Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Regulatory Compliance and Enforcement Gaps under the Cyber Cafe Rules 2011: A Doctrinal Evaluation

Rubaa Sriee T M[a]

[a]Sastra Deemed to be University, Thanjavur, India

Received 10 October 2026; *Accepted* 10 November 2026; *Published* 14 November 2026

Cyber cafes remain a point of public internet access in India, but their open-access character creates risks of cybercrime through anonymity, shared terminals and weak user records. The Information Technology (Guidelines for Cyber Cafe) Rules, 2011 require registration, user identification, log registers and inspection, yet the Rules have not been amended since 2011, even though public access has moved towards Wi-Fi hotspots and mobile internet. This raises serious legal questions about whether the Rules can secure compliance and whether the records they require can support the investigation of cybercrime. This paper examines whether the definition of 'cyber café' in section 2(1)(na) of the Information Technology Act, 2000 corresponds to the obligations in the Rules, and whether registration and inspection under Rules 3 and 7 serve a purpose independent of state Shops and Establishments Acts and police laws. It also analyses whether the user identification and log register records under Rules 4 and 5 meet the admissibility requirements of section 63 of the Bharatiya Sakshya Adhiniyam, 2023, and whether the Rules are consistent with sections 79(2) and 87(2)(zg) of the Act when the only consequence of breach is loss of safe harbour. The study follows a doctrinal methodology, analysing the statutory provisions, the Rules, judicial decisions and supporting legal materials, and it uses no empirical compliance data. Rules 3, 4, 5 and 7 are evaluated qualitatively against five criteria: enforceability, evidentiary reliability, legal validity, privacy proportionality and deterrence. It argues that the Rules set general duties for terminal-based cyber cafes but leave registration and inspection without a time limit or consequence, that their records are unlikely to be reliable evidence, and that loss of safe harbour is too weak a sanction to compel compliance. The gaps are therefore likely to weaken the traceability and investigation of cybercrime committed through cyber cafes, although the study does not measure the actual effect, and the paper proposes reforms.

Keywords: *cyber cafe, intermediary liability, log register, cybercrime, evidentiary value.*

INTRODUCTION: BACKGROUND OF THE STUDY

In the early 1990s, the cyber cafe emerged, giving people internet access to communicate and exchange information globally.[1] The first internet cafe opened in San Francisco in 1991, and the name 'cyber cafe' was coined in London in 1994. Although the internet cafe has largely disappeared in the West, it remains a main source of internet access in many developing countries.[3]

Before the Information Technology Act 2000 (IT Act) was amended in 2008, there was no central law regulating cyber cafes. Rathore and Hinduja argue that the cyber cafe became 'a huge hub for online speculative business and illegal activities with no records of the users by the owner of the cafe.'[2] Some states, such as Karnataka and Tamil Nadu, passed their own laws to protect the public from offences associated with cyber cafes.[3]

The 2008 amendment defined a cyber cafe in section 2(1)(na) as 'any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public', and included cyber cafes within the meaning of 'intermediary' in section 2(1)(w).[4] The Information Technology (Guidelines for Cyber Cafe) Rules 2011 (the Rules) were notified on 11th April 2011 and require cyber cafes to register with a notified agency, verify user identity, install filtering software and retain user records for one year.[5]

Today, people who can't or don't use mobile internet still go to cyber cafes,[6] which suggests that they are now one access point among many, alongside Wi-Fi and mobile phones. In 2024, 19 metropolitan cities recorded 34,958 cybercrime cases, an increase of 3.0 per cent over 2023,

[1] Magda Romanska, 'CAFÉ CULTURE HISTORY, PART 5: THE HISTORY OF THE CYBERCAFÉ' (*ArtsEmerson*, 23 March 2012) <https://artsemerson.org/2012/03/23/cafe-culture-history-part-5-the-history-of-the/> accessed 03 October 2026

[2] Aditi Rathore and Neeraj Hinduja, 'Need for Regulation of Cyber Cafe in India' (2021) 4(2) International Journal of Law Management & Humanities 153 <https://ijlmh.com/paper/need-for-regulation-of-cyber-cafe-in-india/> accessed 03 October 2026

[3] *Ibid* 154–55

[4] Information Technology Act 2000, ss 2(1)(na), 2(1)(w)

[5] Information Technology (Guidelines for Cyber Cafe) Rules 2011, rr 3–7

[6] Sailen Routray, 'The Many Lives and Sites of Internet in Bhubaneswar' (*CIS India*, 21 September 2015) <https://cis-india.org/raw/blog_the-many-lives-and-sites-of-internet-in-bhubaneswar> accessed 03 October 2026

and IT Act offences formed 8.3 per cent (20,587 cases) of Special and Local Laws crimes.[7] The NCRB report does not identify offences committed through cyber cafes and only shows the scale of cybercrime. The law has evolved through Puttaswamy, Shreya Singhal, the 2021 Intermediary Rules and the Digital Personal Data Protection Act 2023, but the Rules have not been amended to reflect these changes.[8]

The Rules were drafted fifteen years ago, and the previous studies have not tested them against these changes. This paper examines whether section 2(1)(na) corresponds to the obligations in the Rules, whether Rules 3 and 7 can secure compliance when they prescribe no time limit or consequence, whether Rules 4 and 5 produce reliable evidence, and whether the Rules are consistent with section 87(2)(zg) read with section 79(2). It then proposes amendments.

LEGAL FRAMEWORK

The IT Act: Section 2(1)(na) of the IT Act defines a cyber cafe as 'any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.'[9] The definition covers any facility regardless of place. A cyber cafe is also an intermediary, because section 2(1)(w) expressly includes cyber cafes.[10]

Section 79(1) protects an intermediary from liability for third-party information. Under section 79(2), the protection is conditional: the intermediary's role must be limited to providing access, must not initiate the transmission, select the receiver or modify the content, and it must observe due diligence and the guidelines the Central Government prescribes.[11] Under section 79(3), the protection is lost if the intermediary helps or induces an unlawful act, or does not expeditiously remove or disable access to material after actual knowledge or government notice.[12] In Shreya Singhal, the Supreme Court read section 79(3)(b) to mean that 'actual knowledge' requires a court order, or a notification by the appropriate government

[7] National Crime Records Bureau, *Crime in India 2024: Snapshots (Metropolitan Cities – >2 million Population)* (Ministry of Home Affairs 2024) xviii, xxi
[8] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1; *Shreya Singhal v Union of India* (2015) 5 SCC 1 [121]; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021; Digital Personal Data Protection Act 2023.
[9] Information Technology Act 2000, ss 2(1)(na), 2(1)(w)
[10] *Ibid* s 2(1)(w)
[11] *Ibid* s 79(1)-(2)
[12] *Ibid* s 79(3)

or its agency, relating to the subjects listed in Article 19(2) of the Constitution.[13] Section 87(2)(zg) allows the Central Government to make rules on the guidelines intermediaries must follow under section 79(2), and the Rules were made under this power.[14] Sections 43 and 66 apply to the person who does the unauthorised act, ordinarily the user and not the cyber cafe.[15] Section 67C requires intermediaries to preserve and retain specified information in the manner the Central Government prescribes.[16]

The Rules: The Information Technology (Guidelines for Cyber Cafe) Rules 2011 (the Rules) were notified on 11 April 2011.[17] Rule 3 requires every cyber cafe to be registered, with a unique number, with an agency notified by the Appropriate Government, but prescribes no time limit for registration and no consequence for non-registration.[18] The agency may follow up with a visit and publish the details on its website.

Rule 4 restricts the user to use a computer until identity is established with a listed document.[19] The cyber cafe must retain the copy for at least one year, may photograph the user with a webcam, and must report to the police if it has reasonable doubt about a user.[24] Rule 5 requires a log register, retained for at least a year, with the user's details and log-in and log-out times.[20] The cyber cafe must send a monthly report as the registration agency directs, and keep backups of websites visited and proxy server logs for a year. Rule 6 deals with the physical layout and the computer resources, such as cubicle height, screen position, minors and filtering software.[21] Rule 7 allows an officer authorised by the registration agency to inspect the cyber cafe and its computers at any time and requires the owner to produce documents on demand.[22] It states no procedure for inspection, and no consequence if the owner refuses.

---

[13] *Shreya Singhal v Union of India* (2015) 5 SCC 1 [121]
[14] Information Technology Act 2000, s 87(2)(zg)
[15] *Ibid* ss 43, 66
[16] *Ibid* s 67C
[17] Information Technology (Guidelines for Cyber Cafe) Rules 2011
[18] *Ibid* r 3
[19] *Ibid* r 4
[20] *Ibid* r 5
[21] *Ibid* r 6
[22] *Ibid* r 7

LITERATURE REVIEW

Nimmi Rangaswamy, 'Regulating India's Digital Public Cultures: A Grey or Differently Regulated Area' (2007): The author in this study undertakes an ethnographic study of urban and peri-urban cyber cafes in Mumbai, Alibaug and Surat, which examines how digital security and privacy form where state regulation is inconsistent and arbitrary.[23] The author finds that owners put business survival before security and place responsibility on banks, vendors and site providers.[30] Cafes were expected to register, seek permission from local bodies and inform the police, but no governing body oversaw how they functioned.[24] The register recorded a name and the mobile number, which the cyber cafe owner treated as sufficient and checked by calling.[25] Owners also called the police-issued filtering software as inadequate, and the firewalls and site blocks were installed more to appease the state than to protect users.[26] The study predates the 2008 amendment to the IT Act 2000 and the Information Technology (Guidelines for Cyber Cafe) Rules 2011, so it cannot test their provisions. Its findings on weak oversight, identity records and owner indifference nonetheless give early empirical support for this study's concern with compliance and enforcement gaps.[27] It does not consider whether such records can serve as reliable evidence in cybercrime investigations.

'Bhairav Acharya (CIS), 'Comments on the Information Technology (Guidelines for Cyber Cafe) Rules (2011)': The author on behalf of the Centre for Internet and Society (CIS) submitted comments to the Committee on Subordinate Legislation of the Fifteenth Lok Sabha, arguing that the rules are poorly drafted and, in parts, invalid.[28] CIS argues that they exceed the delegated power under section 87(2)(zg) read with section 79(2) of the IT Act 2000 (as amended in 2008), which limits the liability of cyber cafes for third-party information, and are therefore ultra vires. It also argues that the definition of 'cyber cafe' under section 2(1)(na) is broad, since it covers airports, restaurants, libraries and public transport offering Wi-Fi,

---

[23] Nimmi Rangaswamy, 'Regulating India's Digital Public Cultures: A Grey or Differently Regulated Area' in Nuray Aykin (ed), *Usability and Internationalization. Global and Local User Interfaces* (Springer 2007) 183
[24] *Ibid* 189
[25] *Ibid* 190
[26] *Ibid* 189-190
[27] *Ibid* 183, 189-191
[28] Bhairav Acharya,' Comments on the Information Technology (Guidelines for Cyber Café) Rules,2011' (*CIS India*) paras 1.1-1.2 <https://cis-india.org/internet-governance/blog/comments-on-the-it-guidelines-for-cyber-cafe-rules-2011 accessed 2 October 2026> accessed 03 October 2026

whereas the Rules were framed only for commercial establishments that mainly sell internet access.[29] On registration, it argues that 'all cyber cafes across India are already registered under applicable local and municipal laws', such as state Shops and Establishments Acts and the relevant Police Acts, yet Rule 3 sets out no clear procedure, no definite timeframe and no consequences for denial of registration.[30] On Rule 4, it criticises the absence of security for stored data, including webcam photographs, and the vagueness of the duty to report to the police.2[31] On Rules 5 and 7, it says that privacy concerns are not addressed and the consequences of an inspection are not stated.[32] CIS's submission centres on validity, constitutionality and privacy. It does not examine how the Rules are enforced, whether the records under Rules 4 and 5 are reliable evidence under Bharatiya Sakshya Adhiniyam 2023 or whether loss of safe harbour under section 79 secures compliance. This study builds on CIS's findings. It analyses the effectiveness of Rules 3 and 7, the evidentiary value of Rules 4 and 5 and the potential consequences of these gaps on cybercrime investigation, and recommends amendments.

Litton, 'The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression' (2015): She argues that India's Central Monitoring System (CMS) will replace 'private censorship' through intermediaries with widespread self-censorship by citizens.[33] She says that cyber cafes are the main source of access for most Indians, but that the government's cyber cafe regulations, which she calls the IT Rules 2011, stunt cyber cafe growth and restrict access.[34] She points to identity verification, one-year retention of identity records and browsing logs, and a definition of 'cybercafe' broad enough to cover airports and hotels.[35] This article treats cyber cafes as a side issue within a broader argument on surveillance, and its claims on cyber cafes are largely uncited.[36] It offers no empirical evidence: the claim that cyber cafes are the main access point is uncited, and the rest rests on

[29] *Ibid* para 3.1
[30] *Ibid* para 4.1
[31] *Ibid* para 4.4-4.5
[32] *Ibid* paras 5.1-7.1
[33] Addison Litton, 'The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression' (2015) 14 Washington University Global Studies Law Review 799, 800, 807 <https://repository.library.washu.edu/cgi/viewcontent.cgi?article=1556&context=law_globalstudies> accessed 03 October 2026
[34] *Ibid* 819
[35] *Ibid*
[36] *Ibid* 805, 819

secondary summaries and a 2008 blog post that predates the Rules.[37] It does not examine section 2 (1)(na), registration, inspection, or the consequences of non-compliance, and it cites the definition to the 'IT Act 2011'. The study fills these gaps. It treats the Rules as a matter of law against section 2(1)(na), the effectiveness of Rules 3 and 7, the evidentiary value of Rules 4 and 5, and consistency with section 87(2)(zg) read with section 79(2) and recommends amendments.

Rathore and Hinduja, 'Need for Regulation of Cyber Cafe in India' (2021): Here the authors note that some states, such as Karnataka and Tamil Nadu, had their own definitions of a cyber cafe before the Rules.[38] They describe the registration process, user identification, the log register, webcam photography, filtering software and the one-year retention of records and monthly reports to the registration agency.[39] They conclude that the present law is inadequate because cybercrime keeps increasing, and they call for a stronger law.[40]

The article is mainly descriptive. The discussion of enforcement is thin and inaccurate. It cites a penalty provision that does not appear to correspond to any provision of the IT Act, and it does not address that the Rules prescribe no penalty, so non-compliance results only in loss of safe harbour protection under section 79. It also does not examine the registration and inspection, which prescribe no time limit and no consequence for non-registration. The study fills these gaps. It analyses the Rules as a matter of law, examining section 2(1)(na) of the IT Act, the effectiveness of Rules 3 and 7, the evidentiary value of Rules 4 and 5, and consistency with section 87(2)(zg) read with section 79(2), and recommends amendments.

Gupta and Srinivasan, 'Evolving Scope of Intermediary Liability in India' (2023): The authors deal with the scope of Intermediary Liability in India from section 79 of the IT Act 2000 (as amended in 2008) and the Intermediary Guidelines 2011 to the 2021 Rules, and conclude that considerable uncertainty remains.[41] They note that, when the IT bill was drafted, stakeholders treated cyber cafes as a special category of intermediary, and that the

[37] *Ibid*
[38] Rathore (n 2) 154-155
[39] *Ibid* 157-158
[40] *Ibid* 158-159
[41] Indranath Gupta and Lakshmi Srinivasan, 'Evolving scope of intermediary liability in India' (2023) 37(3) International Review of Law, Computers & Technology 294, 294–96 <https://doi.org/10.1080/13600869.2022.2164838> accessed 03 October 2026

Delhi Police commissioner suggested user identification and records for later investigation.[42] They say that the rules on the traditional cyber cafes have become redundant because the internet is now more accessible.[43] The article focuses on social media and e-commerce intermediaries and refers only to cyber cafes. Its redundancy claim is a single unsupported sentence, and it does not examine the definition under section 2(1)(na), Rules 3 to 5 and 7, or the consequences of non-compliance. The study fills these gaps by testing whether the Rules remain effective as a matter of law.

STATEMENT OF RESEARCH PROBLEM

The Information Technology (Guidelines for Cyber Cafe) Rules 2011 (the Rules) require registration and inspection (Rules 3 and 7), and user identification and log registers (Rules 4 and 5).[44] They have not been amended since 2011, although public access has moved towards Wi-Fi and mobile phones; laws have changed through Puttaswamy and Shreya Singhal, the 2021 Intermediary Rules and the Digital Personal Data Protection Act 2023.[45]

The research problem is whether the Rules secure compliance and can be enforced. Registration has no time limit, non-registration has no consequence, and the inspection process is not specified.[46] Identity records and logs are to be retained for one year, but no standard governs how they are secured or proved.[47] The only consequence is loss of safe harbour protection under section 79, which may not compel compliance.[48] The Rules regulate users, and so they may go beyond the power in section 87(2)(zg) read with section 79(2).[49] It is therefore unclear whether the Rules help to prevent and investigate cybercrime committed through cyber cafes.

The existing literature does not answer this. Rangaswamy's ethnographic study predates the Rules.[50] The CIS criticised the Rules on validity, overlap with state licensing and privacy, but

[42] *Ibid* 297
[43] *Ibid* 310
[44] Information Technology (Guidelines for Cyber Cafe) Rules 2011
[45] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1; *Shreya Singhal v Union of India* (2015) 5 SCC 1 [121]; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021; Digital Personal Data Protection Act 2023
[46] Information Technology (Guidelines for Cyber Cafe) Rules 2011, rr 3, 7
[47] *Ibid* rr 4, 5
[48] Information Technology Act 2000, s 79
[49] *Ibid* ss 79(2), 87(2)(zg)
[50] Rangaswamy (n 25) 189-90

did not examine enforcement, the evidentiary value of the records, or whether loss of safe harbour secures compliance. Rathore and Hinduja do not analyse registration, inspection or the consequences of non-compliance. Litton and Gupta and Srinivasan paper speaks largely about intermediary liability, and only minor parts deal with cyber cafes. The study addresses the gap. It examines whether the definition in section 2(1)(na) fits the rules, whether registration and inspection secure compliance, whether the records are reliable evidence, and whether the Rules are consistent with the IT Act, and it proposes amendments.

RESEARCH OBJECTIVE

This research studies whether the concept of 'cybercafé' in section 2(1)(na) of the IT Act corresponds to the responsibilities under the Cyber Cafe Rules, 2011 given advances in public internet access. It examines whether the Rules' registration obligation has independent significance alongside State Shops and Establishments Acts and police laws; whether registration and inspection (Rules 3 and 7) form an effective compliance system despite no time limit or consequence for non-registration; whether user identification and log registers (Rules 4 and 5) produce legally valid evidence; and whether the Rules are consistent with s 79(2) and s 87(2)(zg). It then proposes specific amendments to the Rules.

RESEARCH QUESTIONS

1. To what extent does the cyber cafe definition under section 2(1)(na) of the IT Act, 2000 correspond to the obligations imposed by the Cyber Cafe Rules, 2011 with respect to the developments in public internet access points?

- Where the cyber cafe is already registered and licensed under state Shops and Establishments Acts and police laws, does the registration requirement under the Rules serve any independent purpose?
- To what extent do the registration and inspection provisions (Rules 3 and 7) create an effective compliance mechanism given that there is no prescribed time limit and no consequence for non-registration?
- To what extent do the user identification and log register requirements (Rules 4 and 5) provide legally reliable evidence for investigating offences facilitated through cyber cafes?

2. To what extent are the Cyber Cafe Rules, 2011 consistent with section 79(2) and the rule-making power under section 87(2)(zg) of the IT Act, 2000?

- Given that the Rules prescribe no penalty and the only consequence of breach is loss of protection under section 79, to what extent can they secure compliance from cyber cafes?

3. To what extent are the compliance and enforcement gaps under the Rules likely to affect the investigation of cybercrime committed through cyber cafes in India?

SCOPE AND LIMITATION OF STUDY

The study focuses on the laws governing cyber cafes in 'India': sections 2(1)(na), 2 (1)(w), section 87(2)(zg) read with section 79(2) of the IT Act, 2000 and Rules 3,4,5 and 7 of the Cyber Cafe Rules, 2011; Rule 6 is only referred to briefly. Sections 43, 66 and 67C of the IT Act and section 63 of the BSA 2023 are referenced only to the extent they are relevant to the Rules, together with relevant case law and case commentary. The Shops and Establishments Acts and Police laws are referred to only to assess how the current legal regime works and whether the registration requirement in the rules serves an independent purpose. The study relies on the Centre for Internet and Society for the content of the state laws and does not examine each state Act.

However, the findings of the study must be read in light of certain limitations. The Digital Personal Data Protection Act 2023 and the Information Technology (Intermediaries Guidelines) Rules 2011 and NCRB reports are considered as supporting material. For the same reason, the study does not measure the actual effect of the Rules on cybercrime rates or on investigation and conviction outcomes. Statements about the effect of the Rules on investigation are legal assessments of likely effect, not empirical findings; testing them empirically (for example, through Right to Information requests on registration and inspection) is left for future research. Finally, the study suggests amendments.

RESEARCH METHODOLOGY

The study is doctrinal, examining what the law provides and whether it is consistent and effective. The primary sources are the IT Act 2000 (as amended in 2008), the Cyber Cafe Rules 2011, the Bharatiya Sakshya Adhiniyam (BSA) 2023, state Shops and Establishments Acts,

police laws and judicial decisions located through SCC Online. The secondary sources are commentary, journal articles, and government and NCRB reports. The texts are construed using ordinary tools of statutory interpretation, including the presumption against action beyond delegated power. Section 2(1)(na) is compared with the obligations in the Rules, and Rules 3, 4, 5 and 7 are tested for enforceability and evidentiary value.

Rules 3, 4, 5 and 7 are each rated 'Met', 'Partly met', 'Not met' or 'Not applicable' against five criteria: (1) enforceability (time limit, procedure, sanction); (2) evidentiary reliability (section 63 of the BSA); (3) legal validity (sections 87(2)(zg) and 79(2)); (4) privacy proportionality (the Puttaswamy test); and (5) deterrence. The ratings are the author's doctrinal judgments, summarised in Table 1.

ANALYSIS AND FINDINGS

Does the definition of a cyber cafe correspond to the obligations in the Rules? (Q1): The definition in section 2(1)(na) is wide enough to cover Wi-Fi hotspots, gaming cafes and co-working spaces, but Rules 4 to 6 assume a cyber cafe with terminals.[51] A Wi-Fi establishment cannot verify every person who connects a personal device under Rule 4, and a co-working space cannot keep the terminal-wise log register under Rule 5.[52] The definition and the obligations therefore align on paper but not in practice.

Does registration under Rule 3 serve an independent purpose? (Q1(a)): Rule 3 asks for the name, address, ownership and type of service of the cyber cafe, and CIS argues that these details are already given under the state Shops and Establishments Acts and police laws, so another layer of registration is unwarranted.[53] The only new features are the unique registration ID and its publication on the agency's website, which help traceability but do not regulate the cyber cafe. This study relies on CIS for the content of the state laws and does not examine each state Act.

Do Rules 3 and 7 create an effective compliance mechanism? (Q1(b)): Registration depends on the Appropriate Government notifying a registration agency, and inspection under Rule

[51] Information Technology Act 2000, s 2(1)(na); Information Technology (Guidelines for Cyber Cafe) Rules 2011, rr 4–6
[52] Information Technology (Guidelines for Cyber Cafe) Rules 2011, rr 4, 5
[53] Acharya (n 30) paras 4.1–4.3

7 is possible only through an officer that agency authorises.[54] CIS reported that most states had not notified an agency, so there was no registration and no inspection, though this evidence is from 2011 and no current data was found. The Rules prescribe no time limit for registration or inspection, and Rule 7 states no procedure and no consequence if the owner refuses.

Do Rules 4 and 5 provide legally reliable evidence? (Q1(c)): An electronic record produced as a computer output needs the certificate under section 65B of the Indian Evidence Act 1872, now section 63 of the BSA, 2023.[55] Rule 5 allows an online log register with a digital signature but sets no standard for authenticity, tamper-evidence or certification for court, so a small cyber cafe with a paper register is unlikely to meet this threshold. A copy of an identity document also shows only that a document was produced, not that the person who produced it is the person named in it, so on a shared terminal it is weak proof of the user.[56]

Are the Rules consistent with the IT Act, and can they secure compliance without a penalty? (Q2 and Q2(a)): The Rules were created under Section 87(2)(zg) read with Section 79(2) under the central government power, which deals with third-party information and due diligence.[57] Rules 4 and 5 regulate the identification and logging of the person at the terminal, and CIS argues that Rules going beyond the information and communication links of users are ultra vires. In Shreya Singhal, the Supreme Court read down section 79(3)(b) so that the duty arises only on a court order or a government notification under Article 19(2), which shows that the section is tied to content.[58] The argument has force, but no decision on the validity of the Rules has been found, so it remains an argument. The Rules prescribe no penalty, and the penalty provisions in the IT Act are not tied to them, so the main consequence of breach is loss of safe harbour, which arises only if the cyber cafe is sued. An operator who is never sued has no reason to comply.[59]

How do the gaps likely to affect the investigation of cybercrime? (Q3): They are likely to weaken traceability and raise privacy concerns. Where registration is not enforced,

[54] Information Technology (Guidelines for Cyber Cafe) Rules 2011, rr 3, 7
[55] Indian Evidence Act 1872, s 65B; Bharatiya Sakshya Adhiniyam 2023, s 63; *Anvar PV v PK Basheer and Ors* (2014) 10 SCC 473; *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal and Ors* (2020) 7 SCC 1
[56] Information Technology (Guidelines for Cyber Cafe) Rules 2011, rr 4, 5
[57] Information Technology Act 2000, ss 79(2), 87(2)(zg)
[58] *Shreya Singhal v Union of India* (2015) 5 SCC 1 [121]
[59] Information Technology Act 2000, ss 43, 45, 67C

inspection is untimed, and records are weak, an investigator has fewer factors to rely on, and Rathore and Hinduja say that without records of users, hackers are hard to trace. The NCRB figures show the scale of cybercrime but do not identify offences committed through cyber cafes. Rules 4 and 5 also compel one-year retention of identity documents, photographs and logs, and CIS criticised the lack of security standards for the stored data. In the Puttaswamy case, a restriction on privacy needs legality, a legitimate aim, proportionality and safeguards, and the Rules are doubtful on the privacy parts.[60] This is a legal assessment of likely effect; without compliance or case data, the study cannot measure the actual effect.

Table 1: Qualitative assessment of Rules 3, 4, 5 and 7

Rule	Enforceability	Evidentiary Reliability	Legal Validity	Privacy Proportionality	Deterrence
Rule 3 (Registration)	**Not Met** No time limit or consequence; agency often not notified	**Not Applicable**	**Partly Met** No ruling on validity; CIS argues invalid in parts	**Met** Collects business details, not user data	**Not Met** Only loss of safe harbour, and only if sued
Rule 4 (User ID)	**Partly Met** Duties stated, but reporting duty vague and no sanction	**Not Met** ID copy does not prove who used the terminal	**Partly Met** May exceed s 87(2)(zg); untested	**Not Met** One-year retention of IDs and photographs; no security standard	**Not Met** Only loss of safe harbour, and only if sued
Rule 5 (Log Register)	**Partly Met** Register and reports	**Not Met** No standard for	**Partly Met**	**Not Met**	**Not Met** Only loss of safe

[60] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1

	required, but no standard of proof and no sanction	authenticity or s 63 certificate	May exceed s 87(2)(zg); untested	One-year logs; no security standard	harbour, and only if sued
Rule 7 (Inspection)	**Not Met** No procedure; no consequence if owner refuses; needs notified agency	**Not Applicable**	**Partly Met** No ruling on validity; CIS argues invalid in parts	**Not Met** Inspection at any time; privacy not addressed	**Not Met** Only loss of safe harbour, and only if sued

Note: Ratings are the author's qualitative, doctrinal judgments based on the analysis in sections 1 to 6; they are not empirical measurements. 'Not applicable' means the criterion does not bear on the Rule.

CONCLUSION

This study assesses whether the Cyber Cafe Rules 2011 secure compliance and support the investigation of cybercrime. It finds that they do so only to a limited extent. The definition in section 2(1)(na) is wide, but Rules 4 to 6 assume a terminal-based cyber cafe. Rules 3 and 7 set no time limit or consequence, and the records under Rules 4 and 5 may fail the requirement in section 63 of the BSA 2023. Rules 4 and 5 may exceed the delegated power, and loss of safe harbour is a weak sanction. On the five-criteria assessment in Table 1, none of Rules 3, 4, 5 and 7 is fully met: each fall short on at least one criterion, and deterrence is not met for any of them. The gaps are therefore likely to weaken traceability and the investigation of cybercrime committed through cyber cafes, although the study, being doctrinal, cannot measure the actual effect. The study recommends amendments to the Rules.

RECOMMENDATIONS

Proposed Amendments to the Rules –

Rule 2 - As Rule 2 only incorporates the definition under Section 2(1)(na), it needs amendment to classify establishments for functional application of the Rules - (a) terminal-based cyber cafes (full compliance with Rules 4-6); (b) access-point providers like Wi-Fi-only cafes, gaming lounges and co-working spaces (router-level authentication and session logs); and (c) incidental providers like hotels (registration exempt, log retention only).

Rule 3 - Registration should be issued on production of an existing Shops and Establishments registration and police licence, and deemed granted after 30 days.

Rules 3 and 7 - The Appropriate Government should notify a registration agency within six months. Rule 7 should require an annual inspection, a written protocol and recorded reasons.

Rules 4 and 5 - Rule 4 should accept digital identity, with webcam photographs only where none is produced. Rule 5 should require an electronic, tamper-evident register that supports the section 63 certificate, produced on written request for a specific investigation.

Delegated Power - Rules 4 and 5 should be redrafted as due diligence duties under section 79(2)(c), with Puttaswamy safeguards: a stated purpose, security standards and deletion after retention.

Consequence - The Rules should state that compliance with Rules 3 to 5 is part of due diligence, and prescribe a tiered procedure - notice, warning, and post-hearing suspension of registration.