Notification on Storage of Payment System Data (Apr. 6, 2018); Ministry of Electronics and Information Technology, Draft E-Commerce Policy 4.2 (2019).

surveillance,

it would also increase costs, reduce operational flexibility, and not always lead to improved security in cases where local storage systems are not sufficiently secured.[48]

Jurisdictional Challenges

Transnational aspects of cybercrimes create jurisdictional issues.[49] The lack of effective mutual legal assistance treaties with many jurisdictions makes it hard to conduct cross-border investigations in India, and the standardized international cooperation frameworks do not exist that can guide the cybercriminals abusing the jurisdiction gap.

Future Aspects and Reform Imperatives

Legislative Reforms

Comprehensive Cybersecurity Legislation: To address the existing piecemeal situation, which cuts across the Information Technology Act, the Indian Penal Code, and numerous industry-specific laws, India has to pass a unified Cybersecurity law.[50] Explicit definitions of cybercrimes, strict investigational procedures, mandatory reporting, and industry-specific security standards that are both enforceable and agile to the changing threat levels need to be instilled in such a statute.[51]

Critical Infrastructure Protection Act: A jurisdictionally different law is one that defines sectors of critical information infrastructure.[52] The proposed law would enforce security standards, codify incident reporting, and establish liability systems against the operators of the infrastructure. The major requirements would include regular security audit and penetration testing and effective business-continuity plans to enhance the resiliency of critical services.

Intensifying the enforcement of Data Protection: The Digital Personal Data Protection Act,

[48] Rishab Bailey & Smriti Parsheera, *Data Localization in India: Questioning the Means and Ends*, NAT'L INST. PUB. FIN. & POL'Y Working Paper No. 242 (2018). Rishab Bailey & Smriti Parsheera, *Data Localization in India: Questioning the Means and Ends*, NAT'L INST. PUB. FIN. & POL'Y Working Paper No. 242 (2018).
[49] Pavan Duggal, CYBERLAW: THE INDIAN PERSPECTIVE 345-67 (2016).
[50] Information Technology Act, 2000, No. 21 of 2000, INDIA CODE (2000); Indian Penal Code, 1860, 463-489, No. 45 of 1860, INDIA CODE (1860).
[51] Standing Committee on Information Technology, Report on Cyber Security and Data Privacy 15-22 (2023).
[52] Information Technology Act, 2000, 70, No. 21 of 2000, INDIA CODE (2000).

2023, requires effective mechanisms of implementation.[53] This incorporates sufficiently staffed and statutory authority of the Data Protection Board, formal enforcement mechanisms and schedules, substantial fines of non-compliance, and time limits that limit general government exemptions. Courts ought to be strengthened in order to ensure the protective purposes of the law are achieved without excessive watering down.[54]

Regulating Artificial Intelligence and Emerging Technologies: With the spread of AI-based cyber threats, India needs a regulatory framework to take care of the issue of algorithmic accountability, the dangers of adversarial machine learning, detection of deep-fakes, and the security of IoT devices and smart infrastructure.[55] Laws should therefore include accountability measures to AI systems and enforceable security regulations to the new technologies.

Institutional Restructuring

Unified Cybersecurity Command Structure: Forming a National Cybersecurity Authority, granted explicit hierarchy over all cybersecurity agencies, would simplify the coordination process, eradicate overlap, and make coordinated threat-response stance possible.[56] This power needs to unify the efforts of intelligence, coordination of incidents response, policy-making, and international interplay into a harmonious governance framework.

Sectoral CERT Mechanisms: National CERT In addition to the national CERT. In sectoral CERTs, such as healthcare, finance, energy, transportation, and education, would provide specific threat intelligence, incident-response capability, and security advice that is sensitive to sector-specific demands.[57]

Capacity Building Intensives: National Cybersecurity Training Institutes are to be instituted as a way of imparting specialized training to law enforcement, the judiciary, and government officials.[58] Schools and university programmes should include cybersecurity curricula, and certification careers in cybersecurity professionals should be institutionalised. Besides, the

[53] Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE (2023).
[54] Malavika Jayaram, *India's Data Protection Bill: Strong on Government Access, Weak on Corporate Accountability*, TECH POL'Y PRESS (Jan. 12, 2023).
[55] NITI Aayog, National Strategy for Artificial Intelligence #AIForAll 56-62 (2018).
[56] Lt. Gen. Rajesh Pant (Retd.), *India Needs a Unified Cyber Command*, INDIAN EXPRESS (Mar. 15, 2022).
[57] CERT-In, Guidelines for Sectoral CERTs 8-12 (2021).
[58] Ministry of Electronics and Information Technology, National Cyber Security Strategy 2020, at 23-26 (2020).

implementation of cybercrime laboratories in all states will enhance investigative power.[59]

Public-Private Partnerships: The institutionalisation of formal information-sharing relations between government and industry, joint threat-analysis centres, policy-formulation forums, and innovation hubs should be realised in order to mobilise the joint technical and resource capacities.[60]

Technological Imperatives:

Zero Trust Architecture: Governments and other critical infrastructure networks must move beyond perimeter-based security frameworks and move to zero-trust frameworks that presuppose compromise and implement ongoing verification of user identity, device integrity, and network access.[61]

Quantum -Resistant Cryptography: In the event of quantum-computing technology capability, India has to invest in research, development, and implementation of quantum-resistant cryptographic algorithms to protect sensitive data over the long term.[62]

AI-Powered Detection of Threats: The implementation of artificial intelligence and machine-learning systems to perform threat detection in real-time, behavioural analytics, and automatic incident response will significantly increase defensive posture against advanced adversarial behaviour.[63]

Blockchain to Critical Systems: Blockchain technology may also be used to strengthen the security of supply-chain, secure identity management and offer tamper-evident logging of critical infrastructure systems to enhance transparency and responsibility.[64]

International Cooperation:

Multilateral involvement: India must also engage actively in international cybersecurity meetings like UN Group of Governmental Experts on Information Security, the Budapest

[59] Bureau of Police Research & Development, *supra* note 42, at 67-71.
[60] Data Security Council of India, Framework for Public-Private Partnership in Cybersecurity (2021).
[61] NAT'L INST. STANDARDS & TECH., ZERO TRUST ARCHITECTURE, Special Publication 800-207 (2020).
[62] Ministry of Electronics and Information Technology, Quantum Computing Mission Roadmap 34-38 (2023).
[63] CERT-In, AI and ML in Cybersecurity: Implementation Guidelines 15-22 (2022).
[64] Ministry of Electronics and Information Technology, National Blockchain Strategy 45-51 (2021).

Convention on Cybercrime, strategic bilateral cyber dialogues, etc. to make sure that domestic policy is not in contradiction with the international norms and best practices.[65]

MLATs and Cross-Border Investigation Frameworks: To overcome the jurisdiction obstacles, it is necessary to expand mutual legal assistance treaties, accelerate cross-border data-access agreements in investigations and to become a member of international law-enforcement networks such as the cybercrime programmes of the INTERPOL.[66]

Capacity Building Support: India has an information-technology base that could be used to expand cybersecurity capacity-building support to developing countries not only to increase the regional cyber resilience but also to establish India as a leader in cyber-governance globally.[67]

Industry-Specific Reforms:

Financial Sector: The cybersecurity system by the Reserve Bank of India must require advanced threat-intelligence dissemination, mandatory coverage of financial institutions by cyber liability insurance, strict protocols and guidelines of vendor-risk management, and automatic fraud detection systems.[68]

Healthcare Sector: There is an urgency to protect the extremely sensitive healthcare information through Health Information Security and Privacy Regulations and HIPAA-like, which are equivalent in nature, and cybersecurity certification of healthcare IT systems and specific investments in cyber-security infrastructure of hospitals.[69]

Defence and Strategic Sectors: Mandatory indigenous air-gapped critical systems, quantum-key distribution of secure communications, mandatory indigenous hardware and software on sensitive applications, and frequent red-team exercises to test current defensive designs will be better tools in the defence water.[70]

---

[65] U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015).
[66] Convention on Cybercrime, opened for signature Nov. 23, 2001, E.T.S. No. 185 (entered into force July 1, 2004) [hereinafter Budapest Convention].
[67] Ministry of External Affairs, India's Cyber Diplomacy Framework 28-33 (2022).
[68] Reserve Bank of India, Master Direction on Cyber Security Framework (2016); Reserve Bank of India, Cyber Security Framework for Primary (Urban) Co-operative Banks (2021).
[69] Ministry of Health & Family Welfare, Draft Health Data Management Policy 5 (2022).
[70] Ministry of Defence, Defence Cyber Agency Strategic Roadmap 2023-28, at 45-52 (2023).

Legal Process Reforms:

Specialised Cyber Courts: The creation of special cyber courts with specially trained judges, where case-handling is governed by digital evidence management procedures, will simplify the adjudication process and cut down on case-backlogs.[71]

Streamlined Evidence Processes: A reform of the Indian Evidence Act to include digital evidence and codify the chain-of-custody procedures, as well as, to allow remote testifying by cybersecurity professionals will increase the admissibility of evidence and prosecutor effectiveness.[72]

Whistleblower Protection: A strong legislative protection of security researchers and employees to report risks to consumers or organisational incompetence will trigger responsible disclosure and create a culture of continuous improvement.[73]

Conclusion

India is currently at a decisive point in the history of its cyber defence. The fast-growing digital economy of the country, its strategic geopolitical location, and its initial democratic principles altogether demand a very strong and rights-abiding cybersecurity framework. The available legal and institutional framework, however, though mandated, is proving to be insufficient to tackle the advanced cyber threats of the modern times.

The legal framework, which is mainly based upon the Information Technology Act of 2000 needs a thorough rewrite to suit the new technologies, advanced threat groups, and security of critical infrastructure. The Digital Personal Data Protection Act, 2023, a recent legislative move, is a welcome development that should be carefully implemented to prevent abuse of surveillance, but at the same time, it serves the real interests of protecting data.

The problem of institutional fragmentation is still topical. This multi-agency presence (lacking well-defined coordination mechanisms) is a barrier to efficient response to threats and to optimal resource allocation. Defining an integrated cybersecurity command unit that has

[71] Law Commission of India, Report No. 302: Computer Related Offences and Cyber Courts 78-85 (2022).
[72] Indian Evidence Act, 1872, 65A-65B, No. 1 of 1872, INDIA CODE (1872); *see also* Arjun Pandit v. State of Maharashtra, (2009) 11 SCC 1 (India).
[73] Centre for Internet & Society, Protecting Security Researchers: A Legislative Framework for India (Policy Paper, 2021).

explicit hierarchical authority may significantly improve the Indian defensive posture.

The case studies that are under analysis such as AIIMS ransomware, alleged CoWIN breach, Domino data leak, ransomware against Maharashtra power grid, and vulnerabilities in Aadhaar are eye-opening to some of the vulnerabilities existing in the healthcare system, government websites, the commercial sphere, and critical infrastructure. Such cases highlight the need to have compulsory security policies, legally required breach notification, and increased sanctions on negligence; and industry-specific regulations.

Constitutionally, the conflict between the national security demands and the basic rights in compliance with Articles 14, 19, and 21 must be approached with care. The statements by the Supreme Court of in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, *Shreya Singhal v. Union of India* set clear boundaries: the tests of proportionality should be met by cybersecurity measures; privacy is a basic right that should not be withheld, and free speech should not be chilled by broad clauses.

India should incorporate a number of imperatives in its cybersecurity approach in the future. The legislative changes must bring together the scattered provisions into one wholesome piece of cybersecurity legislation with sectored standards. The restructuring in institutions is supposed to encourage integrated command, sector Computer Emergency Response Teams, and effective capacity-building. The investments into the zero-trust architecture, quantum-resistant cryptography, and threat detection based on artificial intelligence should be made. Cooperation among countries will increase cross-border laws and resilience on the region through international cooperation based on mutual legal assistance treaties, multilateral participation, and capacity-building support.

The way to go requires acknowledging that cybersecurity is not only a technical problem but a multidimensional issue of governance that cuts across the law, technology, economics, geopolitics, and human rights. The response that India has to give must therefore be equally multidimensional- integrating of powerful legal frameworks, powerful institutions, state of the art technology, global collaborations, and a war on terror commitment to constitutional values.

With India having a vision of having a 5 trillion economy and becoming a global digital powerhouse, cybersecurity cannot be treated as a side note; it has to form a pillar of digital governance. The reforms discussed in this paper are ambitious but not optional to achieve the

digital future of India, safeguard the right of its citizens, and make the country resilient to the changing cyber threats. The time of gradual change is long gone, and broadly speaking, a complete overhaul of the Indian cybersecurity system is now a strategic requirement.