
CERT-IN DIRECTIONS: RECONCILING CYBERSECURITY, INFORMATIONAL PRIVACY AND THE RIGHT TO FREEDOM

Vanshika Rathi, JGLS

Research Question

Are the CERT-In Guidelines combatting cyberthreats effectively and without undermining the constitutional principles of informational privacy and freedom?

I. The Cybersecurity Framework in India

India is the most cyber-attacked nation in Asia and the 10th most cyber-attacked country in the world. This has made it extremely important that the state ensures that appropriate preventive and curatory steps are being taken towards resolving cybersecurity issues and shielding the digital ecosystem in the country. The most malicious tactics used by hackers worldwide include malware, phishing, ransomware, insider threats, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, etc. These have gained momentum in the Indian cyberworld as well and warrant criminal action being taken against them.

Artificial intelligence has drastically and dramatically expedited and scaled up the way cyberattacks are being discovered, refined and carried out. It has amplified **cyber threats** at an unprecedented speed and scale across the cyber kill chain, from automated vulnerability discovery to AI-generated deepfakes and AI-enabled social engineering (using AI to trick/persuade people to take harmful actions). More significantly, AI is developing the ability to act as an autonomous agent that can identify, plan, adapt and carry out offensive cyber operations.¹

In response to these hovering problems and opportunities, CERT-In, the national agency established under Section 70B of the Information Technology Act, 2000 (“IT Act”), has issued

¹ ‘India is one of the most cyber-attacked nations. Here’s how AI adds another layer to the threat’ (*The Indian Express*, 26 August 2026) <AI Cybersecurity Threats: How Prepared Is India to Defend Its Cyberspace?> accessed 1 September 2026.

new cybersecurity guidelines that will require technology vendors to adopt AI-assisted security testing, disclose critical vulnerabilities immediately and significantly accelerate patch deployment across India's digital ecosystem. It has also urged organizations and MSMEs to step up defenses through stronger threat detection, continuous monitoring, vulnerability disclosures, and rigorous log preservation, among others.²

The primary objective of the Guidelines promulgated by this nodal agency appears to provide a structured and standardized framework for combating the ever-increased threat of cyber-attacks.

Before analyzing the 2026 guidelines by CERT-In in detail, it is imperative that we understand the most basic provisions of the 2022 Guidelines and their significance in tackling cyber threats.

II. CERT-In 2022 guidelines: A herald for cybersecurity

The landmark cybersecurity directions issued by the CERT-In in April 2022 that have been contested on grounds of violating informational privacy and freedom citizens have made serious inroads to the framework for cybersecurity laws in the country.

From introducing the 6-hour reporting window which mandates that entities (technology providers) must report cyber security incidents to CERT-In within 6 hours of becoming aware of them to encapsulating the time period for retaining customer data for Virtual Private Sector providers, Cloud service providers and VPN operators, these guidelines have been a significant milestone in addressing the systemic problems associated with addressing cyber threats.

Some of the most controversial provisions of these guidelines include the strict incident reporting requirements and data retention mandates. The 5-year period for data retention for VPNs/Cloud providers and the 180-day log retention for the maintenance of ICT system logs within the Indian jurisdiction have been heavily criticized for violating the informational privacy of citizens.³

² 'CERT-In outlines safeguards for Indian orgs, MSMEs amid Mythos AI cybersecurity risk concerns' (*The Indian Express*, 28 April 2026) <CERT-In outlines safeguards for Indian orgs, MSMEs amid Mythos AI cybersecurity risk concerns | Technology News - The Indian Express> accessed 1 September 2026.

³ 'Reporting cyber incidents in 6 hrs mandatory' (*The Indian Express*, 28 April 2026) <Reporting cyber incidents in 6 hrs mandatory | Business News - The Indian Express> accessed 1 September 2026.

III. CERT-In 2026 Guidelines: AI and Cybersecurity

The advisory issued on 26 April 2026 titled ‘Defending against Frontier AI driven Cyber Risks’ has flagged concerns about AI-generated malware, automated reconnaissance and deepfake-enabled social engineering as emerging threat categories. It is third in line of the fast-moving regulatory sequence rolled out by CERT-In to target and tackle AI-assisted attacks and harness the opportunities that come with using AI to deal with cyber-attacks more effectively.

While AI is seen both as a threat and a means to achieve a secure defence mechanism, CERT-In is positively incorporating both its benefits and its vices into its framework of laws to effectively combat the increased threat of Artificial Intelligence in securing and strengthening cybersecurity by deploying and utilizing AI as a tool for compliance to deal with AI-assisted cyberwarfare.

The six compliance obligations that has been placed on the shoulders of technology providers vide this advisory are Continuous Vulnerability Assessment, Immediate Disclosure of Critical and High-Severability Vulnerabilities, Zero-Day Vulnerability Protocol, AI-assisted security testing Certification, Secure Development Lifecycle (SDL) and Bill of Materials and lastly, Incident Response and Customer-facing Transparency.⁴

The first two in the sequence, are a detailed technical playbook called ‘Blueprint for Reducing Exposure and Defending Against AI-assisted Vulnerabilities Exploitation in Digital Infrastructure’ and instructions designed to address the evolving cybersecurity threat landscape driven by artificial intelligence and automated exploitation techniques. They emphasize the need for continuous vulnerability management, rapid remediation, and AI-aware governance to protect against AI-assisted cyber threats.

These guidelines in totality have structurally addressed the growing concern of Artificial Intelligence being deployed by hackers to attack Indian technology providers. While it does not specifically mention Anthropic’s new AI model ‘Mythos’ but as per leading news outlets, these guidelines have been primarily rolled out to address the significant concerns of increased

⁴ Thakur R and Gupta R, ‘Cert-in’s New AI-Vulnerability Guidelines: A Quick-Reference for Oems, Tech Vendors and in-House Counsel’ (S.S. Rana & Co., 4 August 2026) < <https://ssrana.in/articles/cert-ins-new-ai-vulnerability-guidelines-a-quick-reference-for-oems-tech-vendors-and-in-house-counsel/> > accessed 1 September 2026.

risk to cybersecurity injected by the highly capable AI model 'Mythos'.⁵

IV. Right to Privacy, Freedom and the CERT-In Guidelines

Informational privacy is an inherent right in the right to life and liberty as laid down by the Constitution in Article 21. In the *K.S Puttaswamy*, the court laid down the four-fold test to assess the validity of a law in view of its impact on the privacy of the citizens it applied to. This fourfold test comprises of legitimate aim, rational connection, necessity and proportionality.

The law must have lawful and legitimate object, it must bear a rational connection between the measure adopted and the goal specified, the restriction imposed on the citizens that affects their privacy must be necessary and lastly, it must balance the twin concerns of privacy and nation's interest.⁶

Privacy is an essential element of life and its taking away must be for a purpose as important as national security and social welfare. Similarly, a private life is the cornerstone of a wholesome life and its curtailment in the context of cybersecurity must satisfy the essential requirement of maintaining cybersecurity which directly impacts national security and order of the nation. Furthermore, such measures adopted to achieve the ends must satisfy the 4-fold test laid down in the *Puttaswamy* case.

Many courts in landmark cases like *Kartar Singh v State of Punjab*, where the constitutional validity of TADA (Terrorist and Disruptive Activities (Prevention) Act) was confirmed, have upheld the superiority of national security over individual rights and thus, justifying state action violating fundamental rights like freedom of speech, privacy rights. In the context of cybersecurity guidelines rolled out by the CERT-In, it has been observed that the data retaining mandates have a violative effect on the privacy rights of the individual/customer whose data is being retained which is in direct conflict with the right to erasure as mandated and required by the DPDP Act.

It has also been argued that this violative effect on the privacy of an individual has a chilling on the free speech, a citizen is entitled to under Article 19 of the Indian Constitution.⁷ The fear

⁵ 'India is one of the most cyber-attacked nations. Here's how AI adds another layer to the threat' (*The Indian Express*, 26 August 2026) <AI Cybersecurity Threats: How Prepared Is India to Defend Its Cyberspace?> accessed 1 September 2026.

⁶ *Justice KS Puttaswamy (Retd) & anr v Union Of India & ors* (2017) 10 SCC 1.

⁷ The Constitution of India 1950, art 19(1)(g).

of surveillance, it has been contended, directly impacts freedom of speech and expression as an individual fearing surveillance may fear that he may be prosecuted based on his private data if he opposes the government and thus, he hides away or withholds himself from expressing himself.

However, the superior interest that lies in upholding and maintaining cybersecurity by protecting individual data from hackers, justifies this effect on privacy on grounds of the four-fold test and superiority of national security.

V. A Comparative Analysis of the Indian Legal Framework on Cybersecurity

India's legal framework on cybersecurity is very unique and addresses the local problems effectively, however, to elevate it to bring it at par with global gold standards, India must shift from rigid, compliance-heavy mandates to an outcome based, threat-resilient culture.

For eg., the 6-hour reporting window, though a significant policy instrument in advancing the quick reporting of an incident, is an impractical tool in so as it makes the entire process extremely unreliable. This implies that India's framework might have prioritised swiftness over reliability which makes the entire process extremely speed-oriented as compared to outcome oriented. The priority focus of the lawmakers should be on successfully defusing cyber-attacks, however, a disproportionate focus on time limits is shifting the focus away from the actual cause.

This is not to say that the Indian framework is impotent and ineffective. As per the Global Cybersecurity Index (GCI), India is currently standing in the Tier 1 of the list of countries with a strong legal framework and institutional commitment to strengthen cybersecurity network.⁸ Several technology vendors have even praised, collaborated with, and supported CERT-In's guidelines. Despite various concerns being raised against the legal framework for cybersecurity, it is true to its origin and cause and remains highly respected in the world for network-wide cyber resilience.

India has long regarded Cybersecurity as the cornerstone for a secure digital ecosystem, and that its absence has a significant impact on state prosperity. India's IT sector employs over 5.3

⁸ The Hitavada, 'India among Top 10 in Global Cybersecurity Index' (*The Hitavada*, 1 July 2021) <<https://www.thehitavada.com/Encyc/2021/7/1/India-among-top-10-in-Global-Cybersecurity-Index.html>> accessed 1 September 2026.

million people and is a significant contributor to the national income and thus, it is imperative that its safety is of paramount consideration to the government. Thus, it is no triviality, to say that the Indian framework on cybersecurity, with all its shortcomings addressed, can effectively foster national security and enhance the quality of life of a citizen.