VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CYBER THREAT INTELLIGENCE SHARING IN INDIA — ADEQUACY OF LEGAL FRAMEWORK UNDER THE INFORMATION TECHNOLOGY ACT 2000 AND THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

- K. Anu Priyanka[1]

ABSTRACT

India today faces cyber attacks every single day. Individuals lose money, hospitals get locked out of patient records, banks face intrusions and government systems are constantly under attack. Organisations that experience these attacks gather intelligence about the nature of the attack and the identity of those behind it. When this intelligence is shared with other organisations and with the government each organisation's experience becomes a shield for everyone else. However this sharing is not happening effectively in India today because the existing legal framework does not support or protect it. The Information Technology Act 2000[2] was written in a different era and says nothing specific about how threat intelligence should be shared. The Digital Personal Data Protection Act 2023[3] which came much later has actually made things more complicated because sharing threat intelligence often means sharing personal data and the Act creates legal risk for organisations that do so in good faith. The United States passed a dedicated law for this in 2015[4] and the European Union addressed it through GDPR[5] and the NIS2 Directive.[6] India has done neither. This paper looks at the existing Indian legal framework governing Cyber Threat Intelligence sharing, examines where privacy law and cybersecurity requirements conflict with each other and argues for specific legislative reforms that India must urgently adopt.

[1] PhD Scholar, Tamil Nadu Dr. Ambedkar Law University Chennai

[2]The Information Technology Act, 2000 (Act 21 of 2000).

[3]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

[4]Cybersecurity Information Sharing Act, 2015, Pub. L. No. 114-113, Division N (United States of America).

[5]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation) OJ L 119 (European Union, 2016).

[6]Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) OJ L 333 (European Union, 2022).

Keywords: Cyber Threat Intelligence, CTI Sharing, IT Act 2000, DPDP Act 2023, CERT-In, Cybersecurity Law India.

I. INTRODUCTION

Not a single week passes in India today without a major cyber attack making news. Hospitals lose access to patient records, banks face intrusions, power infrastructure is targeted and government networks come under attack from cybercriminals, hacktivists and state sponsored groups who have identified India's digital infrastructure as a valuable and vulnerable target.

Organisations that face these attacks do not simply suffer and move on. They collect information about what happened, who was responsible and how the attack was carried out and this collected and analysed information is what we call Cyber Threat Intelligence. It tells security teams not just that an attack occurred but who the attacker was, what methods they used and what indicators to watch for next time. When one organisation shares this with others the same attack does not need to happen twice because a threat identified at one bank can protect every other bank in the country if the intelligence is shared in time.

India recorded more than thirteen lakh cybersecurity incidents in 2022 alone according to CERT-In[7] and this number has only grown since then. Despite this India still has no law that specifically governs how organisations should share this intelligence with each other and with the government. The Information Technology Act 2000[8] was not designed for this purpose and the Digital Personal Data Protection Act 2023[9] has introduced privacy obligations that sit very uncomfortably alongside what effective threat intelligence sharing actually requires. In my opinion this gap directly affects India's ability to defend itself against cyber attacks and this paper is an attempt to examine what is missing and what needs to change.

II. UNDERSTANDING CYBER THREAT INTELLIGENCE

There is a difference between knowing that an attack happened and knowing who carried it out, how they did it and what they are likely to do next. Raw data gives you the first. Intelligence gives you all of it. A log file that records an unauthorised access attempt is data. The same log file analysed alongside threat actor profiles, known attack patterns and indicators of compromise from

[7]Indian Computer Emergency Response Team, Annual Report 2022 (Ministry of Electronics and Information Technology, Government of India, New Delhi, 2022).
[8]The Information Technology Act, 2000 (Act 21 of 2000).
[9]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

other organisations becomes intelligence that a security team can actually act on. A security team working only with raw data is always reacting and they find out about attacks after the damage is done. A security team that actually works with properly processed intelligence stands a far better chance of stopping an attack before any damage is done. Getting to that level of intelligence from raw data takes real effort and this is exactly why organisations invest so heavily in the process.

When we take a deeper look at Cyber Threat Intelligence we can understand that it does not serve a single uniform purpose within an organisation. The people at the top of the organisation need a wide view of what threats are out there so they can decide where money should go and what policies need to change. Those on the security team on the other hand need to understand the precise methods that attackers are using today so they know what defences to build. And the team dealing with an attack that is happening at this very moment needs precise and immediate information to stop it. Cyber Threat Intelligence that is properly built and shared serves all three of these needs at once.

Sharing this intelligence makes it far more valuable than keeping it private. Consider a bank that spots a new malware attack and immediately passes that information on to other banks. Every bank that receives it is now protected from the same attack without having to discover it themselves. But this is not what is happening in India today. Organisations that do not know their legal position simply stay quiet. They keep their intelligence to themselves and in doing so they leave every other organisation in the country more vulnerable than it needs to be.

III. CURRENT INDIAN LEGAL FRAMEWORK FOR CYBER THREAT INTELLIGENCE SHARING

No single law in India specifically covers Cyber Threat Intelligence sharing. What exists instead is a collection of statutes and rules each of which was written with something else entirely in mind and which together fail to give any organisation the legal clarity it needs before it can share threat intelligence with confidence.

3.1 Information Technology Act 2000 and CERT-In

Section 70B of the Information Technology Act 2000[10] established the Indian Computer Emergency Response Team as the central government agency for cybersecurity in India and CERT-In is required to collect and analyse information on cyber incidents, send out alerts about threats,

[10]Section 70B, The Information Technology Act, 2000 (Act 21 of 2000).

coordinate responses and publish cybersecurity guidelines.[11]A closer reading of Section 70B reveals that Parliament created the institution but forgot to give it the tools. The section says nothing about what private organisations are permitted to share with CERT-In. It says nothing about what happens to an organisation that shares intelligence in good faith and something goes wrong. It says nothing about how sharing should actually work — whether manually, automatically or through some prescribed platform. Organisations that want to share threat intelligence with CERT-In today are doing so in a legal vacuum and that vacuum is not an accident — it is what Section 70B left behind.

3.2 CERT-In Rules 2013

The CERT-In Rules 2013[12]operationalise Section 70B and require certain categories of cyber incidents to be reported to CERT-In including targeted intrusions, unauthorised access to IT systems, defacement of websites, malicious code attacks, denial of service attacks and attacks on e-governance applications. However the reporting requirements apply only to these specific categories and for everything else organisations can voluntarily report but this voluntary nature means most organisations choose not to report at all because they worry about reputational damage, regulatory scrutiny and competitive harm. From this we can understand that the incomplete picture CERT-In is working with is not accidental. It is the predictable result of building a national cybersecurity intelligence system on voluntary disclosure and the resulting intelligence gaps make it impossible for CERT-In to build a comprehensive understanding of the actual national cyber threat landscape.

3.3 SPDI Rules 2011

The Information Technology Rules 2011 on Sensitive Personal Data[13] govern the collection and processing of sensitive personal data by corporate entities in India and these Rules mandate consent for the collection of personal data, require organisations to maintain a privacy policy, set out data retention requirements and impose restrictions on disclosure and data transfer. In the context of Cyber Threat Intelligence sharing the SPDI Rules create a tension between the privacy obligations of organisations and the need to share threat intelligence that may contain personal data because Cyber Threat Intelligence often includes personal data such as IP addresses, email addresses and

[11]Ministry of Electronics and Information Technology, Government of India, 'CERT-In Functions and Responsibilities' available at https://www.meity.gov.in/content/icert (last visited May 5, 2026).
[12]The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.
[13]The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

other identifiers associated with threat actors and victims. The SPDI Rules say consent is needed before sharing personal data but nobody is going to ask a cybercriminal for permission before sharing information about their attack with CERT-In. This is a contradiction that the existing framework has never addressed and organisations operating in India today have no legal guidance on how to deal with it.

3.4 Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Act 2023[14] is the first time India has had a comprehensive law on data protection. Under Section 4[15] of this Act personal data cannot be processed unless the person it belongs to has given consent or unless the processing falls within one of the specific legitimate uses that Section 7[16] of the Act allows. The trouble is that when organisations share Cyber Threat Intelligence they are almost certainly passing around personal data such as IP addresses, email addresses and account details and none of the legitimate uses in Section 7 specifically say this is allowed. Section 7 does not specifically list Cyber Threat Intelligence sharing as a legitimate use and this gap means organisations sharing threat intelligence in good faith may unknowingly be violating the Act. This conflict between the Act's privacy requirements and the practical necessities of cybersecurity intelligence sharing is a problem that Parliament has not yet found the time to fix.

IV. PRIVACY VERSUS SECURITY CONFLICT IN CYBER THREAT INTELLIGENCE SHARING

The most serious problem in India's legal framework is not just the absence of a dedicated Cyber Threat Intelligence sharing law. What the Digital Personal Data Protection Act 2023[17] has done is introduce a direct and unresolved clash between what privacy law now demands and what effective threat intelligence sharing actually needs organisations to do.

To understand why this conflict exists we only need to look at what threat intelligence actually contains. A phishing email comes from an email address and that address belongs to a person which makes it personal data under the Act.[18] A network intrusion happens from an IP address and that address can also be traced to a person which again makes it personal data. When stolen account

[14]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[15]Section 4, The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[16]Section 7, The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[17]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[18]Section 2(t), The Digital Personal Data Protection Act, 2023 (Act 22 of 2023) defines personal data as any data about an individual who is identifiable by or in relation to such data.

credentials are discovered in a breach investigation those credentials belong to real people and are therefore personal data.

Every piece of intelligence that organisations need to share with each other and with CERT-In to stop the next attack contains this kind of personal data and the DPDP Act 2023 has very specific rules about when processing such data is lawful.[19]

Under the Digital Personal Data Protection Act 2023 processing personal data requires either the consent of the Data Principal or a legitimate use under Section 7[20] and obtaining the consent of a threat actor before sharing their personal data is practically impossible and defeats the purpose of Cyber Threat Intelligence sharing. Section 7 simply does not mention Cyber Threat Intelligence sharing as a permitted use and this means that organisations sharing threat data in good faith are technically in breach of the Act even when they are doing exactly what good cybersecurity practice requires. The United States resolved this directly in 2015 by passing the Cyber Information Sharing Act[21] which says that sharing under that law does not violate any privacy legislation. The European Union did the same through Article 6(1)(f) of GDPR[22] which recognises cybersecurity as a legitimate interest that justifies processing personal data without consent. India's DPDP Act 2023 says nothing about any of this and organisations today are left in an impossible position trying to do their cybersecurity job while staying within the law.

V. COMPARATIVE ANALYSIS

5.1 United States — Cyber Information Sharing Act 2015

America had the same problem India has right now. Companies knew things about the threats they were facing but kept that knowledge to themselves because sharing it felt legally risky. Congress responded in December 2015 with the Cyber Information Sharing Act[23] which did one simple thing very well. It told companies clearly that sharing threat information under this law would not get them sued. Under this Act companies are free to watch over their own networks and pass whatever they find on to the government and to other organisations in their sector.

What makes this Act work is not what it demands from companies but what it protects them from. American companies were staying silent about the threats they faced because they were worried that

[19]Section 4, The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[20]Section 7, The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[21]Cybersecurity Information Sharing Act, 2015, Pub. L. No. 114-113, Division N (USA).
[22]Article 6(1)(f), Regulation (EU) 2016/679 (GDPR) OJ L 119 (2016).
[23]Cybersecurity Information Sharing Act, 2015, Pub. L. No. 114-113, Division N (USA).

sharing threat data would expose them to lawsuits for privacy violations or competition law breaches. This Act took those fears away. A company that shares threat indicators in good faith under this Act cannot be sued for it.[24] Before sharing organisations must strip out any personal information that has nothing to do with the actual threat itself and the Act calls this scrubbing.[25] This scrubbing requirement is what actually makes the whole system function without running into privacy law problems. Beyond this the Act also put in place an automated platform operated through the Department of Homeland Security[26] through which threat indicators move instantly across networks without anyone having to write a report or wait for an advisory.

5.2 European Union — GDPR and NIS2 Directive

Rather than passing a separate law it worked within the GDPR framework through Article 6(1)(f) which allows personal data to be processed without consent when a legitimate interest exists that is strong enough to outweigh the individual's privacy interest. Cybersecurity has been specifically recognised as qualifying under this provision which means a European organisation sharing threat data that contains a threat actor's personal information is acting lawfully under GDPR without needing that person's consent. The NIS2 Directive of 2022 built on this by making incident reporting mandatory across critical sectors and establishing Computer Security Incident Response Teams in each member state with a structured mechanism for sharing threat intelligence across borders.[27]

5.3 What India Can Learn

From the above discussion it is clear that the United States and the European Union offer important lessons for India. Organisations will not share threat intelligence if they face legal risk for doing so and liability protection is therefore not optional but essential. The conflict between privacy law and cybersecurity cannot be left for organisations to resolve themselves and it must be specifically addressed in the law. And the whole system of waiting for organisations to write up incident reports and waiting for CERT-In to turn those into advisories days later simply cannot keep up with threats that spread in minutes. Automated real time sharing is not a nice to have feature but the only approach that can actually work.

[24]Section 106(b)(1), Cybersecurity Information Sharing Act, 2015, Pub. L. No. 114-113 (USA).
[25]Section 104(d)(2)(A), Cybersecurity Information Sharing Act, 2015, Pub. L. No. 114-113 (USA).
[26]Section 105(c)(1)(B), Cybersecurity Information Sharing Act, 2015, Pub. L. No. 114-113 (USA).
[27] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) OJ L 333 (European Union, 2022)

VI. GAPS IN THE INDIAN FRAMEWORK

From everything discussed above it is clear that India's legal framework was designed for a completely different era and nobody has yet gone back to bring it in line with what cyber threat intelligence sharing actually needs today. What follows is not a list of minor technical complaints. They are the reason India's collective cybersecurity defence is weaker than it should be.

India has no dedicated Cyber Threat Intelligence sharing legislation at all. The United States has the Cyber Information Sharing Act 2015[28] and the European Union has the NIS2 Directive[29] while India relies only on the general provisions of the Information Technology Act 2000[30] which say nothing specific about Cyber Threat Intelligence sharing.

Reporting to CERT-In under the CERT-In Rules 2013[31] is largely voluntary and as discussed above this voluntary nature results in serious underreporting that prevents CERT-In from ever having a complete picture of the national cyber threat landscape.

Third organisations that share Cyber Threat Intelligence in good faith have no liability protection under Indian law and the fear of legal liability discourages organisations from participating in intelligence sharing.

The Digital Personal Data Protection Act 2023[32] contains no specific exemption for Cyber Threat Intelligence sharing and organisations today face a direct and unresolved conflict between their privacy obligations under the Act and their cybersecurity responsibilities that they cannot navigate without risking violation of one or the other.

Fifth India has no sector specific Information Sharing and Analysis Centres equivalent to those that operate in the United States[33] for sectors such as banking, healthcare and energy and without these platforms organisations in critical sectors have no structured mechanism to share threat intelligence.

Sixth India has no automated mechanism for real time sharing of threat indicators between CERT-In and private sector organisations and the current framework relies on manual reporting and advisory issuance which is too slow to be effective against rapidly evolving cyber threats.

[28]Cybersecurity Information Sharing Act, 2015, Pub. L. No. 114-113, Division N (USA).
[29]Directive (EU) 2022/2555 (NIS2 Directive) OJ L 333 (2022).
[30]The Information Technology Act, 2000 (Act 21 of 2000).
[31]The Information Technology (CERT-In) Rules, 2013.
[32]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[33]United States Computer Emergency Readiness Team, 'Automated Indicator Sharing' available at https://www.cisa.gov/ais (last visited May 5, 2026).

VII. RECOMMENDATIONS

The six gaps identified above will not fix themselves and each one needs a direct legislative answer.

The Central Government should enact a dedicated Cyber Threat Intelligence Sharing Act. Parliament has the model available in the United States Cyber Information Sharing Act 2015.[34] India's version must give organisations clear legal permission to monitor their own systems, share threat indicators with CERT-In and with each other and must include unambiguous liability protection for good faith sharing because without this protection most organisations will continue to stay silent.

The voluntary reporting system must end. An organisation that suffers a breach today can choose not to tell CERT-In and many do exactly that to avoid scrutiny and reputational damage. Every significant incident must be reported to CERT-In whether or not the organisation wants the scrutiny because a national threat picture built on whatever organisations feel comfortable disclosing is no threat picture at all.

The DPDP Act 2023[35] must be amended to include a specific exemption for Cyber Threat Intelligence sharing. Cybersecurity should be treated as a legitimate use under Section 7[36] with a clear exemption for Cyber Threat Intelligence sharing. Organisations should be allowed to share threat data without consent as long as they strip unnecessary personal information before sharing and use the data only to identify and block threats.

Banking faces different threats from healthcare and healthcare faces different threats from energy and a single generic platform cannot serve all of them. Every critical sector should have its own dedicated Information Sharing and Analysis Centre. Within such a centre organisations in the same sector can share what they know about current threats with each other under CERT-In supervision without worrying that their sensitive internal information will end up in the hands of organisations in entirely unrelated fields.

CERT-In must develop a platform capable of receiving threat indicators from organisations and getting them out to everyone else immediately without waiting for any human to draft a report or put together an advisory. The current manual approach simply cannot move fast enough. India also needs this platform to connect with international counterparts like the US Automated Indicator

[34]Cybersecurity Information Sharing Act, 2015, Pub. L. No. 114-113, Division N (USA).
[35]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[36]Section 7, The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

Sharing system[37] so that Indian organisations are not limited to what they can learn from incidents happening within India alone but can draw on the full picture of what is happening globally.

Individual reforms without coordination are like separate pieces of a puzzle that never get assembled. What India needs alongside all of these legislative changes is a National Cyber Threat Intelligence Strategy[38] a document that tells every government body, every regulator, every critical infrastructure operator and every private company exactly where they sit in the national cybersecurity picture and what they are expected to contribute to it.

VIII. CONCLUSION

After examining everything the honest conclusion is that India's legal framework is actively getting in the way of effective cybersecurity. Section 70B[39] created CERT-In but left it without the legal tools to build a proper national threat picture. The DPDP Act 2023[40] introduced privacy obligations without anyone apparently asking what happens when those obligations collide head on with the requirements of cybersecurity intelligence work. Organisations that want to do the right thing and share what they know find themselves in a legal grey area and most of them resolve that uncertainty by simply not sharing. The result is that India's collective cyber defence is weaker than it needs to be not because of a lack of technical capability but because of a legal framework that was never designed for this purpose.

The United States passed its law in 2015 and the European Union built its framework through GDPR[41] and NIS2[42] because both understood early that without legal clarity organisations will not share and without sharing no country can defend itself. India has allowed a gap of more than a decade to open up on this issue and the cyber threat environment has become considerably more dangerous during that time. Parliament needs to treat the enactment of a dedicated Cyber Threat Intelligence Sharing Act not as something to get around to eventually but as something that needs to happen now.

[37]United States Computer Emergency Readiness Team, 'Automated Indicator Sharing' available at https://www.cisa.gov/ais (last visited May 5, 2026).
[38] National Cyber Security Policy, 2013 (Ministry of Electronics and Information Technology, Government of India). The existing National Cyber Security Policy of 2013 provides a broad framework but does not specifically address Cyber Threat Intelligence sharing.
[39]Section 70B, The Information Technology Act, 2000 (Act 21 of 2000).
[40]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[41]Regulation (EU) 2016/679 (GDPR) OJ L 119 (2016).
[42]Directive (EU) 2022/2555 (NIS2 Directive) OJ L 333 (2022).

With over a billion internet users, a digital economy that is growing faster than almost anywhere else in the world and critical infrastructure that cannot afford to be compromised, India has no time left to wait for the legal framework it needs.

REFERENCES

I. STATUTES

1. The Information Technology Act, 2000 (Act 21 of 2000)

2. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023)

3. Cybersecurity Information Sharing Act, 2015, Pub. L. No. 114-113, Division N (United States of America)

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation) OJ L 119 (European Union, 2016)

5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) OJ L 333 (European Union, 2022)

II. SUBSIDIARY LEGISLATION AND RULES

6. The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013

7. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

8. The National Cyber Security Policy, 2013 (Ministry of Electronics and Information Technology, Government of India)

III. REPORTS AND OFFICIAL DOCUMENTS

9. Indian Computer Emergency Response Team, Annual Report 2022 (Ministry of Electronics and Information Technology, Government of India, New Delhi, 2022)

10. Ministry of Electronics and Information Technology, Government of India, "CERT-In Functions and Responsibilities" available at https://www.meity.gov.in/content/icert (last visited May 5, 2026)

11. Department of Homeland Security and Department of Justice, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (United States Government, Washington D.C., 2016)

12. United States Computer Emergency Readiness Team, "Automated Indicator Sharing" available at https://www.cisa.gov/ais (last visited May 5, 2026)

13. European Union Agency for Cybersecurity, "NIS2 Directive Overview" available at https://www.enisa.europa.eu (last visited May 5, 2026)

IV. JOURNAL ARTICLES

14. PavanDuggal, "Cyber Security Law in India: An Analysis of the Legal Framework" 54 Journal of Indian Law Institute 201 (2012)

15. Nappinai N.S., "Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study" 5 Journal of International Commercial Law and Technology 22 (2010)

16. DebaratiHalder and K. Jaishankar, "Cyber Crime and the Victimization of Women: Laws, Rights and Regulations" 1 Pandora's Box 1 (2011)