



A Quantitative Investigation of Cyber Offences Under the Information Technology Act in India: State-wise Patterns and Marketing Impact

¹Dr Prasanta Chatterjee Biswas, ²Dr Amar Vijay Gandhi, ³Zenab Hatim Trivedi

¹Professor, CDOE, Faculty of Management Studies, Parul University, Vadodara, Gujarat, India

²Assistant Professor, Darshan Institute of Management, Darshan University, Rajkot, Gujarat, India

³Assistant Professor, Darshan Institute of Management, Darshan University, Rajkot, Gujarat, India

Email – ¹pra_chat_bis@yahoo.com, ²amarvgandhi@gmail.com, ³zainabtrivedi18@gmail.com

Abstract: India's digital landscape has undergone unprecedented expansion, bringing with it an alarming rise in cyber offences. This paper provides a quantitative analysis of cybercrime patterns across Indian states, examining offences registered under the Information Technology (IT) Act, 2000, and their cascading implications on consumer trust and marketing ecosystems. Drawing on data from the National Crime Records Bureau (NCRB) Crime in India reports (2019–2024), the study employs the Kruskal-Wallis non-parametric test to assess regional variation in cybercrime distribution. Key findings reveal a 17% surge in registered cybercrimes in 2024 (reaching 1,01,928 cases), with Telangana, Karnataka, and Maharashtra emerging as the most affected states. The marketing implication is critical: digital fraud erodes consumer trust, undermines participation in e-commerce, and inflates cybersecurity compliance costs for businesses. The paper concludes with policy recommendations to strengthen India's cyber governance and restore market confidence.

Keywords: Cybercrime, IT Act, Kruskal-Wallis Test, Marketing Trust, Digital Fraud, NCRB, Consumer Behaviour.

1. INTRODUCTION

India's internet user base has crossed 900 million as of 2024, making it one of the world's largest digital economies. This rapid penetration, however, has created fertile ground for cybercriminals. The Information Technology Act, 2000 (IT Act) — amended significantly in 2008 — provides the primary legal framework for addressing digital offences, covering tampering with computer source documents (Section 65), computer-related offences (Section 66), identity theft (Section 66C), cyber terrorism (Section 66F), and the publication of obscene content (Sections 67–67B), among others. The National Crime Records Bureau (NCRB) data reveal a trajectory of escalating cybercrime: from 44,546 cases in 2019 to 52,000 in 2021, 86,420 in 2023, and 1,01,928 in 2024 — a staggering 129% increase over five years. This surge has profound implications not just for law enforcement, but for commerce, marketing, and digital trust. Cyber fraud now accounts for over 72% of all cybercrime motives (NCRB, 2024), directly affecting consumer behaviour in online marketplaces.

Legislators and marketers alike must understand how and why cybercrimes manifest across regions and legislative categories to formulate effective deterrents (Holt, Burruss & Bossler, 2015). This paper bridges that gap by statistically profiling state-wise cyber offences and drawing actionable marketing implications.

2. LEGAL FRAMEWORK: IT ACT 2000 AND AMENDMENTS

The IT Act, 2000, enacted as India's first comprehensive cyber law, established civil and criminal liability for digital offences and created a regulatory regime for certifying authorities. The Information Technology (Amendment) Act, 2008 significantly broadened its scope, adding new offences such as cyber terrorism (Section 66F), sending offensive messages (Section 66A, later struck down), violation of privacy (Section 66E), and intermediary liability provisions (Section 79).



Key offences under the IT Act relevant to this study include:

- Section 65: Tampering with computer source documents
- Section 66: Computer-related offences (hacking, data theft)
- Section 66C: Identity Theft
- Section 66D: Cheating by personation using computer resources
- Section 66E: Violation of Privacy
- Section 66F: Cyber Terrorism
- Sections 67, 67A, 67B: Publication of obscene/sexually explicit content
- Section 84B/84C: Abetment and attempt to commit offences

Complementary IPC provisions — such as Sections 420 (fraud), 354D (cyber stalking), and 506 (criminal intimidation) — are frequently invoked alongside the IT Act, broadening the prosecutorial framework.

3. CYBERCRIME TRENDS IN INDIA: 2019–2024

The NCRB's Crime in India series documents a consistent and steep upward trajectory in cybercrime registrations across India. Total cybercrime cases grew from 44,546 in 2019 to 1,01,928 in 2024, marking a 17.9% year-on-year increase from 2023 to 2024 alone. The cybercrime rate per lakh population rose from 6.2 in 2023 to 7.3 in 2024.

3.1 DOMINANT OFFENCE CATEGORIES (2024)

Cyber fraud remains the overwhelming driver, accounting for 72.6% of cybercrime cases (73,987 cases) in 2024. Other significant categories include:

- Sexual exploitation: 3,190 cases
- Extortion (including digital arrest scams): 2,536 cases
- Causing disrepute: 2,231 cases
- Personal revenge: 1,850 cases

A major emerging trend in 2024 was the rise of 'Digital Arrest' frauds, where impersonators posing as law enforcement agencies (CBI, Customs, or Police) coerce victims over video calls to extort money. AI-enabled phishing, voice cloning, and deepfake-assisted identity fraud have further sophistication the cybercrime landscape.

3.2 STATE-WISE DISTRIBUTION

State-wise, Telangana recorded the highest cybercrime cases in 2024 (27,230 cases), representing a nearly 50% rise from 2023, followed by Karnataka (21,003 cases) and Maharashtra. These states, characterised by high IT penetration and digital transaction volumes, continue to bear a disproportionate share of the cybercrime burden. In the 2019 data (the study's baseline), Karnataka led with 12,020 total cybercrimes (26.9% of all India's cases), followed by Uttar Pradesh, which dominated under specific IT Act sections.

Among northern states, Haryana recorded 751 cybercrime cases in 2023 (the highest in its zone), while Uttar Pradesh dominated multiple IT Act sections — contributing 82.4% of Section 66 cases and 86.1% of ransomware offences (2019 data). In the North-East, Assam remains the primary contributor with 2,231 total cybercrimes. Nearly 35,000 cybercrime cases were registered in metro cities in 2024 alone.

4. STATISTICAL ANALYSIS: REGIONAL VARIATION

To test whether cybercrime distributions across India's geographic zones differ significantly, the Kruskal-Wallis H-test — a non-parametric alternative to one-way ANOVA — was applied to state-level crime data grouped into six zones: North, East, South, Central, North-East, and West.

4.1 HYPOTHESES

H₀: The mean ranks of cybercrime cases across all zones are equal (no significant regional difference).

H₁: At least one zone differs significantly from the others.



4.2 TEST RESULTS

The Kruskal-Wallis test yielded a test statistic $H = 6.678$ ($p = 0.246$), which falls within the 95% acceptance region. The overall null hypothesis cannot be rejected, indicating no statistically significant difference in cybercrime distribution across all six zones at the 5% level. However, pairwise multiple comparison tests reveal important nuances:

- North Zone vs. North-East Zone ($p = 0.028$): Statistically significant — rejects H_0
- East Zone vs. North-East Zone ($p = 0.041$): Statistically significant — rejects H_0
- All other pairwise comparisons ($p > 0.05$): Fail to reject H_0

The statistical significance observed between the North/East zones and the North-East zone reflects the outlier concentration of cybercrime in Assam (2,231 cases) within the North-East, contrasting sharply with comparatively lower-crime states such as Sikkim (2 cases), Nagaland (2 cases), and Manipur (4 cases). This disparity underscores the role of digital infrastructure penetration, urban density, and enforcement capacity in shaping cybercrime geography.

5. MARKETING IMPLICATIONS OF CYBERCRIME

The proliferation of cybercrime in India has measurable and multidimensional consequences for the marketing environment, affecting consumer trust, purchasing behaviour, brand equity, and the cost of doing business digitally.

5.1 EROSION OF CONSUMER TRUST

Cybersecurity breaches and fraud incidents significantly erode consumer trust in digital commerce. A 2023 YouGov survey found that 47% of Indian respondents reported a friend or family member losing money to an online scam. High-profile data breaches — such as the 2024 breach of Signzy (a digital identity verification company serving 600+ financial institutions) — illustrate how systemic vulnerabilities in third-party providers can compromise consumer confidence at scale. Research confirms that digital trust tenets are now “nearly as important as cost and delivery time” in consumer purchase decisions (PwC Digital Trust Insights, 2024).

5.2 IMPACT ON E-COMMERCE AND DIGITAL MARKETING

India's e-commerce sector, valued at over \$70 billion in 2024 and growing at 20%+ annually, faces headwinds from rising cybercrime. The National Payments Corporation of India reported a 71% increase in UPI-linked fraud in 2023, which has made many first-time digital users reluctant to transact online. The Indian Cyber Crime Coordination Centre (I4C) projects India may lose over ₹1.2 lakh crore to cyber fraud in 2025, averaging ₹1,000 crore per month — losses that directly impair digital advertising ROI, customer lifetime value, and brand loyalty.

Phishing attacks in the BFSI sector surged 175% in 2024 compared to 2023 (Digital Threat Report 2024). AI-driven deepfakes and executive impersonation scams are bypassing traditional security measures, forcing organisations to invest heavily in cyber defence — costs that are ultimately passed to consumers or absorbed as reduced marketing budgets.

5.3 REGULATORY COMPLIANCE AND BRAND RESPONSIBILITY

The Digital Personal Data Protection Act (DPDP), 2023, has introduced new accountability standards for organisations handling consumer data. Non-compliance — or high-profile breach incidents — results not only in regulatory penalties but reputational damage that can take years to remedy. Marketers are increasingly required to embed cybersecurity as part of their brand promise: 38% of executives surveyed by PwC identified harmonising data protection laws as critical to future revenue growth.

6. CONCLUSION AND RECOMMENDATIONS

India's cybercrime landscape has undergone a dramatic transformation over the past five years, with registered cases surpassing 1,01,928 in 2024 and projected losses set to exceed ₹1.2 lakh crore in 2025. The statistical analysis confirms that while overall regional variation is not statistically significant at the aggregate level, specific zone pairs (particularly involving the North-East) exhibit meaningful differences, reflecting disparities in digital infrastructure and enforcement capacity.

For the marketing community, the implications are clear: cybercrime is no longer merely a technology risk — it is a marketing risk that undermines brand trust, suppresses digital adoption, and inflates the cost of customer acquisition and retention. The following policy and strategic recommendations are proposed:



- Strengthen enforcement of the IT Act and DPDP Act, particularly for financial fraud, identity theft (Section 66C), and AI-enabled crimes.
- Invest in cybersecurity awareness campaigns targeting first-time internet users and senior citizens, who are disproportionately victimised.
- Integrate ‘Security by Design’ into India’s digital public infrastructure (UPI, Aadhaar) through Zero-Trust Architectures.
- Establish a UN-backed global convention on cybercrime to address cross-border jurisdiction gaps.
- Marketers should prioritise digital trust as a brand equity metric, transparently communicating data protection practices to consumers.

With over 900 million internet users and rapid digital financial inclusion, India stands at a critical juncture. Translating legislative intent into effective enforcement, while building consumer confidence in digital channels, will be decisive for sustainable digital economic growth.

REFERENCES:

1. Catherine Friend et al. (2020). Fighting Cybercrime: A Review of the Irish Experience. *International Journal of Cyber Criminology*, 14(2), 383–399.
2. Holt, T., Burruss, G. & Bossler, A. (2015). *Policing Cybercrime and Cyberterror*. Carolina Academic Press.
3. Jigar, S. (2016). A Study of Awareness About Cyber Laws of Indian Youth. *International Journal of Trend in Scientific Research and Development*, 1(1), 10–16.
4. Lee, G., & Sanchez, M. (2018). Cyber Bullying Behaviors, Anonymity and General Strain Theory. *International Journal of Cyber Criminology*, 12(1), 84–96.
5. Mittal, S., & Sharma, P. (2017). A Review of International Legal Framework to Combat Cybercrime. *International Journal of Advanced Research in Computer Science*, 8(5), 1372–1374.
6. Mohammed Shamiulla Arab (2020). Global Surge in Cybercrimes — Indian Response and Empirical Evidence. *International Journal of Cyber Criminology*, 14(2), 497–507.
7. National Crime Records Bureau (NCRB). (2019–2024). *Crime in India*. Ministry of Home Affairs, Government of India. www.ncrb.gov.in
8. PwC India. (2024). *Global Digital Trust Insights Survey 2024*. PricewaterhouseCoopers.
9. Sanjna Agarwal & Dr Adeel Maqbool. (2026). Impact of Cybercrime on the E-Commerce Industry in India. *Well Testing Journal*, 35(S1), 118–138.
10. Seid Mahdi Seidzadeh Sani & Zahra Farhadi Alashti. (2020). Relationship between Religious Identity and Cyberbullying. *International Journal of Cyber Criminology*, 14(2), 508–522.
11. Udris, R. (2016). Cyber Deviance among Adolescents and the Role of Family, School and Neighbourhood. *International Journal of Cyber Criminology*, 10(2), 127–146.