International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(22s) 2026 pp. 362-376
https://doi.org/10.70917/ijcisim-2026-5436
Article

LEGAL GOVERNANCE OF CRITICAL INFORMATION INFRASTRUCTURE IN INDIA: A CRITICAL AND COMPARATIVE ANALYSIS

Puneet Sharma[1*], Divya arora[2]

[1]Phd Scholar, The North Cap University, Gurugram, Haryana-122017, Email id puneetsharma1812@gmail.com
[2]Phd Scholar, The North Cap University, Gurugram, Haryana-122017, Email id: divya_arora@yahoo.com

Abstract: In today's digital world, the Critical Information Infrastructure (CII) is the foundation for many essential services. CII also forms the backbone for national security, economic stability, and public welfare. The increasing dependence on digital technology and even faster-evolving cyber threats has made the protection of CII a matter of utmost importance. In India, the protection of CII is primarily recognized under the IT Act, 2000. Sections 70, 70A and 70B of the IT Act, 2000 provide the statutory basis of identification and protection of CII. In addition to these, the sector-specific guidelines and the Digital Personal Data Protection Act, 2023 (DPDP Act) also contribute to a broader cybersecurity framework. In an era of digitalization where dependence on technology is increasing, cyber threats have also become more sophisticated. This article aims to critically examine India's existing legal framework for the protection of CII. Starting with the primary law – the IT Act 2000, it then covers various institutional mechanisms, sector-based regulations, and the relevance of the DPDP Act 2023. A comparative analysis with the legal approach adopted by various international jurisdictions – USA and UK – for protection of CII is also made. The methodology adopted during the study is doctrinal, which is supplemented by comparative analysis. The major legal and institutional issues and challenges are being identified during this study, which are affecting the effective protection of CII in today's digital era. These include the absence of updated legal provisions, limited regulatory coordination, limited public-private cooperation, overlapping responsibilities, low incident reporting, etc. The article concludes by briefly suggesting the need for a more coherent, coordinated, and comprehensive legal framework for strengthening India's legal regime governing CII.
Keywords: Digital technology, Cyber threat, Cyber security framework, Critical Information Infrastructure, Digitalization

1. INTRODUCTION

A. Background and Significance

In the present digital era, most of the government services are being managed digitally through the use of ICT, and many of these services are vital for citizens and businesses. Even governments depend on these digital systems for their daily work of providing services and governance. Many critical services like energy, transport, telecommunications, health care, and even administration are now increasingly dependent on digital systems using technology, which is also gradually improved as innovations take place. To provide such services, the systems have interconnected information systems. Together, these systems are referred to as Critical Information Infrastructure (CII).

Overall, CII – Critical Information Infrastructure includes information and communication technology (ICT) systems, networks, assets, and services which, if disrupted or destroyed, may have an adverse effect on national security, economic stability, and public health and safety. For proper functioning in society, not only should such

infrastructure be developed, maintained, and improved for better services, it should also be ensured that it is protected from any destruction. Today, these systems are referred to as the backbone of modern societies.

One of the important features of CII is that it includes complex digital ecosystems which are made up of numerous interconnected systems, networks, databases and communication technologies. These systems interact with one another across geographical locations and sectors. Another important feature of CII is interdependence. The present-day modern infrastructure systems do not work in isolation. On the contrary, they work as a component of a larger interconnected network where several sectors rely on information and on each other for effective and efficient services.

Disruption or destruction of one of the sectors may have an adverse effect on other sectors due to this interdependence. For example, if a cyber-attack takes place on a financial organization, it may adversely affect the digital payment system and the banking system. This disruption or destruction of CII may have an adverse effect on the organization's functioning, government services and activities, supply chain systems, transport logistics, healthcare, etc.

Similarly, power generation, transmission and distribution are referred to as critical infrastructure, and any large-scale power outages can impact telecommunications, transport networks, and healthcare institutions. Hospitals depend on uninterrupted power for life support equipment and information systems, and they may be impacted.

A comprehensive and coordinated approach is therefore required for protecting CII. This needs to be done in such a way that risks across sectors are considered instead of depending on the issues exclusively of any particular individual system.

The following are the sectors typically classified as Critical Information Infrastructure in India:

1. Power and Energy - This category includes systems related to generating, transmitting, and distributing electricity, as well as infrastructure for oil and gas, nuclear energy systems, and grids for renewable energy sources.

2. Banking, Financial Services and Insurance - This includes banking systems, payment platforms, ATM (Automated Teller Machines), Insurance Management systems, and any infrastructure that supports financial markets.

3. Telecommunications - Includes all networks that are involved in communication, like the internet infrastructure, satellite communication systems, and mobile network technologies.

4. Transport - This consists of railway systems, air traffic control mechanisms, road transport networks, port facilities, highway systems, and logistics operations.

5. Government - This sector is made up of the digital platforms for governance, national databases like those for Aadhaar, Passport, and all the internal IT systems of the Government Agencies.

6. Strategic and Public Enterprises - There are several Public Enterprises involved in strategic work, like the ISRO, DRDO, defense communication networks, space-related systems, and other government-owned organizations with strategic importance.

B. Designation of CII and Protected Systems

Identification and classification of protected systems and Critical Information Infrastructure (CII) is one of the most important components of India’s cyber security framework. To determine which information systems are critical infrastructure, analysis of the contribution of networks, platforms and resources in facilitating the delivery of vital national services is necessary. Thus, it can be said that critical infrastructures are those that are essential for the operation of important sectors like power, energy, finance, telecommunication, transportation, and governance.

Section 70 of the IT Act 2000 provides legal authority for identifying the protected systems. The government, using this clause, can declare certain systems and resources as protected systems if disruption, destruction, or compromise of such systems has an adverse impact on national security, economic stability, or public safety. To decide

this, the government needs to carefully review and assess the operational significance and potential implications if the system fails or is subjected to a cyber-attack.

Once under this law a system is designated as a protected system, it becomes subject to increased security requirements. It can then be accessed only by authorized users. The organizations that are responsible for managing a protected system have to implement strong cybersecurity measures so that the system is protected from unauthorized attack or intrusion. These cybersecurity measures include stringent access controls, constant monitoring, risk management techniques, and technical protection to ensure that there is no unauthorized entry, cyber invasion, or system failure and that the critical services are not disrupted and run smoothly.

The National Critical Infrastructure Protection Centre is the nodal agency responsible for protection of the nation's CII. It plays a crucial and central role and works closely with sectoral regulators, government ministries and private sector operators, so as to determine which infrastructure is vital. It creates suitable security standards for the protection of such critical information infrastructures. It helps the operators of the infrastructure in making their digital systems more resilient through guidelines, recommendations and best practices.

It may be summarized that designation and protection of essential information infrastructure is vital for protecting the national interests in this increasingly digital and interlinked world. In this regard, India has taken considerable steps to strengthen the security of digital infrastructure. Enactment of statutory measures have been enacted to allow classification of protected systems and the establishment of specialized institutions with responsibility for cybersecurity oversight. But still, there is a need to ensure that, for the long-term resilience of CII, policies should be reviewed and improved. The regulatory mechanisms should be strengthened because the nature of digital infrastructure is that it is prone to evolving cyber threats and technological developments.

2. LEGAL AND REGULATORY FRAMEWORK RELATED TO CII PROTECTION IN INDIA

A. The Information Technology Act, 2000 (IT Act)

The Information Technology Act, 2000 (IT Act) is the primary legal structure implemented for regulating cybersecurity in India. It was primarily enacted to provide legal recognition to electronic transactions and electronic governance. With the growing dependence on digital technology, key amendments were made to the Act in order to address evolving cybercrimes and cybersecurity threats.

The country's critical information infrastructure is protected and cyber incidents are managed by sections 70, 70A and 70B of the IT Act, 2000. These sections define the protected systems, describe the legal procedures that the government uses to identify these protected digital systems, establish institutional authorities for protecting critical information infrastructure, and plan responses to cyber incidents.

Section 70 of the IT Act enables the government to identify specific information systems as "protected systems" if those systems are considered vital to the functioning of critical information infrastructure, frame policies for the security of such critical digital systems and lays down penalties for unauthorized access or damage to these systems.

Section 70A of the IT Act gives the Central Government the authority to appoint a national agency responsible for protecting and managing such CII systems. The National Critical Information Infrastructure Protection Centre (NCIIPC) is an organization created by the Government of India, which acts as the primary agency for the identification, protection, and resilience of India's critical information infrastructure. It operates under the National Technical Research Organization (NTRO).

Section 70B of the IT Act provides that the Indian Computer Emergency Response Team (CERT-In) will be functioning as

India’s national nodal agency for cybersecurity incident response. Functioning in this capacity, CERT-In performs functions which involves collection, analysis, and dissemination of information related to cyber incidents, issuance of alerts and advisories, and coordinating emergency response activities.

These rules, taken together, provide the legal foundation for India's cybersecurity and CII protection, monitoring, and response systems.

B. Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018

The Information Technology (Information Security Practices and Procedures for Protected Systems) Rules, 2018, were promulgated under Section 70 of the Information Technology Act to strengthen the protection of pivotal computer resources designated as "Protected Systems".

These systems are termed as Critical Information Infrastructure. These regulations outline the security measures for the protection of Critical Information Infrastructure. The key security measures and procedural safeguards that are implemented by these rules include authentication procedures, access control systems, monitoring systems, and regular security audits. Furthermore, these rules also lay out for the appointment of a Chief Information Security Officer (CISO) who will be responsible for maintaining security policies and monitoring cybersecurity compliance within the organization.

These rules also impose certain mandatory procedures on the organization managing the protected systems, related to

implementing robust identity management, regular penetration testing, comprehensive vulnerability assessment, and proactive incident response. In addition to this, these rules also mandate organizations to create plans and policies related to disaster recovery, risk management, and cybersecurity. Also requiring organizations to involve continuous monitoring, reporting of cybersecurity issues, and interaction with authorized agencies such as NCIIPC and CERT-In. These are all intended to secure these protected systems from cyberattacks, illegal access, and disruptions which otherwise can impact public safety, economic stability, or national security. These steps provide for the protection of the critical information infrastructure and thus ensure the continuity of essential services during a cyber incident.

In general, the 2018 Rules provide the operational guidelines for establishing cybersecurity measures for critical systems and thus strengthening India’s legislative framework governing Critical Information Infrastructure protection.

C. The National Critical Information Infrastructure Protection Centre (NCIIPC)

NCIIPC was established in 2014 under the National Technical Research Organisation (NTRO). It functions as the national coordinating body responsible for the protection of Critical Information Infrastructure (CII) in India. The Centre is entrusted with the tasks of identifying, securing, and managing the country's essential information systems that are vital for national security, economic stability, and public welfare.

The main functions of the NCIIPC include:

- Identifying and classifying computer resources as critical information infrastructure (CII).
- Performing vulnerability and risk assessment for the protected systems.
- Assisting organizations in managing CII in developing security policies and adopting standards.
- Emphasizing on coordination and sharing of information between public and private sector entities.
- Coordinating with CERT-In and also with sector-specific Computer Emergency Response Teams (CERTs) for managing cyber incidents.

- Responsible for creating awareness regarding cybersecurity and enhancing the skills of personnel through training.
- Providing guidance to the government entities on the policy matters and legal framework related to the protection of CII.

D. The Indian Computer Emergency Response Team (CERT-In)

CERT-In is a national authority formed under the Ministry of Electronics and Information Technology (MeitY) for addressing cybersecurity. The task scope of CERT-In is much wider than that of the National Critical Information Infrastructure Protection Centre (NCIIPC). NCIIPC specifically deals with the protection of critical information infrastructure (CII), whereas CERT-In deals with the cybersecurity incidents related to the entire Indian cyberspace, including government networks, private sector systems, and individual users. CERT-In manages and coordinates responses to general cyber incidents, except those related to Critical Information Infrastructure (CII) as this comes under the purview of NCIIPC. This clearly indicates that the scope of CERT-In is much broader than NCIIPC, which results in a significant jurisdictional overlap. The key functions of CERT-In mainly include issuing advisories, guidelines, and alerts regarding cyber threats and vulnerabilities.

CERT-In Directives, 2022, mandate reporting cyber incidents within six hours. The revised and updated directives of CERT-In, i.e., Directives 2022, aim to strengthen India's cybersecurity framework and establish a safer and more resilient digital ecosystem by ensuring:

- Mandating organizations to report cyber incidents to CERT-In within 6 hours.
- Enhancing coordination between organizations and CERT-In to ensure prompt incident response, which enables prompt analysis of the incident.
- Requiring organizations to maintain and retain system logs, thereby ensuring accountability and traceability.
- Ensuring standardization of security practices across all vital sectors.

E. National Cyber Coordination Centre (NCCC)

National Cyber Coordination Centre (NCCC) is established under the Ministry of Electronics and Information Technology (MeitY). It serves as an important part of India's cybersecurity framework. It acts as a centralized platform for monitoring of cyber threats and sharing cybersecurity intelligence among other government entities.

The principal objective of NCCC is to strengthen situational awareness related to the cyber threats affecting India's digital ecosystem. It requires the analysis of vast amount of internet traffic and identifying patterns that could be suggestive of potential cyberattacks, harmful activity, or vulnerabilities in security. Thus, detecting the cyber threats in real time. NCCC helps government agencies in taking proactive preventive and defensive measures. The NCCC also enables coordination and information exchange between many cybersecurity parties, such as sectoral regulators, law enforcement agencies, and intelligence services.

F. Ministry of Home Affairs (MHA)

The Ministry of Home Affairs (MHA) has a pivotal role in India’s cybersecurity framework. It primarily oversees law enforcement, cybercrime investigations, and national security aspects of cybersecurity. While organisations like CERT-In and NCIIPC mainly deals with technical cybersecurity management, MHA is responsible for cybercrime investigation and prosecuting cyber criminals,

The Indian Cyber Crime Coordination Centre (I4C) was established under MHA to enhance the nation's ability to fight cybercrime. The I4C acts as a central point across various law enforcement agencies for coordinating cybercrime investigations, exchanging intelligence, and creating national strategies to prevent cybercrime in the country.

The MHA also collaborates with state police and various cybercrime units for the purpose of investigating cases related to financial fraud, identity theft, ransomware attacks, and cyber espionage.

G. The National Cybersecurity Policy, 2013

National Cybersecurity Policy, 2013 is India's first comprehensive cybersecurity policy. It provides a strategic vision for a secure and robust cyberspace in India by protecting both public and private infrastructures against cyber threats. The policy provides a framework for strengthening cybersecurity capabilities by addressing concerns such as threat intelligence exchange, human resource development, and infrastructure protection.

The primary objectives of the policy are as follows:

- The policy aims to provide a secure and resilient cyberspace to individuals, businesses, and government sectors.
- Strengthening the critical information infrastructure by implementing techniques to prevent, detect, and respond to cyber-attacks.
- Enhancing collaboration between public and private sector organisations to share information and best security practices.
- Providing for enhancing capacity building, skill development and research & development of cybersecurity techniques.
- Strengthening the legal and regulatory framework for ensuring compliance with cybersecurity standards.
- Encouraging international collaborations for tackling cyber threats.

Despite the fact that the policy lays out the groundwork for India's cybersecurity strategy, the policy is today regarded as outdated because of the speed at which technology is developing and the cyber threats are becoming more sophisticated in nature.

3. CII PROTECTION AND DATA GOVERNANCE MECHANISM IN INDIA

A. Overview of Data Protection Obligations Imposed on CII Entities

In today's digital ecosystem, the regulatory framework governing CII cannot be understood in isolation; rather, it must be understood in the light of the rapidly evolving personal Data Protection regime. The introduction of the Digital Personal Data Protection Act, 2023 (hereinafter referred to as the Act of 2023) is a significant step towards regulating the processing of personal data by both public and private entities in India. Safeguarding the information privacy of an individual in India is one of the core objectives of the Act of 2023. Various provisions of the Act of 2023 have been designed in such a manner that they will have explicit and implicit implications on the organizations designated as CII under Section 70 of the Information Technology Act, 2000. Entities designated as CII usually process large quantities of confidential and critical operational data; some of them might be qualified to be personal data protected under the Act of 2023. Accordingly, the obligation imposed by the Act of 2023 has significantly restructured the compliance requirements for CII entities by establishing a layered interface between Data Protection mandate and Cyber Security obligations.

The wide definition of "Personal Data" as well as detailed compliance obligations imposed on "Data Fiduciaries" are foundational elements of the Act of 2023. Many CII designated entities such as Banks, Transportation Network, Energy Sector, Digital Payment Network, Telecom Service Providers usually function as a large-scale Data Fiduciaries. Under Sections 5 to 9 of the Act of 2023, various obligations have been imposed on such Data Fiduciaries, such as lawful processing of data, data minimization, purpose limitation, limitation on storage, maintaining data accuracy, and comprehensive security measures. Although these compliance obligations are at par with global data protection principles, when it comes to CII-designated entities, these compliance obligations give rise to distinct

concerns. As per many cybersecurity experts, the operational dynamics of cybersecurity governance often demand a vast volume of data collection and retention, monitoring of user behavior, real-time data analysis etc. Many of the above-mentioned operational practices may not easily align with the requirements of the Act of 2023, specifically the requirement of storage limitation and purpose-specific data collection.

B. Areas of Overlap and Potential Conflict Between CII Protection and Data Governance

The implementation of "Reasonable Security Measures" is another important obligation imposed on the Data Fiduciaries by the Act of 2023 in order to protect personal data breaches. Although, the parameters of such safeguards are not defined in the Act of 2023, whereas these obligations align closely with the cyber security duties imposed by the National Critical Information Infrastructure Protection Centre (NCIIPC) and CERT-In on CII entities through its's directives. However, the presence of these two parallel regimes may result in duplication and inconsistency in compliance obligations. For example, on the one hand directions issued by CERT-In mandates retention of system log for minimum 180 days period, whereas the Act of 2023 stress upon limitation on data storage and erasure of such data once purpose of such processing is fulfilled. The lack of a clearly defined statutory relationship between the Act of 2023 and CERT-IN directives give rise to legal uncertainty for CII designated operators aiming to harmonize both cyber security directives and data protection obligations.

The introduction of "Breach Notification framework" in the Act of 2023 is another important area of intersection. The Act of 2023 imposes obligation on Data Fiduciary to inform affected Data Principles and Data Protection Board of India in case of a personal data breach. Similarly, as per the CERT-In directives of 2022 it is mandatory to report Cyber Crime incident within 6 hours of detection. As per many experts, the obligations of dual reporting may arise in the matter of CII Cyber Security breach because such Cyber incidents might involve both personal data and operational disruptions. The absence of any standard applicability criteria under Act of 2023 and CERT-In directive in the cases of CII Cyber Security breach might create a regulatory duplication and operational confusion. Additionally, early-stage disclosure in public relating to breaches in CII cyber security could compromise national security interests- an issue that Act of 2023 doesn't addressed fully.

The introduction of concept like "Significant Data Fiduciaries" in the Act of 2023 is another significant step that was taken to protect Personal Data Breach cases. These significant data fiduciaries are subject to enhanced compliance requirements such as appointment of Data Protection Officers, Data Protection Impact Assessments, and Audits. Taking into consideration the scale and sensitivity of data that CII-designated entities usually process, they may be notified as significant Data Fiduciaries under the Act 2023. Imposing such obligations on the CII entities appears to be justified from the point of view of protecting individual data privacy, but at the same time such obligations impose an additional regulatory burden on the CII entities who are already overburdened by stringent cybersecurity oversight measures taken by national and sector-specific security agencies. The IT Act 2000, DPDP Act 2023, various sector-specific as well as executive-led rules and guidelines create a multilayered and fragmented regulatory compliance mechanism without any coordination mechanisms. It is exactly the opposite of the framework created in data protection laws implemented in the UK, such as UK GDPR, where both essential services and national security aspects are incorporated in a more integrated manner.

Cross-border data transfers is another significant area where challenges will emerge in the future. Section 16 of the Act of 2023 allows transfer of personal data to countries notified by the Central Government, but it is subject to certain conditions mentioned in notifications. Such restrictions on data transfers may hinder working of many CII designated entities because they often operate in collaboration with global cloud service provider, foreign vendors dealing in cyber-Security as well as cross border threat sharing arrangements. The regulatory objectives of the Act of 2023 and cybersecurity frameworks are distinctive. On the one hand, safeguarding the informational privacy of individuals in India is one of the core objectives of the Act of 2023, whereas cyber security frameworks across the globe support information sharing to combat transnational threats. Such distinctions in regulatory objectives may result in conflict between India's data sovereignty goals and global cyber security practical necessities.

C. Implications in Case of Non- Compliance with Data Protection Obligations

In case of non-compliance with the rules and regulations set out in the DPDP Act, 2023 by any Data Fiduciary, strict enforcement mechanisms in the form of financial penalties have been introduced in the Act. The financial penalties in some violations may extend to ₹ 250 crore. A stringent enforcement mechanism is necessary to ensure data protection accountability. However, imposing such financial penalties on CII-designated entities may have unanticipated outcomes, such as core cybersecurity investments being diverted by these entities in order to meet data protection obligations. Moreover, the Data Protection Board, which has been introduced under the Act of 2023 is a Civil adjudicatory body with limited technical knowledge in matters related to National Security and critical infrastructure. As a result, questions may arise regarding the ability of the Data Protection Board to address complicated matters involving CII operational issues, wherein questions related to privacy, public interest, and cyber security intersect.

From a normative perspective, the Act of 2023 is designed to protect individual informational autonomy, which is enshrined in Article 21 of the Indian Constitution. On the other hand, collective security as well as public interest are two rationales on which CII protection fundamentally relies. As per many experts, in order to have an effective cyber governance framework in India, we need to balance the above-mentioned different value systems. Under the Act of 2023, broad exemptions in the name of sovereignty, security, and public order have been carved out in favor of our law enforcement authorities, but no such exemptions or any specific provision has been created in the matters of CII-designated entities' operations. Moreover, no statutory framework has been created to harmonize the privacy rights of an individual with CII operations; thereby, a significant design gap in the DPDP Act, 2023 is easily evident. This creates an ambiguity for CII-designated operators aiming to comply with both cybersecurity directives imposed by authorities and data protection obligations under the DPDP Act 2023.

From the above-mentioned analysis, it can be concluded that the introduction of the Act of 2023 is a landmark reform towards protecting individual informational autonomy, but at the same time, the Act of 2023 fails to address the specificity related to the CII operational framework. For instance, the Act of 2023 regulates the operations of all categories of Data Fiduciaries, but it fails to differentiate between those entities who carried out essential national functions and those that work as commercial entities. Many experts have criticized such a standardized approach, especially when data is processed for the purpose of national security and public safety, whereas in UK, such an issue of maintaining balance between CII regulations and data protection law is addressed through a well-defined statutory mechanism. India’s approach in such matters is based on more executive co-ordination and implicit assumptions, thereby leaving room for confusion and interpretive conflicts still left.

4. COMPARATIVE ANALYSIS OF CII GOVERNANCE MODEL IN UNITED KINGDOM, UNITED STATES INDIA

In order to have a comprehensive understanding of CII governance framework operating in India, analyzing the manner in which mature jurisdictions like United Kingdom and United States govern and safeguard their digital infrastructure through its legal framework is imperative. In order to protect their CII both United Kingdom (herein after referred as UK) and United States (herein after referred as USA) have taken comprehensive approach as compared to India. Both the UK and USA have not considered it as a mere technical issue; rather, they have linked CII protection with public-private cooperation, imposing accountability on the entities as well as considering it as a matter of national cyber security. In India, Sections 70, 70A, and 70B of the Information Technology Act, 2000 (herein after referred as IT Act) constitute a statutory foundation for CII regulations. Under Section 70 of the IT Act, the Central government has been empowered to declare any computer resource as a “protected system”. Apart from the IT Act, there is no other legal framework that regulates CII operations in India. In Contrast to India, mature jurisdictions like the UK and USA rely mainly on sector-specific laws, enforceable standards, and accountable governance frameworks. Experience of the UK and USA shows that protection of CII-designated entities can be ensured only when a coherent legal structure has been created, rather than merely relying on technological capabilities.

A. Position in United Kingdom

The foundational legal framework existing in the United Kingdom for the protection of CII entities is the Network and Information Systems Regulations 2018 (herein after refer as the NIS Regulations 2018). It is borrowed from the European Union NIS directives. The UK NIS Regulations 2018 impose the same legally binding cybersecurity obligations on CII-designated entities in the UK as were established in the European Union NIS directives. The UK follows a decentralized and sector-specific statutory instrument approach for regulating CII-designated entities instead of a centralized model or single legal framework named as "CII Act". For instance, in the UK, instead of designating any entity as CII, they designate such entities as "operators of essential services" under regulation 6 of NIS Regulations 2018. Moreover, such declaration is not carried out by a centralized agency; rather, it is carried out by sector-specific competent authorities.

In contrast to India, the UK has statutory criteria for designating any entity as "operators of essential services". Some of the major criteria for designating under NIS Regulations 2018 are as follows: -

- The nature of services - Such operators must provide services which are essential for social or economic stability of the country. Moreover, services provided by such operators depend on network and information systems.
- Kind of impact on society due to disruption of such services.

In the UK, various sector-specific competent authorities such as department of transport, Ofcom for digital infrastructure, Ofgem for the energy sector, and the NHS for the health sector impose obligations on the operators designated "operators of essential services" under NIS Regulations 2018 to comply with cybersecurity guidelines issued by them.

Apart from NIS Regulations 2018, the UK has statutes like the Telecommunications (Security) Act 2021, Data Protection Act 2018 and UK GDPR that supplement governance of critical information infrastructure. The Telecommunications (Security) Act 2021 imposes various cybersecurity responsibilities on telecom providers in the UK, such as mandatory vendor risk assessment, legal codification of supply chain security etc. Similarly, the Data Protection Act 2018 operating in the UK integrates cyber security obligations within data governance.

As per many scholars, some of the major strengths of the UK CII governance model is the existence of a clear legal framework regulating cyber security obligations and an enforcement mechanism to enforce such obligations. Under Regulation 10 of NIS Regulations 2018, various mandatory obligations are imposed on operators such as the implementation of "appropriate and proportionate" measures both at the technical level as well as the organizational level to combat cyber security breach cases and timely reporting of any cyber security incidents. In order to ensure that operators are complying with these directives, the enforcement mechanism of the NIS Regulations includes financial penalties up to 17 million euros, regular audits and inspections by competent authorities, and mandatory binding improvement notices. The UK cyber security framework includes data protection compliance, regulatory oversight mechanisms, administrative laws and national cyber security aspects.

India's nodal agencies for the protection of CII are the National Critical Information Infrastructure Protection Centre (hereinafter referred to as NCIIPC) and CERT-In, which have been established under Sections 70A and 70B of the IT Act. But the IT Act doesn't provide any specific statutory provision that demarcate enforcement hierarchy of these nodal agencies. As a result, legal uncertainty, regulatory duplication, and operational confusion have been created for CII-designated entities. Whereas, the UK has multilayered but coordinated models for CII protection, such as the National Cyber Security Center acting as a technical authority, an advisory role is given to the National Protective Security Authority, and sector regulators are responsible for enforcement. CII governance framework operating in the United Kingdom is able to blend regulatory flexibility with clear legal safeguards because they deal CII protection mainly through already established regulatory frameworks instead of treating it as an exceptional national security matter.

B. Position in United States

For protecting the CII, the legal framework followed in the United States is quite different from what is followed in India and the UK. Instead of any centralized model or sector-specific statutory instrument for declaring any entity as CII, the United States relies on core executive instruments, such as Presidential Policy Directive-21. In the US, sixteen sectors have been designated as Critical infrastructure under Presidential Policy Directive-21. The major emphasis of Presidential Policy Directive-21 is on risk management and resilience. Under the Cybersecurity and Infrastructure Security Act 2018, the US has also established a Cybersecurity and Infrastructure Security Agency (hereinafter referred to as CISA). CISA functions as a national coordinating agency for CII protection in the USA. Facilitating information sharing, incident response, and capacity building are some of the primary functions of CISA in the USA.

The US model for protecting CII relies heavily on establishing partnerships between government and private entities that manage critical systems, as well as on complying with standards set for operators rather than drafting rigid legal rules. As per many scholars, this is the main reason for the USA model's success in protecting CII infrastructure effectively. In the USA there are various sector-specific statutory instruments have been created to regulate CII operations. For instance, the Federal Power Act for the energy sector, the Gramm-Leach-Bliley Act for the financial sector, and TSA security directives for the transportation sector, etc. are some of the sector-specific statutory instruments operating in the USA. Moreover, the National Institute of Standards and Technology has been created under the NIST cybersecurity framework in the USA. The core function of the National Institute of Standards and Technology is to identify, protect, detect, respond, and recover from cyber incidents on CII in the USA. The NIST cybersecurity framework of the US has been designed in such a manner that both public and private entities are complying with best practices laid down by it, although it is voluntary in nature.

Both the UK and USA governance models help to achieve a balanced relationship between data protection laws and cyber security regulations. The UK GDPR and its 2018 Data Protection Act contain an explicit provision where departure from standard data protection rules has been permitted in matters where national security or essential services are involved. Similarly, in the USA, the sector-specific privacy laws as well as security laws have been designed in such a manner that they can be operated simultaneously without creating any direct conflict between them. From the above analysis, both these jurisdictions have understood that privacy and cyber security are two goals which need to be achieved for protecting CII as well as that they are complementary to each other; therefore, these must be harmonized through legislative design as well. In contrast, the underlying tension between privacy governance and security governance in the digital age is not dealt with adequately under India’s Digital Personal Data Protection Act, 2023. Although the Digital Personal Data Protection Act, 2023 strengthens individual informational autonomy and introduces stringent enforcement mechanisms to ensure data protection accountability in India’s informational ecosystem, at the same time it complicates the regulatory framework for CII operators. The lack of a clearly defined statutory relationship gives rise to legal uncertainty for CII-designated operators aiming to harmonize both cybersecurity directives and data protection obligations.

After the comprehensive understanding of CII governance framework operating in India, UK and USA, it can be concluded that India’s framework is more in the nature of reactive instead of systemic as well as the emphasis of Information Technology Act, 2000 is to criminalize conducts instead of securing cybersecurity, recovery of lost data or continuity planning. On the other hand, the major emphasis of the USA and UK framework is on ensuring supply chain risk, continuity planning, and recovery capability. Moreover, mature jurisdictions like the USA and UK demonstrate that CII protection can be ensured through risk-based identification, strong penalties, enforcement, statutory obligations, and integrated data protection alignment.

5. CRITICAL GAPS IN INDIA’S CII LEGAL REGIME

A. Institutional Fragmentation and Legislative Ambiguity

1. **Lack of dedicated CII-specific statutory framework**

- In India, Sections 70, 70A and 70B of the Information Technology Act, 2000 (herein after referred as IT Act) constitute a statutory foundation for CII regulations. Apart from the IT Act, there is no other law that regulates CII operations in India.
- Under Section 70 of IT Act, Central government has been empowered to declare any computer resource as "protected system". But IT Act fails to provides any clear procedural safeguards, legislative standards and oversight mechanism for designation.
- The lack of well-defined statutory parameters for such designation undermines transparency and reduces regulatory predictability, unlike sector specific statutory frameworks approach followed in advanced jurisdiction.

2. **Executive-led governance framework**

- In India, we have a nodal agency for the protection of CII, namely the National Critical Information Infrastructure Protection Centre (hereinafter referred to as NCIIPC). NCIIPC has been established under Section 70A of the IT Act via notification instead of a dedicated legislative instrument that defines its explicit compliance and sanctioning authority.
- Similarly, for dealing with cyber security incidents in India, we have CERT-In, a specific authority established under Section 70B of IT Act. CERT-In performs its operations mainly through executive directives instead of a well-defined, comprehensive regulatory framework specifically designed for its operations.
- According to many experts, such over-dependence on executive directives and advisories will undermine institutional accountability as well as weaken regulatory certainty.

3. **Overlapping jurisdiction and sectoral isolation**

- Apart from the IT Act framework, there are sector-specific directives and regulations issued by various bodies in India for CII protection, such as for the banking sector, RBI issues cybersecurity circulars; for the insurance sector, guidelines are issued by IRDAI; for security market, cyber security framework is issued by SEBI etc. All these directives operate independently of the IT Act architecture.
- India's legal framework doesn't provide any specific statutory provision that will ensure coordination between NCIIPC oversight mechanism and these sector-specific directives issued for securing cybersecurity.
- It will create legal uncertainty, regulatory duplication, operational confusion, and fragmented accountability for CII-designated entities.

4. Legislative Vagueness in defining CII

- Critical Information Infrastructure has been defined widely under Section 70 of the IT Act. IT Act uses phrases like *"incapacitation or destruction shall have a debilitating impact on national security, economy, public health or safety". As per many experts, the IT Act,* on the other hand, fails to provide any ascertainable evaluation standards.
- Since the IT Act doesn't define terms like "*debilitating impact". As a result, the IT Act leaves scope for discretionary executive interpretation.*
- The IT Act also fails to provide any statutory differentiation between essential services operated privately and military infrastructure having strategic value.

5. Limited Judicial Interpretation

- Section 70 and 70A of IT Act have not been substantially interpreted by the Indian judiciary. It means that issues like state responsibility or operator liability in matters of CII protection have not been dealt with in

detail by Indian Courts. So much clarity regarding the scope of state responsibility or operator liability is not available in judicially.

- As far as Privacy jurisprudence is concerned, it has been developed significantly post Justice K.S. Puttaswamy v. Union of India (2017) judgement. Now privacy has been recognized as a fundamental right under Article 21 of the Indian Constitution. But cybersecurity jurisprudence is still underdeveloped in India. It is a grey area which still needs to be dealt with legally as well as judicially in India.

B. Security Oriented Approach and Lack of Proactive Resilience Mechanism

1. Reactive security orientation

- The Information Technology Act, 2000 has been designed with legislative intent to protect computers from "unauthorized access" and, in case unauthorized access happens, then sanctions in the form of imprisonment and fines can be imposed.
- The emphasis of the IT Act is to criminalize such conduct instead of securing cybersecurity, recovery of lost data, or continuity planning.
- The IT Act doesn't prescribe any specific requirement for mandatory risk assessment or regular audits for CII-designated entities.

2. Absence of statutory risk assessment mechanism

- Mature jurisdictions have legislative frameworks like the NIST Cybersecurity Framework operating in the USA and NIS Regulations operating in UK that governs cyber security compliance models. But such a specific legislative framework is absent in India.
- On the one hand, directions issued by CERT-In mandate retention of system logs for a minimum of 180 days. Similarly, as per the CERT-In directives of 2022, it is mandatory to report cyber-crime incidents within 6 hours of detection, but it fails to embed institutional resilience principles such as stress testing or sector-wise simulation exercises.

3. Absence of explicit duty of care imposed on CII operators

- Section 70 of the IT Act confers status of protected systems on CII entities, but apart from this status, the IT Act fails to prescribe any structure and long-term compliance responsibilities for CII-designated entities.
- Moreover, no statutory obligation has been imposed on CII entities to maintain cybersecurity standards under the IT Act.
- In matters of securing cybersecurity of CII-designated entities, India still follows a reactive and occurrence-based policy instead of a proactive and anticipatory risk management policy.

4. Insufficient integration with national security laws

- The IT Act fails to establish any formalized legislative nexus with the National Security Act and internal security laws. CII is framed within a national security framework. As a result, the legislative framework for protecting CII is largely symbolic instead of embedded within operational security architecture.

5. Data Governance disconnect

- Introduction of DPDP Act 2023 is a landmark reform towards protecting individual informational autonomy, but specificity related to the CII operational framework was not kept in mind while drafting the Act. The act has been designed to regulate the working of all categories of data fiduciaries, without differentiating between organizations working toward essential national functions and those working as commercial entities. This standardized approach is ill-suited to all sectors, especially where data is processed for national security and public safety.

- The DPDP Act 2023 strengthens individual informational autonomy and introduces stringent enforcement mechanisms to ensure data protection accountability in India's informational ecosystem; at the same time, it complicates the regulatory framework for CII operators. The existing legal framework operating in India clearly lacks established doctrines for balancing data protection with nation cyber security framework.

6. CONCLUSION AND RECOMMENDATIONS

The Critical Information Infrastructure (CII) plays a crucial role in today's highly digitally interconnected and interlinked world. All essential services such as banking, power, telecommunication, transportation, and governance rely on interconnected information systems, thus making them highly vulnerable to cyber threats and disruptions. This poses concerns for national security, economic stability, and public welfare, thereby making the protection of Critical Information Infrastructure (CII) central to contemporary cyber governance. In India, the CII is primarily governed by the IT Act 2000 through sections 70, 70A, and 70B. In addition to this, there are institutional mechanisms such as NCIIPC and CERT-In and various sector-specific regulatory frameworks for the protection of CII. The Digital Personal Data Protection Act, 2023 also contributes to enhanced cybersecurity by providing obligations related to data protection and breach reporting.

Although as a foundation, India has a well-established legal and institutional framework for the protection of CII, this existing framework lacks a comprehensive approach, remains protection-centric, fragmented, and insufficient to address the ever-evolving, sophisticated cyber threats. The study also identifies various other gaps in the existing legal regime for the protection of CII. This includes a lack of a unified and comprehensive cybersecurity law specifically addressing CII protection, vagueness in statutory criteria for defining CII, overlapping institutional responsibilities, an excessive reliance on executive directions, limited judicial interpretation, and the lack of mandatory statutory duties relating to risk assessment, resilience planning, etc. In addition to the above, the scope of the DPDP Act 2023 is basically confined to sensitive personal digital data protection rather than direct infrastructure-specific protection. Also, if on the one hand, this 2023 Act played an important role in strengthening individual informational autonomy as well as ensuring data protection accountability in India's information ecosystem, but at the same time it complicates the regulatory framework for CII operators.

Comparative reference to the legal approaches followed by the USA and UK also makes it clear that legal obligations clarity, improved incident reporting mechanisms, regular security audits, stronger regulatory coordination, and structured public-private cooperation are essential for protecting critical information infrastructure. Therefore, it is a matter of the hour for India to have a more coherent, coordinated, and comprehensive legal framework for governing CII. The existing legal framework needs updating so that it can address present-day sophisticated and systemic cyber-attacks and provide clear standards for CII protection.

Stronger coordination between various regulatory authorities such as NCIIPC, CERT-In, and other sector-specific regulators is essential for implementing effective CII governance. The harmonization between the existing cybersecurity, data protection laws, and sector-specific regulations is also an essential requirement. This will ensure effective protection of critical information infrastructure and strengthen national cybersecurity governance.

References

1. James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats" (Center for Strategic and International Studies, 2002), available at: https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats?
   (last visited May 1, 2026).
2. Rolf H. Weber & Evelyne Studer, "Cybersecurity in the Internet of Things: Legal Aspects", 26 Computer Law & Security Review 715 (2016).
3. Scott J. Shackelford, "Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk", 15 Chapman Law Review 445 (2012).
4. Richard A. Clarke & Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It (HarperCollins, 2010).
5. Devika Sharma, "Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges" 2 Legal Studies in Digital Age 456 (2023).

6. The Information Technology Act, 2000 (Act 21 of 2000), s. 70.
7. The Information Technology Act, 2000 (Act 21 of 2000), s. 70A.
8. The Information Technology Act, 2000 (Act 21 of 2000), s. 70B.
9. Ashish Sharma and Savyasanchi Pandey, "Legal Mechanisms for Cyber Threat Mitigation in India: A Comparative Jurisprudential Analysis" 3 International Journal of Research in Academic World 122-125 (2024).
10. Arpan Patel, "Cyber Security in India: Legal and Policy Challenges", 7 Indian Journal of Law and Technology 45 (2011).
11. Mr. Saraswat Pathak1 and Dr. Vir Vikram Bahadur Singh, "A Critical Study on Legal Framework of Cyber Law in India" 7(2) International Journal for Multidisciplinary Research 1-8 (2025).
12. Manvi Gupta, "Cyber Security Legal Framework in India – Overlaps, Problems and Challenges" 12 Journal of Business Management and Information System 11-19 (2025).
13. Government of India, "National Cyber Security Policy, 2013" (Ministry of Electronics and Information Technology,2013) available at: https://www.meity.gov.in/content/national-cyber-security-policy-2013? (last visited on May 2, 2026).
14. Supra note 6.
15. S.Chandana, "Critical Analysis Of Cyber security Due Diligence And Its Impact On M&A Agreements Under The Digital Personal Data Protection Act, 2023 (DPDP Act)" 7 Indian Journal of Law and Legal Research 2023 (2025).
16. Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (Happer Collins, New Delhi, 2018).
17. The Digital Personal Data Protection Act, 2023 (Act 22 of 2000), s. 2(i), (t).
18. Bharvi Shahi and Anand Raj Dev, "Naviqating India's Digital Personal Data Protection Act: Critical implications and Emerging Challenges" 3 International Journal of Legal Studies and Social Science 415 (2025).
19. The Digital Personal Data Protection Act, 2023 (Act 22 of 2000), s. 8.
20. National Critical Information Infrastructure Protection Centre, "Guidelines for Protection of Critical Information Infrastructure" 5 (January, 2015).
21. CERT-IN Direction, issued on April28,2022 , clause 4 (xiv) (Log retention requirement).
22. Sonali Srivastav, "India: Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL" IJLT Blogs, 21st march 2024, available at https://forum.nls.ac.in/ijlt-blog-post/india-decrypting-critical-concepts-under-indias-digital-personal-data-protection-act-2023-and-comparison-with-gdpr-and-pipl/? (last visited on 5/3/2026).
23. The Digital Personal Data Protection Act, 2023 (Act 22 of 2000), s. 2(z).
24. Anumodan Tiwari, "Decoding the right to privacy in the Digital age: A critical analysis of Data protection laws in India under the DPDP ACT,2023" Lawful Legal, 21st December 2024, available at https://lawfullegal.in/decoding-the-right-to-privacy-in-the-digital-age-a-critical-analysis-of-data-protection-laws-in-india-under-the-dpdp-act-2023/? (last visited on 3/3/2026).
25. The Digital Personal Data Protection Act, 2023 (Act 22 of 2000), s. 16.
26. Paul Schwartz & Daniel Solove, "The PII Problem: Privacy And A New Concept of Personally Identifiable Information" 86 New York University Law Review 1821 (2011).
27. The Digital Personal Data Protection Act, 2023 (Act 22 of 2000), s. 33-36.
28. The Digital Personal Data Protection Act, 2023 (Act 22 of 2000), s. 27,28.
29. Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
30. Supra note 6.
31. The Network and Information Systems Regulations, 2018, SI 2018/506 (UK), reg. 6.
32. Adejoke T. Odebade and Elhadj Benkhelifa, " A Comparative Study of National Cyber Security Strategies of Ten Nations" Arxiv 5-20 (2023), available at https://arxiv.org/abs/2303.13938 (last visited on 5/4/2026).
33. Arlo Sterling, "Risk Control and Security Governance Practices for Critical Informational Infrastructure in the AI era" 2 Sustainability Horizon 18-27 (2026).
34. National Cyber Security Center, Cyber Assessment Framework (2023), available at https://www.ncsc.gov.uk/collection/cyber-assessment-framework (last visited at 15/4/2026).
35. Nitish Kumar, "India's Cyber Security Policies And The Road Ahead" Research Gate (2024), available at https://www.researchgate.net/publication/385079983_INDIA'S_CYBER_SECURITY_POLICIES_AND_THE_ROAD_AHEAD/link/67146c1024a01038d0f862be/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 (last visited on 5/4/2026).
36. Supra note 12.
37. Presidential Policy Directive-21, The White House (Feb. 12, 2023), available at:https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (last visited on 5/3/2026).
38. OECD, "Development of Policies for Protection of Critical Informational Infrastructures" (OECD Digital Economy Papers, 2007), available at https://www.oecd.org/content/dam/oecd/en/publications/reports/2007/02/development-of-policies-for-protection-of-critical-information-infrastructures_g17a1c08/231008575813.pdf (last visited on 5/3/2026).
39. Observer Research Foundation, "Towards a Cyber Security Framework for Critical Infrastructure" (2023), available at https://www.orfonline.org/public/uploads/posts/pdf/20230712122323.pdf (last visited on 12/3/2026).
40. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cyber Security" (2018), available at https://www.nist.gov/cyberframework (last visited 15/3/2026).

41. D.M. Ekadshi, “Comparative analysis of cyber security laws India, United States and United Kingdom” 9 International Journal of Law 88-91 (2023).
42. UK Government, Critical 5 Shared Narrative on Critical Infrastructure Security and Resilience (2024), available at https://www.gov.uk/government/publications/critical-5-shared-narrative-on-critical-national-infrastructure/adapting-to-evolving-threats-a-summary-of-critical-5-approaches-to-critical-infrastructure-security-and-resilience-html (last visited on 7/4/2026).
43. N. Singh, “Data Protection and Privacy Challenges in Digital age in India” 16 White Black Legal International Law Journal 13-28 (2024).
44. Saurabh Kumar Mishra, “Legal Implications Of Cyberattacks On Critical Infrastructure” 5(7) Indian Journal Of Legal Review 678-693 (2025).
45. Supra note 5.
46. Supra note 6.
47. R. Gupta R & M.Sinha,“ Evaluating India's Cyber Law Framework: Gaps and Opportunities” 15(1) Indian Journal of Law & Technology 55–78 (2023).
48. A. Kumar, “International Legal Instruments and India's Cybersecurity Challenges” 10(2) Journal of International Law and Policy 21–38 (2022).
49. R. Mehta and P. Singh, “Toward a Unified Cyber Security Legistation India: A Legal Prespective” 12(1) Indian Journal of Technology Law 45-46 (2024).
50. A. Chaudhary & P. Roy, “Towards a Cybersecure India: Legislative Needs and Global Lessons”8(2) Journal of International Cyber Law 101-120 (2024).
51. Supra note 11.