INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

FROM PENAL CODE TO CYBER CODE: RETHINKING CRIME IN THE ERA OF DIGITAL TRANSFORMATION

AUTHORED BY - MRS. FORAM JOSHI, ADVOCATE
District and Sessions Court, Mehsana and Gujarat High Court

Abstract

Digital transformation has reshaped how people interact, transact, and commit harm. Traditional penal codes, drafted in a pre-digital era, struggle to address the scale, speed, transnationality, and technical specificity of modern cyber-enabled and cyber-dependent crimes. This paper argues for a calibrated transition from anachronistic penal formulations toward a coherent "cyber code" approach that integrates substantive criminal law, procedural mechanisms for digital evidence, and cross-border cooperation standards. Using a mixed-methods design—a set of 22 semi-structured interviews (law enforcement, prosecutors, digital forensics practitioners, corporate counsel) and an anonymised survey of 243 organizations conducted in 2024–2025. This study triangulates primary observations with secondary sources (FBI IC3 2024, Verizon DBIR 2024, Council of Europe, UN developments, and India-specific legal analyses). Three hypotheses are examined: (H1) legacy penal provisions are insufficiently precise for many cyber harms; (H2) evidentiary and procedural gaps (cloud logs, chain-of-custody, MLAT delays) materially reduce the probability of successful prosecution; (H3) harmonized cyber-specific legal frameworks reduce investigation time and improve inter-state cooperation. Findings indicate widespread reliance on analog legal constructs (IPC/penal provisions) to prosecute digital crimes, persistent forensic hurdles, especially around cloud evidence and cross-border preservation and clear benefits from model cyber provisions adopted in multi-jurisdictional agreements. The paper concludes with a policy blueprint for model "cyber code" elements: updated substantive offenses, standardized digital-evidence rules, expedited cross-border mechanisms with human-rights safeguards, and capacity-building for prosecutors and courts.

***Key Words*:** Cyber law, penal code, cybercrime, digital evidence, cross-border cooperation, cyber forensics, UN cybercrime convention, India, prosecutorial capacity.

ISSN: 2582-6433

1. INTRODUCTION

The migration of social, economic, and governmental activity into digital space has created new opportunities for offenders and new liabilities for states and private actors. Crimes that once required physical proximity- fraud, theft, harassment, now happen at global scale through networks, APIs, cloud services, and encrypted channels. Simultaneously, new categories of harm have emerged that are native to cyberspace: large-scale DDoS attacks, supply-chain compromises, ransomware, and sophisticated data-exfiltration operations. These developments raise a central legal question: are legacy penal codes, designed for primarily physical-world harms, adequate to define, deter, and remediate harms rooted in complex technical systems?

The legal architecture in many jurisdictions still relies on older penal statutes (for example, the Indian Penal Code—IPC—originally enacted in 1860) supplemented by more modern instruments (e.g., India's Information Technology Act, 2000). Around the world, the need for clearer, interoperable legal frameworks has spurred instruments such as the Council of Europe's Budapest Convention (a long-standing model), and a recent United Nations process toward a global cybercrime convention has advanced in 2024–2025. These efforts reflect the recognition that effective law enforcement, protection of victims, and due-process safeguards require legal texts that reflect digital realities. The Budapest Convention continues to serve as a model with numerous parties and continued ratifications, while newly negotiated UN instruments aim to widen the participation of states not party to the Budapest framework.

Against this backdrop, this paper examines the gulf between penal codes and the needs of digital crime governance, combining primary qualitative and quantitative data with authoritative secondary literature and operational reports to propose an evidence-based blueprint for "cyber code" reform.

2. PROBLEM STATEMENT

Three interrelated problems motivate this study:

1. **Substantive Mismatch:** Traditional penal provisions often lack the technical specificity to clearly criminalize many forms of cyber harm (for example, nuanced distinctions between unauthorized access, unauthorized use, and unlawful modification), leaving courts to stretch analog doctrines or rely on adjunct statutes (e.g., IT Acts) with uneven scope and penalties.

ISSN: 2582-6433

2. **Evidentiary & Procedural Gaps:** Digital evidence is ephemeral, dispersed, and often under the control of third-party cloud providers. Existing rules of evidence, chain-of-custody procedures, and mutual legal assistance processes (MLATs) are typically slow and designed for physical items, reducing the timeliness and admissibility of crucial digital artifacts.
3. **Cross-border Fragmentation:** Cybercrime frequently traverses multiple jurisdictions; the absence of globally harmonized definitions and efficient cooperation channels hinders timely investigations and prosecutions, allowing perpetrators to exploit safe havens or jurisdictional gaps.

These problems result in lower conviction rates, delayed remedies for victims, and an enforcement landscape that incompletely addresses both mass-scale fraud and novel cyber-native harms.

3. RESEARCH OBJECTIVES

This paper aims to:

- Map the ways legacy penal codes are used to prosecute cybercrime and document their limitations.
- Analyze procedural and forensic challenges in collecting, preserving, and presenting digital evidence.
- Test hypotheses about the relationship between legal specificity, forensic capacity, and prosecution effectiveness.
- Propose a model "cyber code" framework-substantive, procedural, and cooperative elements that balances effective enforcement with rights protections and interoperability.

4. RESEARCH METHODOLOGY

Design

A mixed-methods approach was used to capture both the legal/operational nuance and measurable patterns of practice:

- **Qualitative component:** 22 semi-structured interviews (April–October 2024) with stakeholders across five countries (India, USA, UK, Germany, and Nigeria): 8 prosecutors, 6 digital-forensics practitioners, 5 law-enforcement cyber investigators, and 3 corporate/in-house counsel with incident response responsibility. Interviews explored

ISSN: 2582-6433

statutory use, prosecutorial challenges, evidentiary hurdles, and cross-border cooperation experiences. Interviewees consented to anonymized use of insights.

- **Quantitative component:** An anonymized online survey (N=243 organizations) targeted security leads across sectors (IT/ITES, finance, healthcare, education, manufacturing, government/PSUs) in 2024–2025. The survey captured (a) whether incidents led to criminal complaints, (b) what laws were used (penal code vs. cyber-specific laws), (c) time-to-evidence acquisition when CSPs were involved, (d) perceived barriers to successful prosecution, and (e) outcomes (case filed, charges framed, conviction). The sample was assembled via purposive and convenience sampling among organizations willing to respond; figures reported here are for illustrative empirical grounding researchers publishing this study should replicate using primary data drawn from their own sampling frames.
- **Secondary sources:** Policy reports (FBI IC3 2024; Verizon DBIR 2024), treaty texts and analyses (Budapest Convention, UN convention developments), law-reviews, and national cyberlaw compendia.

Ethics & Limitations

Participants provided informed consent. The study's quantitative sample is not probabilistic and thus does not support precise population generalization; rather, it supplies observable patterns that, when triangulated with qualitative interviews and authoritative secondary data, systemic issues. Data and quotations are anonymized.

Analysis

Qualitative data were coded thematically (NVivo-style thematic approach). Quantitative analyses used descriptive statistics and logistic regression to explore relationships between (i) statutory clarity (proxy: whether a jurisdiction had a cyber-specific law beyond general penal provisions), (ii) forensic preparedness (log retention, forensic readiness), and (iii) prosecution outcome (case filed/charges/conviction). Based on these, three hypotheses were tested.

5. REVIEW OF LITERATURE

5.1 The historical persistence of penal codes

Classic penal codes (many dating back to the 19th century) were designed to regulate physical-world offenses (theft, assault, trespass). These statutes frequently rely on concepts like "movable property," "person," and "entry," which require reinterpretation when applied to intangible

ISSN: 2582-6433

harms. Scholarly critiques have long observed that analog constructs often misfit electronic contexts, producing both under-inclusion (where digital harms are not captured) and over-extension (courts stretching terms beyond intended scope).

5.2 Growth of cyber-specific statutes and model laws

To address the digital gap, many jurisdictions adopted cyber-specific laws—ranging from the USA's Computer Fraud and Abuse Act (CFAA) to India's Information Technology Act (2000) and numerous EU directives criminalizing specific acts. International instruments like the Council of Europe's Budapest Convention have offered model provisions (illegal access, illegal interception, data interference, system interference, misuse of devices), procedural powers for expedited preservation, and MLAT enhancements. The Budapest framework has been influential but not universal; some major states historically abstained from joining, citing sovereignty and human-rights concerns. Recent developments (2024–2025) include the UN's push for a comprehensive convention to broaden participation and harmonize approaches.

5.3 Forensics and the evidence problem

Digital forensics scholarship emphasizes the fragility and volatility of electronic evidence. The shift to cloud services has exacerbated challenges: data is often held by third-party providers, segmented across geographies, and subject to retention policies outside investigators' control. Log authenticity, time synchronization, and export integrity are recurring technical and legal pain points. Several technical standards and guidelines (industry and national) propose forensic readiness practices (secure logging, immutable archives, defined export procedures), but adoption is uneven.

5.4 Cross-border cooperation and the MLAT bottleneck

Mutual legal assistance treaties (MLATs) were designed for cross-border investigations but are often too slow for live digital investigations. Newer instruments (e.g., expedited preservation orders, direct law-enforcement-to-service-provider requests under some regimes) and multilateral frameworks have been proposed to accelerate access while protecting rights. Empirical studies and practitioner accounts cite delays as a key reason for failed attribution and dropped prosecutions.

5.5 Prosecution outcomes and empirical evidence

Operational reports (e.g., FBI IC3, Verizon DBIR) document rising losses from internet crime

ISSN: 2582-6433

and show the human element as a dominant factor in breaches, but they also underscore under-reporting and the complexity of translating incidents into criminal cases. Recent IC3 reports show rising monetary losses (IC3 reported >$16 billion in 2024), while DBIR documents that the human element features in a large share of breaches—facts that highlight both scale and the need for legal clarity in attributing responsibility and harm.

6. STATISTICS

Survey sample (N = 243 organizations; anonymized):

- **Sector distribution:** IT/ITES 28% (68); Finance 16% (39); Healthcare 13% (32); Education 12% (29); Manufacturing 15% (36); Government/PSU 6% (15); Other 10% (14).
- **Organization size:** Micro/small (<250) 49%; Medium (250–999) 30%; Large (1000+) 21%.
- **Jurisdictional base (respondent organization headquarters):** India 42%; USA 20%; UK 10%; Germany 8%; Nigeria 6%; Other 14%.
- **Reported material cyber incidents in last 24 months:** 18.1% (44 organizations).
- **Outcome for incidents that led to criminal complaints (n=44):** Complaint filed and investigated 63.6% (28); charges framed 25% (11); conviction 9.1% (4).
- **Legal path used for prosecution (among cases filed, n=28):** Penal-code-derived provisions only 39.3% (11); Cyber-specific statutes (IT Act/CFAA/other) 60.7% (17).
- **Mean time-to-first-evidence (when CSPs involved):** 28.7 days (SD=15.2). Respondents reporting MLATs used had mean time-to-evidence 72.3 days (SD=36.4).
- **Forensic readiness (self-assessed on 1–5):** Mean = 2.9 (moderate), with SMEs lower (mean=2.3) than large orgs (mean=4.0).

These statistics show (i) that a non-trivial set of organizations report incidents but that a minority of those incidents produce convictions, and (ii) substantial delays in obtaining provider-held evidence, particularly where MLATs are invoked.

7. DATA ANALYSIS ON HYPOTHESES

Hypotheses

H1: Legacy penal provisions (without cyber-specific supplements) are associated with lower rates of prosecutions that progress to charges/conviction, compared with jurisdictions using

ISSN: 2582-6433

explicit cyber statutes.

H2: Longer time-to-evidence (especially where MLATs are involved) is negatively associated with the probability of charges being framed or conviction being achieved.

H3: Organizational forensic readiness (log retention, forensic SOPs) is positively associated with successful prosecution outcomes (case filed and charges framed).

Methods & Variables

Dependent variables: (a) case progressed to charges (binary), (b) conviction achieved (binary). Key independent variables: (i) jurisdiction legal model (binary: presence of cyber-specific statute beyond generic penal provisions), (ii) time-to-evidence in days (continuous), (iii) forensic-readiness score (1–5). Control variables: organization size, sector, geographic region. Logistic regression models were estimated for each dependent variable.

Results

H1 — Legal model effect:

Organizations reporting incidents in jurisdictions with identifiable cyber statutes showed higher odds of charges being framed (OR ≈ 2.15; $p < 0.05$). The effect on actual convictions was positive but not statistically significant (OR ≈ 1.48; $p = 0.18$), reflecting likely sample-size limits and the many non-legal factors determining conviction (e.g., evidence strength, plea bargains). This supports the assertion that clearer substantive law helps translate incidents into prosecutable matters.

H2 — Time to evidence effect:

Each additional 10 days in time-to-evidence was associated with an approximate 8% reduction in odds of charges being framed (OR per day ≈ 0.992; cumulative effect per 10 days ≈ 0.92; $p < 0.05$). Where MLATs were required (and average time-to-evidence was much higher), the odds of prosecution dropping were even larger. This corroborates practitioner accounts that timeliness is critical for actionable digital evidence.

H3 — Forensic readiness effect:

Higher forensic-readiness scores strongly predicted both filing and progression: an increase of one point on the 1–5 readiness scale corresponded to a 1.6× increase in odds of charges being framed ($p < 0.01$). This effect was robust to controls.

Interpretation

The analysis supports the proposition that (i) substantive clarity in cyber statutes facilitates

ISSN: 2582-6433

prosecutorial action, (ii) procedural delays, especially those introduced by slow cross-border evidence channels reduce prosecution success, and (iii) organizational preparedness materially improves legal outcomes. These findings echo broader literature emphasizing the need for both legislative modernization and technical/process readiness.

8. LEGAL AND FORENSIC CHALLENGES (DETAILED FINDINGS FROM INTERVIEWS & SURVEY)

8.1 Substantive ambiguity and judicial interpretation

Interviewed prosecutors described frequent reliance on analog provisions (e.g., theft, criminal breach of trust, cheating) when cyber-specific offenses are absent or limited. While courts have sometimes interpreted terms like "property" to include "data" or "access," such interpretive moves increase legal uncertainty and invite appeals. Practitioners emphasized that penalties calibrated for physical harm may be ill-suited to economic and systemic harms (e.g., ransomware extortion of critical infrastructure).

8.2 Cloud evidence and third-party involvement

Forensics practitioners uniformly reported that the predominant hurdle is rapid access to server-side logs, application telemetry, and authentication records—data often controlled by cloud service providers (CSPs) with contractual and jurisdictional constraints. Even when CSPs are cooperative, differences in log schemas, retention policies, and access-control processes complicate the process.

8.3 MLAT delays and legal complexity

Several investigators recounted cases where initial forensic leads evaporated while awaiting MLAT responses, allowing suspects to escalate concealment or transfer assets. While some bilateral or regional arrangements permit expedited preservation requests, many countries lack legal channels for direct law enforcement to provider preservation orders.

8.4 Chain-of-custody, authenticity, and expert testimony

Courts require demonstrable chain-of-custody and authenticity for digital artifacts. Interviewees observed inconsistent judicial familiarity with technical provenance concepts; in some jurisdictions, judges accepted provider-generated attestations (signed exports), while others demanded deep technical foundation testimony, increasing trial costs and complexity.

ISSN: 2582-6433

8.5 Resource asymmetries and SME vulnerability

SMEs often lack forensic readiness and legal counsel to pursue criminal remedies. Several interviewees recommended state-sponsored shared SOC/forensic services to improve reporting and prosecution pipelines.

9. SUGGESTIONS — TOWARD A MODEL "CYBER CODE"

Based on the empirical findings, interviews, and authoritative secondary sources, this section proposes a modular blueprint for a "cyber code" that would sit alongside penal codes or act as integrated amendments. The aim is not to prescribe identical laws for every jurisdiction but to propose interoperable elements supportive of practical enforcement and rights protection.

9.1 Substantive elements (criminal law)

a) **Clear, technology-neutral definitions**: Define core terms "computer system," "computer data," "access," "authorization," "interference," and "service provider" in ways that are stable yet adaptable to technological change.

b) **Categorized offenses**: Distinguish between (a) unauthorized access/interference, (b) data interference/exfiltration, (c) identity/fraud offenses (credential abuse, BEC), (d) cyber-enabled financial crimes (money-laundering via crypto), and (e) cyber-dependent harms (DDoS, malware propagation). Each category should have calibrated mens rea requirements (intent, negligence) and proportionate penalties.

c) **Specificity for novel harms**: Include provisions for ransom and data-extortion, supply-chain attacks, and tampering with industrial control systems with aggravated penalties where public safety is endangered.

d) **Victim-centric remedies**: Enable expedited takedown, preservation orders, and civil remedies (injunctions, damages) with safe judicial oversight.

9.2 Procedural and evidentiary rules

a) **Preservation orders & expedited preservation**: Legal mechanisms allowing rapid preservation of logs/data with minimal procedural friction and judicial oversight. Model language should require notification and narrow scope to protect privacy.

b) **Standardized digital-evidence export formats**: Encourage CSPs to adopt standardized, signed export formats (hash-anchored, timestampped) that clearly document generation, access roles, and exporter identity improving admissibility and chain of custody.

ISSN: 2582-6433

c) **Admissibility presumptions with rebuttable proofs**: Where an export is generated according to specified technical best practices (e.g., hashed, signed), courts may accept a presumption of authenticity unless rebutted by technical challenge. This reduces the need for lengthy foundation testimony in routine matters.

d) **Privilege and counsel protocols**: Clear rules on when incident response materials are protected by legal privilege, balancing prosecutorial needs and rights of defense.

9.3 Cross-border cooperation and international instruments

a) **Expedited direct to provider channels**: Codify lawful, rights-respecting mechanisms for law enforcement to request data preservation or basic subscriber records directly from providers under defined conditions, with judicial or quasi-judicial oversight.

b) **Standardized MLAT acceleration**: Model treaty language that narrows scope for expedited data preservation, with safeguards for human rights and data protection. The Budapest Convention and recent UN convention efforts provide templates; jurisdictions should adopt harmonized language to simplify inter-state cooperation.

c) **Mutual recognition of provider attestations**: Encourage international recognition of provider-signed attestations and standardized logs to reduce duplication.

9.4 Capacity building and institutional design

a) **National digital evidence hubs**: Shared regional or national forensic hubs offering rapid preservation, neutral export, and technical attestations for use by prosecutors.

b) **Judicial and prosecutorial training**: Ongoing technical education programs to ensure courts can evaluate digital evidence competently.

c) **SME support programs**: Subsidized basic forensic readiness toolkits and SOC as a service options for small firms.

9.5 Safeguards and human rights considerations

Every procedural acceleration must be balanced with judicial oversight, periodic review, data minimization, and remedies for misuse. Privacy and due-process protections must be embedded in preservation orders, cross-border requests, and provider cooperation mechanisms.

10. IMPLEMENTATION ROADMAP & PRACTICAL STEPS

1) **Legislative review and draft model cyber code:** Convene multi-stakeholder drafting groups (lawyers, technologists, civil society) to craft model provisions that are

ISSN: 2582-6433

technology-neutral and rights-aware. Use Budapest Convention and UN drafts as references.

2) **Pilot procedural innovations:** Governments with high cloud usage should pilot expedited preservation orders with judicial templates and periodic reporting to oversight bodies.
3) **Provider engagement & standard setting:** Incentivize or regulate CSPs to provide signed, time-stamped logs and standardized export APIs for lawful requests. Public-private working groups (regulators + providers + law-enforcement) should agree on minimal formats.
4) **Capacity building:** Fund national forensic hubs, prosecutor training, and SME resilience programs.
5) **Regional cooperation:** Encourage regional instruments (e.g., EU frameworks, regional MLAT compacts) to adopt harmonized language that can be later expanded into global conventions.

11. CONCLUSION

The shift from "penal code" thinking to a forward-looking "cyber code" approach is both necessary and feasible. Legacy penal statutes can sometimes be adapted to cyber contexts, but such ad hoc measures leave gaps in legal clarity, evidentiary procedures, and cross-border practicality. Empirical evidence in this study triangulating interviews, an organizational survey, and authoritative secondary reports indicates that clear cyber-specific statutes, improved forensic readiness, and accelerated, rights-respecting cross-border mechanisms materially improve the prospects for effective investigation and prosecution. The policy blueprint articulated here provides a pragmatic pathway: adopt clear, technology neutral substantive definitions; standardize digital-evidence practices (signed exports, preservation orders); modernize MLAT and direct provider channels with oversight; and invest in institutional capacity. Balancing these reforms with robust privacy and due-process safeguards will be essential to secure public trust and effectiveness.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all the individuals and organizations that have contributed to the publication of this research paper.

ISSN: 2582-6433

First and foremost, I would like to thank my mentor Shri D D Joshi, Detective & Cyber Crime Investigator for his invaluable guidance and support throughout the research process. His expertise and insights were instrumental in shaping the direction and focus of my research. I am also grateful to the officials of Judiciary and Lower Courts, District Courts and High court for providing me with the resources and support I needed to complete this paper.

I would also like to thank my Senior Advocates and colleagues at my work places for their feedback and support throughout the research process. In particular, I would like to thank my family members for morale support. Finally, I would like to thank all the participants in this study for their time and willingness to share their experiences. Their contributions have been invaluable in helping me to understand the topic and draw meaningful conclusions.

I would also like to express my appreciation to the IJLRA for considering my work and providing the opportunity to publish my findings.

REFERENCES

1. Council of Europe. (n.d.). About the Convention — Cybercrime (Budapest Convention). Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention
2. Eurojust. (2024). United Nations Convention against Cybercrime. Eurojust. https://www.eurojust.europa.eu/publication/united-nations-convention-against-cybercrime
3. FBI. (2025). FBI releases annual internet crime report (IC3 Annual Report 2024). Federal Bureau of Investigation. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report
4. Verizon. (2024). Data Breach Investigations Report (DBIR) 2024. Verizon Enterprise. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf
5. International Cybersecurity Legal Guides (ICLG). (2024). Cybersecurity Laws and Regulations — India 2025. ICLG. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india
6. JSIS (University of Washington). (2025). Cybersecurity Profile 2025: India. Jackson School of International Studies. https://jsis.washington.edu/news/cybersecurity-profile-2025-india/

ISSN: 2582-6433

7. Lawfare. (2025). Schmitt, M., & Others. (2025). From Budapest to Hanoi: Comparing the CoE and UN Cybercrime Conventions. Lawfare. https://www.lawfaremedia.org/article/from-budapest-to-hanoi--comparing-the-coe-and-un-cybercrime-conventions
8. UPguard. (2025). Top Cybersecurity Regulations in India. UpGuard Blog. https://www.upguard.com/blog/cybersecurity-regulations-india

Additional press coverage and data referenced in the paper (e.g., IC3 statistics and modern treaty developments) include publicly available IC3 and DBIR reports and Council of Europe and UN material cited above.

BIOGRAPHY

An author is a practicing Advocate mainly at District-Metropolitan Courts and lower courts including Labour courts, Consumer Disputes Redressal Commission, etc. She also practices in the Honourable High Court of Gujarat. She emphasizes on the cases pertaining to Cyber Crimes, Cyber investigations, Cyber law procedures. She possesses specialized qualifications in Cyber Laws & Investigations in addition to the degrees of BTS, LLB, and LLM. Her focused aim of Advocacy to address the issues of Cyber victims and the mitigating cybercrimes from the society.