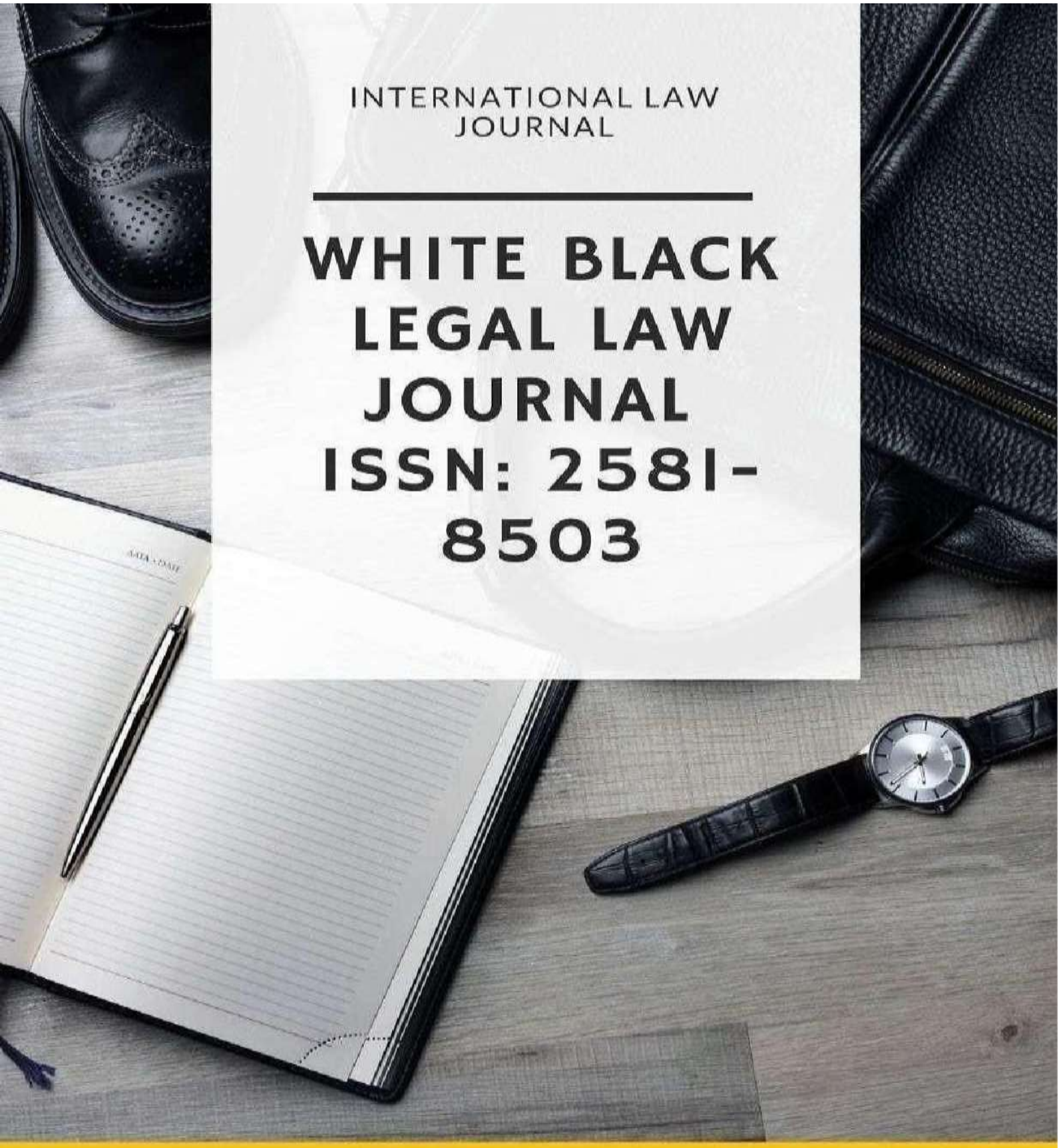

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

ADDRESSING CYBER FRAUDS IN INDIA AND THE EUROPEAN UNION: COMPARATIVE LEGAL AND POLICY PERSECTIVE STUDY

AUTHORED BY - MR. AKSHAY RAJPUT
B.A, LL.B., LL.M. in Criminal Law Group (Pursuing) Gokul Global University

ABSTRACT:

This study examines the growing challenge of cyber fraud in the rapidly expanding digital economies of India and the European Union through a comparative legal and policy perspective. With the widespread use of digital payment systems, e-commerce platforms, and internet-based financial services, cyber fraud has evolved into a significant threat that causes substantial financial losses and undermines public trust in digital infrastructures. The paper analyzes doctrinal legal analysis's of the legal frameworks governing cyber fraud in India, particularly the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023, and compares them with the European Union's regulatory regime, including the GDPR, Digital Services Act, NIS2 Directive, and related cybersecurity policies. It further evaluates institutional mechanisms, enforcement strategies, and major legal challenges such as jurisdictional complexities, technological advancements, and cross-border criminal networks. The study concludes by recommending stronger legislative reforms, enhanced institutional coordination, improved digital awareness, and greater international cooperation to effectively combat cyber fraud in an increasingly interconnected global digital ecosystem.

KEYWORDS:

Cyber Fraud, Digital Economy, Information Technology Act, 2000, European Union Cyber Law, Data Protection and Privacy, Digital Payment Fraud, Cross-Border Cybercrime.

INTRODUCTION:

In an era defined by the inexorable digitization of economies and societies, cyber frauds have emerged as a pernicious threat, inflicting staggering economic losses and eroding public trust in digital infrastructures across jurisdictions. India, with its burgeoning digital economy

propelled by initiatives like Digital India and the Unified Payments Interface, reported cyber fraud incidents surpassing 1.5 million in 2024 alone, resulting in pecuniary damages exceeding ₹20,000 crores, as per data from the Indian Cyber Crime Coordination Centre (I4C). Parallels the European Union grapples with sophisticated scams targeting its Single Market, where Eurostat figures indicate annual losses nearing €50 billion, amplified by cross-border operations exploiting regulatory variances among member states. This study undertakes a comparative legal and policy perspective to dissect the divergent frameworks governing cyber fraud mitigation in these realms: India's evolving statutory edifice, anchored in the Information Technology Act, 2000 (as amended), the Bharatiya Nyaya Sanhita, 2023, and ancillary measures like the Digital Personal Data Protection Act, 2023, juxtaposed against the EU's harmonized regime under the Digital Services Act (DSA), the Digital Markets Act (DMA), and the proposed Cyber Resilience Act, fortified by Directive (EU) 2013/40 on attacks against information systems. By probing doctrinal underpinnings, enforcement mechanisms, institutional capacities, and policy innovations—such as India's Cyber Fraud Reporting Portal versus the EU's Cybersecurity Act (Regulation (EU) 2019/881) this analysis elucidates convergences and lacunae, positing prescriptive pathways for bilateral cooperation, including mutual legal assistance treaties and technology-sharing protocols, to fortify resilience against this borderless scourge.

BACKGROUND OF CYBER FRAUD IN THE DIGITAL ECONOMY:

The digital economy, propelled by the pervasive integration of internet connectivity, e-commerce platforms, and financial technologies since the early 2000s, has inadvertently cultivated fertile ground for cyber fraud, transforming rudimentary online scams into a sophisticated, industrialized criminal enterprise that exploits the anonymity, scale, and interoperability of global networks. In India, where digital transactions exploded with initiatives like Unified Payments Interface (UPI) and widespread mobile banking, reported cybercrime cases surged from 65,893 in 2022 to 86,420 in 2023, escalating further to over 1.91 million complaints in 2024 amid losses exceeding ₹22,812 crore ($2.78 billion), predominantly from phishing, digital arrest scams, and UPI frauds that prey on a burgeoning user base of hundreds of millions engaging in daily digital payments. Parallel developments in the European Union reveal a comparable trajectory, with cyber-enabled fraud networks dismantled in operations like SIMCARTEL yielding over 3,200 cases across Austria and Latvia alone, while ransomware and phishing dominate ENISA's 2025 threat landscape, underscoring how the

EU's advanced digital single market encompassing seamless cross-border data flows and finch innovations amplifies vulnerabilities in manufacturing, digital services, and public administration sectors. This evolution traces back to the 1990s networking boom, which enabled data manipulation, evolving through the 2010s ransomware proliferation and dark web marketplaces into AI-augmented deceptions by 2025, where global losses now span $1-10 trillion annually, eroding trust in digital ecosystems and distorting markets from New Delhi's street vendors to Brussels' corporate boardrooms. As both jurisdictions grapple with this shadow economy, the interplay of rapid digitization, regulatory lags, and transnational actor networks demands a nuanced comparative lens to dissect policy responses.

RESEARCH GAP:

The existing literature and legal discussions on cyber fraud largely examine national legal frameworks or technological threats in isolation, but there is limited comparative and integrative analysis of how legal, institutional, and policy mechanisms operate across jurisdictions such as India and the European Union. While studies discuss India's statutory regime under the IT Act, 2000 and the EU's regulatory architecture including the Digital Services Act and NIS2 Directive, insufficient attention has been given to systematically comparing their enforcement effectiveness, institutional coordination, and cross-border cooperation mechanisms in addressing rapidly evolving cyber frauds such as AI-driven scams, cryptocurrency fraud, and transnational phishing networks. Consequently, a significant research gap exists in identifying how lessons from the EU's harmonized regulatory model and India's centralized enforcement mechanisms can be integrated to develop a more coherent and effective legal-policy framework for combating cyber fraud in an increasingly borderless digital economy.

RESEARCH OBJECTIVES:

1. To examine the nature and growth of cyber fraud in the digital economies of India and the European Union.
2. To analyze the existing legal framework governing cyber fraud in India and the European Union.
3. To evaluate the institutional mechanisms and enforcement strategies adopted to combat cyber fraud in both jurisdictions.
4. To identify the key legal, policy, and enforcement challenges in addressing cyber fraud

in India and the European Union.

5. To propose legal and policy reforms for strengthening cyber fraud regulation and enhancing international cooperation between India and the European Union.

RESEARCH METHODOLOGY:

The present study adopts a doctrinal research methodology, relying primarily on qualitative analysis of secondary sources to examine the legal frameworks addressing cyber fraud in India and the European Union. The research is based on a systematic review of statutory provisions, international directives, judicial decisions, scholarly articles, government reports, and policy documents relating to cybercrime regulation. Key legislative instruments such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023 in India are analyzed alongside the European Union's regulatory framework, including the Digital Services Act, the NIS2 Directive, and Directive 2013/40/EU on attacks against information systems. The study further draws upon authoritative materials from governmental institutions, international organizations, and academic literature to critically evaluate legal principles, enforcement mechanisms, and policy approaches adopted in both jurisdictions. Through comparative doctrinal analysis, the research identifies similarities, differences, and existing legal gaps in addressing cyber fraud, thereby providing a structured legal understanding supported by reliable and authentic sources.

GROWTH OF ONLINE FINANCIAL TRANSACTIONS AND EMERGING CYBER RISKS

The exponential expansion of online financial transactions in India and the European Union has fundamentally reshaped economic interactions, propelled by widespread adoption of digital platforms and instant payment systems. In India, the Unified Payments Interface (UPI) processed over 130 billion transactions by the close of 2025, with volumes surging 33.5 percent year-on-year to 59.33 billion in the third quarter alone and annual values reaching Rs 300 lakh crore, reflecting deeper penetration into everyday micro-transactions averaging Rs 1,293 each. the EU witnessed non-cash transactions projected to exceed 630 billion by 2028 at a compound annual growth rate above 10 percent, fueled by e-money payments that climbed 10.7 percent to 4.7 billion in the first half of 2025, alongside e-commerce's rising share of retail sales and the dominance of digital wallets in over 60 percent of online purchases. This surge, while fostering financial inclusion and efficiency, has concurrently amplified cyber vulnerabilities,

manifesting in India through a 24 percent escalation in cybercrime cases to 28.15 lakh in 2025 entailing Rs 22,495 crore in losses predominantly from investment scams (35 percent of incidents), digital arrests, sextortion, and a 59 percent spike in IoT-targeted attacks alongside phishing that now afflicts nearly three in ten banking attempts and cryptocurrency-enabled Ponzi schemes exploiting regulatory gaps. In the EU, over one in five businesses endured cybersecurity breaches in 2024, with financial institutions comprising 46 percent of 2025 attacks, ransomware incidents up 40 percent amid geopolitical strains causing €1.2 billion in data breach damages, and fraud volumes in instant payments ballooning 175 percent despite regulatory interventions like Verification of Payee, compounded by AI-augmented impersonation, crypto volatility risking systemic contagion from a €600 billion market downturn, and elevated money laundering threats in FinTech sectors. These intertwined dynamics underscore the imperative for robust legal frameworks to mitigate the disproportionate escalation of risks against transactional growth.

IMPORTANCE OF LEGAL REGULATION TO COMBAT CYBER FRAUD

Legal regulation stands as the cornerstone in the battle against cyber fraud, providing a structured framework that not only penalizes offenders but also fosters preventive measures essential for safeguarding digital economies. In jurisdictions like India and the European Union, where cyber fraud incidents have escalated dramatically India witnessing a 24% surge to 28.15 lakh cases in 2025 with losses exceeding ₹22,495 crore, and the EU grappling with millions of attacks amid evolving AI-driven scams robust laws such as India's Information Technology Act, 2000, and the EU's emerging Payment Services Directive revisions impose clear liabilities on financial institutions and platforms, compelling them to deploy advanced authentication and monitoring systems. These regulations transcend mere punishment by mandating compliance audits and inter- agency coordination, which have demonstrably curbed phishing and unauthorized access; for instance, post-IT Act implementation in Indian banking, phishing incidents dropped by 50% through enforced multi-factor authentication and transaction oversight.

Beyond deterrence through stringent penalties ranging from imprisonment under Sections 66 and 66D of the IT Act for identity theft to EU mandates holding payment providers accountable for fraud losses up to €50,000 legal frameworks cultivate public trust in digital transactions,

vital for economies reliant on UPI in India and SEPA in the EU. Empirical evidence underscores this high- value fraud cases in India quadrupled in FY2024, prompting regulatory interventions like the RBI's account freezing protocols, which recovered billions by swiftly disrupting fraud chains. Similarly, the EU's political agreement in November 2025 on online fraud rules extends liability to platforms for scam ads, ensuring rapid takedowns and reimbursements, thereby reducing victim burdens and incentivizing proactive risk assessments across the supply chain.

The deeper imperative lies in legal regulation's capacity to bridge transnational gaps inherent in cyber fraud's borderless nature, harmonizing definitions and enforcement as seen in the Budapest Convention's influence on both Indian and EU approaches. Without such oversight, fragmented responses exacerbate vulnerabilities; India's cybersecurity incidents ballooned from 10.29 lakh in 2022 to over 22 lakhs by 2024, while Europe's DDoS attacks claimed nearly half of global totals in early 2025, highlighting how unregulated spaces enable malware proliferation and deep fake exploits. Effective regimes, therefore, integrate international cooperation evident in EU-India cyber dialogues with domestic tools like India's National Cyber Crime Reporting Portal, which processed millions of complaints, yielding convictions and policy refinements that adapt to threats like AI-assisted BEC scams.

In core of the legal regulation transforms reactive policing into a proactive ecosystem, embedding cybersecurity into corporate governance and consumer rights. Comparative insights from India and the EU reveal that where laws evolve with technology as in the EU's shift toward platform accountability or India's DPDP Act 2023 supplementing the IT Act fraud losses stabilize despite rising digital adoption, proving regulation's role in sustaining economic resilience. This regulatory backbone not only imposes accountability but also drives innovation in secure tech, ensuring cyber fraud does not undermine the digital single markets both regions aspire to build.

NEED OF INDIA AND THE EUROPEAN UNION

The imperative for concerted legal and policy responses to cyber frauds in India and the European Union stems from their escalating prevalence, profound socioeconomic repercussions, and the transnational nature of digital criminality that renders unilateral measures woefully inadequate. In India, the National Crime Records Bureau documented over 1.19 million cybercrime cases in 2024 alone, marking a 24% surge from the previous year, with

financial frauds accounting for 65% of incidents and causing losses exceeding ₹1.25 lakh crore, as per Reserve Bank of India estimates; these figures expose systemic vulnerabilities in a rapidly digitizing economy where UPI transactions hit 16.9 billion monthly by mid-2025, amplifying risks for an unbanked populace increasingly reliant on Aadhaar-linked digital wallets, yet constrained by the Indian Penal Code's antiquated Sections 420 and 468, ill-equipped for phishing, deep fake scams, and ransomware that exploit jurisdictional gaps under the Information Technology Act, 2000. Paralleling this, the European Union confronts a deluge of cyber frauds, with Eurostat reporting €7.8 billion in damages from 2.3 million incidents in 2024, fueled by sophisticated actors leveraging cross-border anonymity in the Schengen digital space; the NIS2 Directive (2022/2555) and Digital Services Act (2022/2065) strive to fortify resilience, yet enforcement disparities among member states—evident in Germany's 28% case clearance rate versus Romania's 12%—underscore the limitations of fragmented national implementations amid rising AI-driven frauds like voice cloning that evade the ePrivacy Regulation. This shared predicament demands bilateral synergy, as cyber fraud circuits often originate in India's porous server farms before targeting EU consumers via mule accounts in Eastern Europe, necessitating harmonized frameworks akin to the India-EU Trade and Technology Council (2022) to align extradition protocols under the Budapest Convention—ratified by India in 2023—and mutual legal assistance treaties, thereby bridging evidentiary standards, enhancing real-time data sharing through proposed INTERPOL-EUROPOL liaisons, and fostering capacity-building in forensic block chain analysis such collaboration not only mitigates economic hemorrhage but fortifies global normative standards against an evolving threat landscape where quantum computing looms to decrypt legacy encryptions by 2030, compelling both jurisdictions to transcend domestic silos for a resilient, interoperable cyber governance architecture.

India and the EU tackle cyber frauds through distinct legal frameworks shaped by federal versus supranational structures. India's approach emphasizes reactive criminal penalties, while the EU prioritizes preventive data protection and harmonized directives.

1. Legislative Framework

ASPECT	INDIA	EUROPEAN UNION
Primary Laws	IT Act 2000 (Sections 43, 66 for hacking/fraud); Bharatiya Nyaya Sanhita	Cybercrime Directive 2013/40/EU; GDPR 2018 (data breaches); Directive

	(cheating/forgery); DPDP Act 2023 (data misuse).	(EU) 2019/713 on attacks against info systems.
Scope	Covers identity theft, phishing, digital arrest scams; state-level enforcement.	Harmonized across 27 states; focuses on fraud, ransomware, transnational crimes.
Recent Updates (2026)	CFCFRMS portal for quick FIRs/fund recovery; I4C coordination.	NIS2 Directive (2022) enhances critical infra resilience; AI Act regulates fraud tools.

2. Enforcement Mechanisms

ASPECT	INDIA	EUROPEAN UNION
Reporting/Investigation	National Cybercrime Reporting Portal; e-FIRs in select states; CERT-In mandates.	Europol's EC3 mandatory breach notifications within 72 hrs under GDPR/NIS2.
Penalties	Up to 3 years jail + fines (IT Act); varies by state prosecution speed.	Fines up to 4% global turnover (GDPR); criminal sanctions up to 5-10 years.
Challenges	Low conviction rates; fragmented policing; awareness gaps.	Cross-border jurisdiction delays; varying member state implementation.

3. Policy Perspectives

ASPECT	INDIA	EUROPEAN UNION
Focus	Financial fraud prevention (e.g., UPI scams); public awareness via I4C.	Privacy-by-design; digital single market; public-private partnerships.
International Ties	Bilateral MoUs; Budapest Convention observer.	Full Budapest Convention party; strong US/EU cyber dialogues.
Gaps/Recommendations	Needs unified cyber police; faster fund tracing.	Strengthen SME compliance; AI-driven fraud detection mandates.

DEFINITION OF CYBER FRAUD:

Generally, Cyber fraud refers to deceptive criminal activities conducted online to trick individuals or organizations into revealing sensitive information, such as passwords or financial data, or to steal money and assets through tactics like phishing, identity theft, ransomware, and malware attacks.

KEY TYPES OF CYBER FRAUD

1. Phishing Attacks

   Phishing attacks are deceptive attempts where cybercriminals impersonate legitimate entities via email, SMS, or websites to lure victims into divulging sensitive data like login credentials or financial details. They exploit trust and urgency for quick clicks. Example: A fake email from your "bank" claims account suspension and links to a bogus site stealing your password.

2. Online Banking Fraud

   Online banking fraud involves unauthorized access to digital banking platforms through malware, keyloggers, or stolen credentials to execute fraudulent transactions or transfers. It targets weak security during logins.

   Example: Hackers infect your phone with malware to capture OTPs and drain your account mid- session.

3. Identity Theft

   Identity theft occurs when fraudsters steal personal identifiers like names, addresses, or SSNs to open accounts, make purchases, or commit crimes in the victim's name. It often stems from data breaches.

   Example: A criminal uses your leaked details to file fake tax returns and pocket the refund.

4. Credit/Debit Card Fraud

   Credit/debit card fraud entails the illicit use of card information for unauthorized purchases, often via skimming devices, online theft, or cloned cards. No physical card is needed for digital frauds. Example: Thieves at a store swap your card for a cloned one, and then max out online purchases.

5. Cryptocurrency Fraud

   Cryptocurrency fraud encompasses scams like fake ICOs, wallet phishing, or exchange hacks to pilfer digital currencies from investors or holders. It leverages crypto's volatility and irreversibility. Example: A fraudulent "pump-and-dump" scheme hypes a token, crashes it, and developers vanish with funds.

6. Ransomware Attacks

   Ransomware is malware that encrypts victims' files or systems, demanding cryptocurrency ransom for decryption keys, crippling businesses or individuals. It spreads via malicious links or attachments.

   Example: A hospital's network locks, halting surgeries until payment, as seen in real-world attacks.

7. Business Email Compromise (BEC)

   BEC defrauds trick companies into wiring funds or sensitive data by spoofing executive emails or vendors, often using social engineering. They target finance teams.

   Example: A fake CEO email instructs the accountant urgently transfer $50,000 for a "deal".

8. Other Types

   Additional cyber fraud types include advance-fee frauds (e.g., lottery wins requiring upfront fees), investment fraud (Ponzi schemes via apps), e-commerce fraud (fake sellers on marketplaces), and social media frauds (fake giveaways stealing data).

CYBER FRAUD AS A FORM OF CYBERCRIME

Cyber fraud stands as a quintessential manifestation of cybercrime, embodying the deliberate exploitation of digital platforms to perpetrate deception for illicit gain, wherein perpetrators manipulate electronic communications, forge identities, or deploy malicious software to extract financial assets or sensitive data from unsuspecting victims. This form of malfeasance permeates the cyber domain through diverse modalities such as phishing expeditions that masquerade as legitimate entities to harvest credentials, ransomware deployments that encrypt assets pending extortionate payments, and investment frauds leveraging bogus trading portals to siphon funds under false promises of lucrative returns, all of which erode trust in digital ecosystems and precipitate profound economic repercussions.

In the Indian context, cyber fraud finds rigorous proscription under the Information Technology Act, 2000, particularly Section 66D which penalizes cheating by personation via computer resources with imprisonment up to three years and fines up to one lakh rupees, alongside Section 66C addressing identity theft through fraudulent appropriation of electronic signatures or passwords; these provisions intertwine with the Bharatiya Nyaya Sanhita, 2023, where Section 318(4) escalates penalties for cheating-induced property delivery to seven years rigorous imprisonment, and Section 111 categorizes large-scale cyber fraud rings as organized crime warranting life terms, reflecting a legislative pivot toward heightened deterrence amid a 24 percent surge in incidents to 28.15 lakh cases in 2025, inflicting losses exceeding ₹22,495 crore predominantly from investment frauds and digital arrest ruses.

Complementing these, the European Union delineates cyber fraud within Directive 2013/40/EU on attacks against information systems, which criminalizes illegal access, data interference, and system sabotage including tools like botnets that facilitate fraudulent incursions, while Directive (EU) 2019/713 specifically targets non-cash payment frauds such as phishing, skimming, and the trafficking of counterfeit payment instruments, mandating minimum penalties escalating to five years for aggravated offenses against critical infrastructure or in organized syndicates, thereby harmonizing member state responses to threats that afflicted one in four small businesses across Europe in recent surveys.

This delineation underscores cyber fraud's intrinsic character as cybercrime: not merely an adaptation of traditional deceit to virtual realms, but a sui generis threat amplified by technology's borderless reach, instantaneous execution, and anonymity, compelling both jurisdictions to evolve punitive frameworks that balance enforcement efficacy with evidentiary challenges in tracing ephemeral digital footprints.

IMPORTANT TIMELINES OF TECHNOLOGICAL EVOLUTION AND CYBER THREATS

1. Technological Evolution and Cyber Threats

   The rapid trajectory of technological advancement has fundamentally reshaped the landscape of cyber fraud, creating both opportunities for innovation and fertile ground for sophisticated criminality. This section traces the evolution of key technologies—from early internet infrastructure to artificial intelligence-driven systems—and

examines the corresponding escalation in cyber threats. By dissecting these developments, we illuminate the regulatory gaps that persist in India and the European Union, setting the stage for a comparative analysis of legal responses.

2. Foundational Internet Expansion and the Dawn of Mass-Scale Cyber Fraud (1990s–Early 2000s)

   The commercialization of the World Wide Web in the mid-1990s marked the genesis of widespread cyber vulnerabilities. Dial-up connections and nascent e-commerce platforms, such as early iterations of Amazon and eBay, exposed users to rudimentary phishing scams and credit card skimming. In India, the liberalization of telecom policies under the National Telecom Policy 1994 spurred internet penetration, rising from negligible levels to over 10 million users by 2000 (TRAI, 2001). Yet this growth outpaced safeguards, enabling frauds like the 1999 "Nigerian Prince" email scams that defrauded Indian expatriates of millions. Similarly, in the EU, the e-Commerce Directive 2000/31/EC aimed to foster digital markets but overlooked transnational threat vectors. Empirical data from the Internet Crime Complaint Center (IC3) reveals a 500% surge in reported cyber frauds between 1998 and 2005, underscoring how packet-switched networks democratized access while amplifying attack surfaces through unsecured SMTP protocols and lack of end-to- end encryption.

3. Broadband Proliferation and the Rise of Organized Cybercrime Syndicates (Mid-2000s–2010s)

   High-speed broadband, coupled with Web 2.0 interactivity, transformed cyber threats from isolated incidents to orchestrated campaigns. Social media platforms like Facebook (launched 2004) and India's Aadhaar-linked digital economy fueled identity theft and account takeovers. A pivotal case is the 2016 Bangladesh Bank heist, where SWIFT network exploits siphoned $81 million via malware-laden servers, exploiting vulnerabilities in legacy banking systems (SWIFT, 2016 report). India's CERT-In logged over 32,000 incidents in 2017 alone, with 40% tied to ransomware like WannaCry, which leveraged EternalBlue exploits in unpatched Windows systems. In the EU, the 2013 Yahoo breach affecting 3 billion accounts highlighted data aggregation risks under fragmented national laws pre-GDPR. This era saw threat actors evolve into syndicates, using botnets (e.g., Mirai in 2016, infecting IoT devices) for DDoS attacks that disrupted financial services, as evidenced by the 2016 Dyn assault

costing enterprises $110 million daily (Akamai, 2017). Legal scholarship, including Kshetri (2010), argues that broadband's asymmetry high upload speeds for attackers necessitated harmonized international protocols, a lesson India partially addressed via the IT Act 2000 amendments but the EU deferred until NIS Directive 2016.

4. Mobile and Cloud Computing Boom: Ubiquity and Endpoint Exploitation (2010s–Present)

   Smartphone adoption exploded globally, with India's 1.2 billion mobile subscribers by 2023 enabling app-based frauds like UPI phishing (RBI, 2024). Technologies such as 4G/5G networks and cloud services (AWS, Azure) introduced zero-day vulnerabilities; for instance, the 2020 SolarWinds supply-chain attack compromised 18,000 organizations, including EU critical infrastructure, via tampered Orion software updates (FireEye, 2021). Cyber threats adapted seamlessly: SIM-swapping bypassed two-factor authentication, defrauding Indian users of ₹1,500 crore in 2022 (NCRB Crime in India Report). EU parallels emerge in the 2021 Colonial Pipeline ransomware shutdown, which halted fuel supplies and exposed cloud misconfigurations. Quantitative analysis from ENISA's 2025 Threat Landscape shows a 300% rise in mobile malware since 2018, driven by Android's open ecosystem prevalent in India versus iOS dominance in the EU. These developments strained forensic capabilities, as ephemeral cloud data evades traditional chain-of-custody rules under India's Evidence Act 1872 or EU's eIDAS Regulation.

5. Artificial Intelligence and Emerging Frontiers: Weaponized Intelligence in Cyber Fraud (2020s Onward)

   Generative AI and machine learning have elevated threats to predictive, autonomous levels. Tools like ChatGPT clones generate hyper-personalized phishing (e.g., deepfake voice scams defrauding Indian elders of ₹10 crore in 2024 cases reported by PIB). Adversarial AI evades detection in GAN-based frauds, as seen in the 2023 MGM Resorts attack using social engineering amplified by LLMs. India's NPCI alerts highlight AI-orchestrated mule accounts in 70% of UPI frauds (2025 data), while EU's AI Act 2024 classifies high-risk cyber tools for mandatory audits. Quantum computing looms as a disruptor, potentially shattering RSA encryption (Shor’s algorithm, 1994), rendering current TLS protocols obsolete a risk unaddressed in India's DPDP Act 2023 or EU's DORA framework. Studies by the RAND Corporation (2024) project a 1,000-

fold increase in breach sophistication by 2030, propelled by edge computing in 6G networks and blockchain exploits like the 2022 Ronin Bridge $625 million theft.

6. Interplay of Evolution and Regulatory Imperatives

   This technological arc reveals a pattern: each innovation expands attack vectors exponentially, outstripping reactive laws. India's IT Rules 2021 mandate platform accountability but falter on cross-border AI threats, while the EU's Cyber Resilience Act 2024 imposes supply-chain due diligence yet grapples with enforcement asymmetry. Bridging these requires proactive foresight, informed by frameworks like NIST's Cybersecurity Framework 2.0, to preempt fraud in an AI- augmented digital commons.

CURRENT LEGAL STRUCTURE GOVERNING CYBER FRAUD IN INDIA

India confronts cyber fraud through a multifaceted legal architecture that integrates specialized cyber laws with traditional criminal statutes and emerging data safeguards, prominently featuring the Information Technology Act, 2000 (IT Act), the Indian Penal Code, 1860 (IPC), and the Digital Personal Data Protection Act, 2023 (DPDP Act).

The Information Technology Act, 2000 stands as the cornerstone of India's cyber regulatory regime, enacted to facilitate electronic commerce and governance while criminalizing a spectrum of digital offenses directly pertinent to cyber fraud. Sections 43 and 43A impose civil liability for unauthorized access, data damage, or negligent handling of sensitive information, enabling victims to seek compensation up to one crore rupees through adjudicating officers, whereas criminal provisions under Sections 65, 66, 66C, and 66D target tampering with computer source documents, dishonest computer-related acts like hacking or identity theft, and cheating by personation using computer resources, with penalties ranging from three to seven years imprisonment and fines. Notably, Section 67 addresses obscene material transmission, often exploited in sextortion scams, and Section 75 extends extraterritorial jurisdiction to offenses committed outside India affecting Indian systems, as affirmed in judicial precedents like *Shreya Singhal v. Union of India (2015)*, which balanced free speech with cybercrime deterrence; amendments in 2008 via the IT Amendment Act expanded these to cover cyber terrorism (Section 66F) and identity theft, empowering the Central Bureau of Investigation

(CBI) and state cyber cells under Section 78 for investigations, though enforcement challenges persist due to resource constraints in tracking anonymous perpetrators across borders.

Complementing the IT Act, the Indian Penal Code, 1860 provides a robust substratum for prosecuting cyber frauds manifesting as conventional crimes in digital guises, with Sections 415- 420 delineating cheating and criminal breach of trust core to phishing, online scams, and Ponzi schemes—punishable by up to seven years rigorous imprisonment and fines, as courts have expansively interpreted in cases such as *Sanjay Pandey v. State of Bihar (2020)* where email frauds triggered Section 420 convictions. Sections 463-471 on forgery extend to digital documents, including manipulated e-signatures or fake UPI transactions, while Section 506 covers criminal intimidation via threatening cyber messages; Section 420's application to cyber realms gained traction post-IT Act integration, evidenced in *Avnish Bajaj v. State (2005)* the Bazee.com case underscoring intermediary liability intersections, and recent National Crime Records Bureau (NCRB) data from 2024 revealing over 65,000 cyber fraud cases annually, predominantly prosecuted under IPC alongside IT Act provisions for comprehensive culpability.

The Digital Personal Data Protection Act, 2023 marks a paradigm shift by prioritizing data privacy as a bulwark against frauds exploiting personal information, mandating consent-based processing under Section 6, data minimization, and purpose limitation to curb unauthorized harvesting seen in SIM swap or KYC frauds.

Significant data fiduciaries such as banks and e-commerce platforms face obligations for accuracy, storage limitation, and breach notifications within 72 hours per Section 25, with penalties up to 250 crore rupees levied by the Data Protection Board; Sections 17-19 regulate cross-border data transfers potentially aiding international fraud probes, while the Act's alignment with Supreme Court directives in Justice K.S. Puttaswamy v. Union of India (2017) on privacy as a fundamental right fortifies victim redressal, though its nascent rules notified in 2025 underscore ongoing implementation hurdles in syncing with IT Act enforcement for holistic cyber fraud mitigation.

INSTITUTIONAL MECHANISMS

In India, the institutional architecture for combating cyber frauds rests primarily on the Indian Cybercrime Coordination Centre (I4C), operationalized under the Ministry of Home Affairs

since 2018 and elevated to an attached office in July 2024, which orchestrates a unified ecosystem for law enforcement agencies by facilitating real-time intelligence sharing, coordinated investigations, and capacity-building initiatives tailored to transnational financial scams and organized cyber networks, as evidenced by its proactive blocking of over 3,962 Skype IDs and 83,668 WhatsApp accounts implicated in fraud operations up to late 2025. Complementing I4C's enforcement mandate, the Indian Computer Emergency Response Team (CERT-In), enshrined under Section 70B of the Information Technology Act, 2000, and housed within the Ministry of Electronics and Information Technology, functions as the national nodal agency for incident response, meticulously addressing vulnerabilities in phishing, ransomware, and data manipulation schemes through initiatives like the Cyber Swachhta Kendra for malware remediation, the National Cyber Coordination Centre for threat metadata scanning, and a federated network of sectoral Computer Security Incident Response Teams (CSIRTs) in finance and power sectors, having managed nearly 30 lakh incidents in 2025 alone to bolster situational awareness and sectoral resilience. Further fortifying this framework, the National Cyber Crime Reporting Portal (cybercrime.gov.in) integrates victim reporting with automated fund freezing mechanisms under the Bharatiya Nagarik Suraksha Sanhita, 2023, while the dedicated helpline 1930 enables swift victim support, channeling complaints to state cyber cells and enabling inter-agency collaboration that has traced and mitigated billions in fraudulent transactions, though challenges persist in uniform state-level implementation given 'police' as a state subject. By contrast, the European Union's institutional response to cyber frauds centers on the European Cybercrime Centre (EC3), a specialized division of Europol established in 2013 and headquartered in The Hague, which serves as the pivotal hub for cross-border operational coordination, channeling forensic expertise, intelligence fusion, and joint investigation teams among 27 member states to dismantle payment fraud syndicates, online scams, and dark web marketplaces, exemplified by its pivotal role in high-profile operations disrupting millions in euro-denominated cyber heists through seamless liaison with national authorities and private sector partners. ENISA, the EU Agency for Cybersecurity, augments EC3's law enforcement focus by spearheading policy harmonization, vulnerability certification schemes under the Cybersecurity Act, and large-scale incident response drills, fostering a multi-layered governance that mandates member states to align national strategies with post-quantum cryptography migrations and NIS2 Directive obligations, thereby ensuring proactive threat mitigation across digital single market infrastructures like banking and e-commerce platforms. Euro just complements these by facilitating judicial cooperation in prosecuting cross-jurisdictional frauds, while recent 2025 legislative pacts impose strict liability on payment

providers for fraud reimbursements, underscoring a supranational enforcement ethos that contrasts sharply with India's more centralized yet federated model. This comparative lens reveals India's strengths in rapid-response national coordination via I4C and CERT-In, which have scaled to handle explosive digital growth with over 100 crore internet users, against the EU's advantage in decentralized yet harmonized multilateralism through EC3 and ENISA, where resource pooling across sovereign states yields superior interoperability for evolving threats like AI-augmented scams, suggesting potential for India to emulate EU-style certification mandates while the Union could adopt India's victim-centric portals for grassroots efficacy.

KEY CHALLENGES IN INDIA:

India confronts formidable challenges in combating cyber frauds, exacerbated by the explosive growth of its digital economy, where cybersecurity incidents escalated from 10.29 lakh in 2022 to 22.68 lakh in 2024, culminating in staggering financial losses of over ₹22,845 crore in 2024 alone and projections exceeding ₹1.2 lakh crore for 2025, representing nearly 0.7% of the nation's GDP. This surge stems largely from the rapid proliferation of digital payment systems like UPI and widespread internet penetration exceeding 86% of households under the Digital India initiative, which inadvertently amplifies the attack surface for sophisticated scams such as investment frauds accounting for 76% of losses in 2025, digital arrests at 9%, and sextortion at 4%, often leveraging AI-generated deepfakes and phishing tactics that prey on vulnerable first-time users, senior citizens, and low-income migrants.

A primary impediment lies in the inadequacy of the existing legal framework, particularly the Information Technology Act, 2000, even post-2008 amendments, which fails to encompass modern threats like ransomware, AI-driven deepfakes, and cryptocurrency scams through specific provisions, relying instead on generalized sections such as 66C for identity theft and 66D for cyber fraud, while the Bharatiya Nyaya Sanhita, 2023 introduces measures like Section 111 for organized cybercrime and Section 318 for digital cheating, yet these provisions grapple with definitional ambiguities, evidentiary hurdles in preserving volatile digital traces, and prolonged delays in victim remediation.

Jurisdictional complexities further erode enforcement efficacy, as cyber frauds transcend territorial boundaries, invoking principles like objective territoriality under Section 179 of the

Code of Criminal Procedure where effects manifest within India, but prosecutions falter amid overlaps between state police, central agencies, and international perpetrators often based in Southeast Asia, compounded by the absence of robust mutual legal assistance treaties tailored to real-time digital evidence sharing.

Institutional fragmentation undermines coordinated responses, with entities like the Indian Cybercrime Coordination Centre (I4C), CERT-In, and the National Critical Information Infrastructure Protection Centre (NCIIPC) suffering from overlapping mandates that impede seamless information exchange, while nascent implementation of the Digital Personal Data Protection Act, 2023 exposes gaps in regulatory oversight and inter-agency collaboration essential for preempting transnational fraud networks.

Resource constraints manifest acutely in the acute shortage of skilled personnel, including over 90,000 digital forensics experts nationwide, particularly in smaller districts where understaffed units delay investigations, coupled with exorbitant costs of proprietary foreign tools and a dearth of indigenous solutions, rendering thorough analysis of IP logs, chat histories, and blockchain transactions infeasible in time-sensitive cases.

Victim under-reporting and awareness deficits perpetuate the cycle of impunity, as nearly 68% of digital fraud sufferers abstain from lodging complaints due to distrust in police responsiveness, fears of online shaming, or perceptions of triviality, disproportionately affecting marginalized groups like rural migrants and the elderly who navigate unfamiliar digital interfaces, with conviction rates languishing below 3% despite rising FIRs that dipped slightly to 55,484 in 2025 owing to proactive fund-blocking yet highlighting persistent judicial backlogs.

LEGAL FRAMEWORK GOVERNING CYBER FRAUD IN THE EUROPEAN UNION

The legal framework governing cyber fraud in the European Union represents a multifaceted architecture anchored in harmonized directives and regulations that priorities victim protection, cross-border cooperation, and robust enforcement mechanisms, with the cornerstone being Directive (EU) 2013/40 on attacks against information systems, which criminalizes unauthorized access, data interference, and system interference while mandating member states

to impose penalties of up to five years imprisonment for basic offences escalating to ten years for aggravated cases involving fraud or significant damage. Complementing this, Directive 2011/93/EU on combating sexual abuse and exploitation extends to online fraud schemes exploiting vulnerable groups, yet the pivotal instrument for cyber fraud per se emerges through the Digital Services Act (DSA, Regulation (EU) 2022/2065) and Digital Markets Act (DMA, Regulation (EU) 2022/1925), which impose stringent obligations on online platforms to swiftly remove illegal content including phishing scams and fraudulent marketplaces, backed by fines up to 6 percent of global annual turnover, alongside the landmark NIS2 Directive (Directive (EU) 2022/2555) that bolsters cybersecurity resilience by requiring critical entities to report incidents within 24 hours and implement risk management for fraud-prone digital services. At the financial nexus, the Fifth Anti- Money Laundering Directive (AMLD5, Directive (EU) 2018/843) targets crypto-asset fraud by mandating virtual asset service providers to conduct customer due diligence and report suspicious transactions via the Financial Intelligence Units, while the proposed Anti-Money Laundering Regulation (AMLR) under the 2024 legislative package seeks to centralize oversight through the new Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). Judicial enforcement draws strength from Euro just and Europol's operational coordination under the European Cybercrime Centre (EC3), facilitating joint investigation teams as seen in Operation Power OFF targeting malware-driven fraud rings, with the Court of Justice of the EU affirming extraterritorial reach in cases like Google Spain SL v. AEPD (C-131/12) to protect data integrity against fraudulent misuse. Recent evolutions, including the Cyber Resilience Act (proposed 2022, adopted 2024) mandating secure hardware-software standards to preempt fraud vectors in IoT devices, underscore a proactive paradigm shift, evidenced by the European Commission's 2023 Cyber Strategy allocating €1.5 billion for AI-driven fraud detection tools, ensuring a cohesive yet adaptive regime that balances innovation with stringent accountability across the single digital market.

Policy Measures

The European Union's cybersecurity architecture, anchored in a multifaceted strategy that has evolved through successive frameworks since the 2013 Cybersecurity Strategy, culminates in the comprehensive 2020 EU Cybersecurity Strategy and its 2023 implementation roadmap, which prioritize resilience across critical sectors by mandating proactive threat intelligence sharing via the EU-CyCLONe network and operational coordination through the Cybersecurity Act (Regulation (EU) 2019/881) establishing the European Union Agency for Cybersecurity

(ENISA) as a central hub for certification schemes and incident reporting; this strategy dovetails with stringent financial institution security requirements under the Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554), effective January 2025, which imposes on credit institutions, payment providers, and crypto-asset service providers a harmonized regime of ICT risk management, including annual testing of critical functions through threat-led penetration testing (TLPT) and mandatory reporting of major incidents within four hours to competent authorities, thereby addressing cyber fraud vectors like ransomware and phishing that target payment systems, as evidenced by the 2023 enforcement actions against non-compliant entities under the European Central Bank's oversight; complementing these are robust data protection measures enshrined in the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679), which equips consumers against cyber-enabled fraud through rights to data portability, erasure, and breach notifications within 72 hours, bolstered by the Data Act (Regulation (EU) 2023/2854) facilitating secure data sharing in financial services while prohibiting unfair contractual terms, and the Digital Services Act (DSA, Regulation (EU) 2022/2065) that compels online platforms to deploy risk-based mitigation for systemic fraud risks including fake reviews and scams, with fines up to 6% of global turnover for violations; consumer protection further intensifies via the Consumer Credit Directive (Directive (EU) 2023/2225) mandating strong customer authentication under the revised Payment Services Directive (PSD3, Directive (EU) 2025 forthcoming) to thwart unauthorized transactions, and the Markets in Crypto-Assets Regulation (MiCA, Regulation (EU) 2023/1114) which licenses stablecoin issuers with capital reserves and redemption rights to shield retail investors from cyber-induced volatility, collectively forging a preemptive, layered policy ecosystem that not only reacts to cyber frauds but anticipates them through cross-sectoral interoperability and enforcement, offering a benchmark for India's nascent Digital Personal Data Protection Act 2023 and RBI cybersecurity directives.

COMPARATIVE LEGAL ANALYSIS: INDIA VS EUROPEAN UNION:

PARAMETER OF COMPARISON	INDIA	EUROPEAN UNION (EU)
Primary Legislation on Cyber Activities	Information Technology (IT) Act, 2000 (specifically Sections 66C for identity theft, 66D for cheating by personation) and the proposed	NIS 2 Directive (Directive 2022/2555) for high common level of cybersecurity and the Cyber Resilience Act for digital products.

	Digital India Act.	
Substantive Criminal Law	Bharatiya Nyaya Sanhita (BNS), 2023 (Sections penalizing cheating, forgery, and organized cybercrime), operating alongside the IT Act.	Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment. Criminal enforcement relies heavily on Member States' national laws.
Data Protection & Privacy Law	Digital Personal Data Protection (DPDP) Act, 2023. Focuses on digital personal data, consent, and fiduciary obligations with significant penalties for breaches.	General Data Protection Regulation (GDPR). Highly comprehensive; establishes a global standard for ata minimization, "privacy by design," and cross-border data transfers.
Payment & Financial Fraud Regulations	Reserve Bank of India (RBI) Guidelines (e.g., Master Direction on Digital Payment Security Controls) mandating multi-factor authentication and limiting customer liability.	Revised Payment Services Directive (PSD2 & PSD3). Mandates Strong Customer Authentication (SCA) and open banking security standards.
Intermediary Liability & Platform Safety	IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Requires swift takedowns of fraudulent content and strict grievance redressal mechanisms.	Digital Services Act (DSA). Establishes a tiered system of accountability for digital platforms to mitigate systemic risks, including cyber scams and deepfakes.
Institutional & Enforcement Bodies	CERT-In (Cyber Emergency Response Team), I4C (Indian Cyber Crime Coordination Centre), and state-level Cyber Police Stations.	ENISA (EU Agency for Cybersecurity), Europol's EC3 (European Cybercrime Centre), and Eurojust for cross-border judicial coordination.
Reporting Mechanisms	Centralized via the National Cyber Crime Reporting Portal (NCRP) and the 1930 helpline.	Decentralized at the national level (Member States' portals), but coordinated regionally via the

		CSIRTs Network.
International Cooperation	Not a signatory to the Budapest Convention (citing sovereignty concerns); relies on Mutual Legal Assistance Treaties (MLATs) and bilateral agreements.	Member states are signatories to the Budapest Convention on Cybercrime, Facilitating rapid cross-border evidence sharing and harmonization.

MAJOR LEGAL AND POLICY CHALLENGES

India's Bharatiya Nyaya Sanhita and the EU's Digital Services Act reveal striking asymmetries in tackling cyber frauds, where enforcement lags behind technological evolution.

- Jurisdictional Fragmentation in Cross-Border Cyber Frauds

  Cyber frauds thrive on the anonymity of digital borders, rendering traditional territorial jurisdiction obsolete; in India, Section 179 of the Bharatiya Nyaya Sanhita empowers extraterritorial application for offences against Indian computers, yet practical enforcement falters due to the absence of mutual legal assistance treaties with key fraud hubs like Nigeria or Southeast Asia, as seen in the 2023 NPCI phishing epidemic affecting millions. The EU fares better through the e- Evidence Regulation (2022/2554), which streamlines cross-border data access, but even here, conflicts arise with non-EU states, exemplified by stalled investigations into Russian-linked scams targeting Eurozone banks; this divergence underscores a policy void where India's bilateral pacts remain nascent compared to the EU's networked approach via Europol.

- Inadequate Harmonization of Substantive Offences

  Disparities in defining cyber frauds erode prosecutorial efficacy; India's IT Act 2000, supplemented by BNS provisions on cheating (Section 318), captures phishing and identity theft but omits nuanced variants like deepfake-enabled scams, leaving gaps exposed in cases like the 2024 SBI impersonation rackets. Conversely, the EU's Directive 2013/40 on Attacks Against Information Systems and the proposed Cyber Resilience Act (2022) impose uniform standards across member states for fraud facilitation, yet enforcement varies, with Germany's BKA reporting higher convictions than laxer jurisdictions like Romania; such inconsistencies demand a unified substantive framework, absent in India's federal structure where state police silos hinder

national cohesion.

- Resource and Capacity Deficits in Investigative Machinery

  Overburdened agencies amplify cyber fraud impunity; India's CERT-In logs over 1.5 million incidents annually but grapples with a mere 1,200 personnel against the EU's ENISA-backed ecosystem serving 450 million users with advanced forensic tools, as highlighted in the 2025 ENISA Threat Landscape Report. Indian challenges intensify through underfunded cyber cells— evident in the delayed response to the 2023 Paytm breach—while EU policies like the NIS2 Directive mandate public-private partnerships, though smaller states struggle with implementation; bridging this requires India to emulate EU's capacity-building via dedicated fraud fusion centers.

- Evolving Anonymity Tools Outpacing Regulatory Response

  Techniques like cryptocurrency mixers and VPN obfuscation shield fraudsters, outstripping static laws; India's FIU-IND guidelines under PMLA 2002 target virtual assets post-2023 amendments, yet evasion persists, as in the WazirX hack siphoning $230 million. The EU's MiCA Regulation (2023/1114) imposes stringent wallet traceability, curbing anonymity but facing pushback from privacy advocates under GDPR; India's policy lag, without equivalent KYC mandates for DeFi platforms, contrasts sharply, necessitating adaptive legislation attuned to blockchain's opacity.

- Victim Compensation and Remediation Gaps

  Restorative justice remains peripheral amid punitive focus; India's Consumer Protection Act 2019 offers limited redress via e-commerce guidelines, but cyber fraud victims recover pennies on the rupee, as RBI data shows sub-10% reimbursements in UPI scams. The EU's Payment Services Directive 2 (PSD2) enforces stronger reimbursement obligations up to €50, bolstered by the Digital Operational Resilience Act (DORA), yet disparities persist across borders; a comparative policy pivot toward mandatory insurance pools, blending India's UPI safeguards with EU models, could fortify victim-centric reforms.

- Data Protection-Privacy Tensions in Fraud Probes

  Balancing surveillance for fraud detection with privacy rights poses acute dilemmas;

India's DPDP Act 2023 permits broad government access sans robust oversight, risking abuse as critiqued in Justice B.N. Srikrishna Committee findings, while EU's GDPR imposes stringent DPIAs for fraud analytics, slowing probes like those into 2024 Revolut breaches. This tension reveals India's permissive stance versus EU's proportionality principle, urging harmonized safeguards to preempt rights erosions without compromising investigative vigor.

RECOMMENDATIONS AND POLICY REFORMS

- India must prioritize comprehensive legislative fortification to combat cyber frauds effectively, emulating the EU's robust framework under the Digital Services Act (DSA) and Cyber Resilience Act. Strengthening cyber fraud legislation demands amendments to the Information Technology Act, 2000, incorporating mandatory due diligence for online platforms akin to Article 34 of the DSA, which imposes risk-based obligations on intermediaries to mitigate systemic fraud risks. Such reforms would shift from India's reactive complaint-driven model under Section 66D to a proactive liability regime, compelling platforms like social media giants to deploy AI-driven fraud detection and swift content takedown protocols, thereby reducing the impunity currently enjoyed by digital enablers of scams.
- Drawing from the EU's integrated regulatory ecosystem, India should integrate cyber fraud provisions into a unified digital markets law, mirroring the DSA's tiered enforcement with fines up to 6% of global turnover. This would address gaps in the Indian Penal Code's fragmented application to cyber offenses, establishing clear extraterritorial jurisdiction over cross-border frauds similar to the EU's NIS2 Directive. By mandating annual compliance audits and a national cyber fraud registry, akin to the EU's transparency reporting under the DSA, Indian authorities could enhance traceability and deterrence, fostering a preventive culture that aligns with global standards while tailoring to India's digital economy scale.
- To bolster efficacy, India ought to cultivate international cybercrime cooperation mechanisms, inspired by the EU's Budapest Convention framework and Europol's Joint Cybercrime Action Taskforce (J-CAT). Formalizing bilateral treaties with key partners like the US and ASEAN nations, alongside accession to the Budapest Convention, would enable real-time data sharing and joint investigations, overcoming current hurdles under the Mutual Legal Assistance Treaty. Establishing a dedicated India-led Cyber

Fusion Centre, modeled on Europol's EC3, would facilitate cross-jurisdictional pursuit of fraud networks, integrating intelligence from CERT-In with international allies to dismantle transnational syndicates exploiting jurisdictional arbitrage.

- Enhancing cyber awareness and digital literacy emerges as a foundational pillar, replicating the EU's Digital Education Action Plan (2021-2027) which embeds cybersecurity modules in national curricula. India should launch nationwide campaigns through the National Cyber Crime Reporting Portal, partnering with schools, NGOs, and platforms for mandatory digital hygiene training, targeting vulnerable demographics like senior citizens who constitute 40% of UPI fraud victims per RBI data. Integrating AI-simulated phishing drills into Aadhaar- linked awareness apps, as seen in EU member states' public-private initiatives, would empower citizens, reducing victimization rates by cultivating a vigilant digital populace essential for sustainable fraud mitigation.
- At Last the creation of specialized cybercrime courts represents a structural imperative, patterned after the EU's specialized digital benches in Germany and the Netherlands under their e-Justice strategies. Amending the Code of Criminal Procedure to designate fast-track cyber divisions in high courts, equipped with forensic experts and block chain evidence protocols, would expedite resolutions beyond the current backlog plaguing Indian magistracy. Pilot programs in tech hubs like Bengaluru and Delhi, with dedicated funding from the Digital India corpus, would ensure judgments within 180 days, harmonizing procedural efficiency with substantive justice to restore public trust in the judicial response to cyber frauds.

CONCLSUION REMARK:

In conclusion, cyber fraud has emerged as a serious challenge in the rapidly expanding digital economies of both India and the European Union, requiring strong legal, institutional, and policy responses. The comparative analysis shows that while India has developed a foundational framework through laws such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023, enforcement gaps, jurisdictional challenges, and limited institutional capacity continue to hinder effective control of cyber fraud. In contrast, the European Union has adopted a more harmonized and preventive regulatory model through instruments such as the GDPR, Digital Services Act, NIS2 Directive, and coordinated institutional mechanisms like Europol’s EC3 and ENISA.

Despite these differences, both jurisdictions face common issues such as cross-border cybercrime, evolving technologies like AI- driven fraud, and the need for stronger international cooperation. Therefore, strengthening legal frameworks, improving institutional coordination, enhancing digital literacy, and promoting international collaboration remain essential for building a resilient cyber governance system capable of effectively preventing and responding to cyber fraud in the digital age.

REFERENCES:

- Yadav, A., & Pandey, R. (2025). Data Privacy across Borders: A Comparative Analysis of European Union and Indian Protection Laws. U. Bologna L. Rev., 10, 177.
- Kavyn, S., Bratsuk, I., & Lytvynenko, A. (2021). Regulatory and legal enforcement of cyber security in countries of the European Union: The experience of Germany and France. Teisė, 121, 135-147.
- Mugamba, E. (2025). Global Data Governance in Digital Law: A Comparative Analysis of EU and Global Approaches to Cybersecurity Legislation. Journal of Smart Computing and Quantum Technologies, 1(1), 1-19.
- Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues: In Cybercrimes, cybercriminals and their policing, in crime, law and social change. Crime, law and social change, 67(1), 3-20.
- Gojali, D. S. (2023). Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective. International Journal of Cyber Criminology, 17(1), 1-11.
- Chatterjee, S., Kar, A. K., Dwivedi, Y. K., & Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. Information Technology & People, 32(5), 1153-1183.
- Didenko, A. N. (2020). Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. Uniform Law Review, 25(1), 125-167.
- Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 11(4), 541-562.
- Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 45, 58-74.

- Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. Journal of Business Ethics, 180(2), 581-604.
- Chatterjee, S. (2019). Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective. International Journal of Law and Management, 61(1), 170-190.