CYBERCRIME LAWS IN INDIA: A COMPARATIVE LEGAL ANALYSIS IN THE CONTEXT OF EMERGING GLOBAL STANDARDS

Prabhash Dalei, Research Scholar & Assistant Professor, Department of Law, Utkal University, Bhubaneswar, Odisha

ABSTRACT

The rising incidence of cybercrime in India, marked by low conviction rates and limited international cooperation, highlights critical weaknesses in the country's current legal and enforcement framework. This paper offers a comparative analysis of India's cybercrime laws vis-à-vis the United Kingdom and the United States, focusing on legislative scope, institutional structures, and global treaty participation. While India relies primarily on the Information Technology Act, 2000, both the UK and USA operate under modern and specific laws such as the Computer Misuse Act 1990 and the Computer Fraud and Abuse Act 1986, supported by specialised enforcement agencies and advanced investigative tools. The UK and USA are also active participants in international instruments like the Budapest Convention and the United Nations Cybercrime Convention (2024), enabling cross-border cooperation and rapid access to digital evidence mechanisms that India currently lacks. The paper identifies gaps in India's statutory coverage of emerging threats such as deepfakes, AI-driven fraud, and ransomware, and evaluates enforcement bottlenecks resulting from under-resourced cyber cells and delays in evidence collection. Using a doctrinal and comparative approach, this study argues for legal reforms including the enactment of a dedicated cybercrime law, accession to key international treaties, strengthening of cyber forensic capacity, and public awareness initiatives. It concludes that without aligning its domestic framework with global standards, India risks falling behind in combating transnational cyber threats and fulfilling its obligations as a digital leader in the Global South.

Keywords: Cybercrime, India, Budapest Convention, International Cooperation, Comparative Legal Framework.

1. Introduction

In an age where digital connectivity underpins almost every aspect of life, cybercrime has emerged as one of the most rapidly evolving and pervasive threats. India, housing over 800 million internet users by mid-2024, stands at the epicentre of this global challenge. According to the National Crime Records Bureau (NCRB), cybercrime incidents surged from 52,974 cases in 2021 to 65,893 in 2022, marking a 24.4% increase, the highest annual tally recorded so far.[1] By early 2025, cumulative daily fraud complaints had reached nearly 7,000 per day, with total registered cases climbing from approximately 740,000 by May 2024 to over 1.2 million by September 2024. These figures are alarming signals of a cyber-offence epidemic unfolding across urban and rural India alike.

Financial cybercrime, constituting nearly 65% of all offences in 2022, caused estimated losses of over ₹22,812 crore in that year alone, contributing to a four-year total of ₹33,165 crore. Sextortion and AI-enabled fraud have been among the most dramatic emerging threats, as evidenced by a recent Delhi case involving fake SIM issuance and synthetic bank accounts used to extort over 100 victims.[2] Alongside these, cyberbullying, deepfake impersonation, digital defamation, and ransomware are increasingly common particularly impacting women and minors; one in three Indian children reportedly faces online bullying.

Cybercrime complaints in India have seen a staggering 900% rise over the past four years, jumping from 1.37 lakh in 2021 to 17.1 lakh in 2024. During this period, financial losses have crossed ₹33,000 crore, with ₹22,812 crore lost in 2024 alone. This alarming increase is attributed to AI-enabled scams, phishing attacks, "digital arrest" frauds, and poor cyber literacy. Tier-2 and Tier-3 cities are increasingly becoming vulnerable targets due to limited awareness and digital safeguards.[3]

Despite the surge in offences, judicial enforcement remains alarmingly weak. Across India, only 1.6% of cybercrime cases resulted in convictions in 2022 a marginal recovery from 0.93%

[1] National Crime Records Bureau, *Crime in India 2022* (Ministry of Home Affairs, Government of India 2023) https://ncrb.gov.in accessed 10 June 2025.
[2] 'Police Bust Sextortion Racket Using Fake SIM Cards and Synthetic Accounts in Delhi' *The Times of India* (18 June 2025) <https://timesofindia.indiatimes.com/city/delhi/police-bust-sextortion-racket-using-fake-sim-cards-and-synthetic-accounts-in-delhi/articleshow/121934480.cms> accessed 14 July 2025.
[3] 'Cyber Frauds Jump 900% in 4 Years: Small Cities like Deoghar, Nuh, Mathura Emerge as New Scam Capitals | India News - The Indian Express' <https://indianexpress.com/article/india/cybercrime-sharp-rise-complaints-2024-govt-data-9816845/> accessed 14 July 2025.

in 2021.[4] The overall charge-sheeting rate stands at a modest 29.6%, reflecting challenges in evidence gathering, inter-agency coordination, and procedural compliance. These low conviction figures are symptomatic of broader systemic deficiencies in investigative capacity and prosecutorial rigor.

India's response has included several structural interventions. The Indian Cyber Crime Coordination Centre (I4C), established under the Ministry of Home Affairs, now oversees multi-layered cybercrime management, ranging from forensic support to specialized task forces. The National Cyber Forensic Laboratory in coordination with CERT-IN also provide technical backbone support. While these developments mark a significant progress, implementation gaps persist, especially at state levels and in international cooperation.

These trends underscore the urgency for alignment with global norms and cross-border frameworks. India has yet to accede to the Council of Europe's Budapest Convention (2001), which remains the cornerstone of international cybercrime cooperation. In contrast, the UK and the USA are fully engaged participants: the UK aligns with EU and bilateral protocols, while the US actively participates in policy diplomacy, enforcement treaties, and cloud legislation like the CLOUD Act.

A significant development in global cyber law is the adoption of the United Nations Cybercrime Convention in December 2024 (UNGA Resolution 79/243). This new treaty, negotiated under the UN Ad Hoc Committee, aims to create a universal framework for combatting cybercrime, enabling cross-border evidence exchange and procedural safeguards. Although India participated in the negotiations, its formal position on signing remains pending raising questions about its readiness to integrate with this evolving multilateral regime.

Through a comparative lens, this article examines how India's cybercrime legislation fares against established benchmarks set by the UK and the US. By analysing definitions, enforcement architecture, treaty adoption, and jurisdictional cooperation, the paper aims to highlight policy gaps and identify viable pathways for reform. The goal is to strengthen India's cybercrime legal infrastructure boosting conviction rates, enhancing international collaboration, and future-proofing the regime against next-generation offences.

[4] 'Only 1.6% Conviction Rate in 2 Yrs amid Surge in Cybercrime Cases' (*The Tribune*) <https://www.tribuneindia.com/news/india/only-1-6-conviction-rate-in-2-yrs-amid-surge-in-cybercrime-cases-2/> accessed 15 July 2025.

2. International Legal Framework Governing Cybercrime

India's cybercrime legislative gaps must be understood within the global context, underpinned by three principal pillars i.e. the Council of Europe's Budapest Convention (2001), the newly adopted UN Convention on Cybercrime (2024), and the action taken by international cooperation mechanisms and agencies.

2.1 The Budapest Convention (2001)

The 2001 Convention on Cybercrime was the first binding global treaty designed to harmonise substantive and procedural criminal law, and to promote rapid cross-border cooperation, particularly in e-evidence preservation and transfer.[5] As of June 2025, it counts around 80 ratifying States including the UK and the USA and additional signatories like Ireland and South Africa.[6] Notably, India has declined accession, citing its non-involvement in drafting and sovereignty concerns over international data sharing.[7] Meanwhile the USA ratified the Convention in 2007, and the UK has incorporated its standards through EU obligations and bilateral accords.

2.2 The UN Cybercrime Convention (2024)

On 24 December 2024, the UN General Assembly adopted the United Nations Convention against Cybercrime, under Resolution 79/243, following a five-year negotiation by an Ad Hoc Committee.[8] This treaty establishes comprehensive procedural mechanisms such as expedited preservation and disclosure of electronic evidence, mutual legal assistance (MLATs), and 24/7 points of contact set to open for signature in October 2025 in Hanoi and at UN Headquarters until December 2026.[9] It requires forty ratifications to enter into force and explicitly extends cooperation to serious crimes like terrorism, trafficking, and corruption.[7] While emphasizing international cooperation, it preserves human rights safeguards by referencing existing instruments rather than embedding new ones. India participated actively in drafting sessions

[5] 'About the Convention - Cybercrime' <https://www.coe.int/en/web/cybercrime/the-budapest-convention> accessed 14 July 2025.
[6] Ibid
[7] Ibid
[8] ' UN Convention against Cybercrime' <https://documents.un.org/doc/undoc/ltd/v24/055/06/pdf/v2405506.pdf> accessed 14 July 2025.
[9] Ibid

but has yet to publicly commit to signature or ratification raising pivotal questions about its engagement with the most universal legal framework of cybercrime governance.

2.3 Role of International Organisations and Mechanisms

Beyond formal treaty frameworks, several international and regional organisations play a vital role in shaping global cybercrime standards. The United Nations Office on Drugs and Crime (UNODC) serves as the Secretariat to the 2024 UN Cybercrime Convention, providing legal and technical support to member states, particularly developing countries, to build capacity and legislative readiness.[10] INTERPOL plays a crucial enforcement role by coordinating cybercrime intelligence globally, facilitating real-time information exchange, and operating technical tools such as email tracing systems, malware analysis hubs, and digital forensics support platforms.[11] The Council of Europe, in addition to managing the Budapest Convention, has continued to evolve its jurisdictional scope through the adoption of Additional Protocols, especially those addressing xenophobic and racist expressions committed through computer systems, thereby expanding the Convention's reach to address hate speech and extremist content online.[12] Regional organisations such as the Association of Southeast Asian Nations (ASEAN), the Organization of American States (OAS), the Asia-Pacific Economic Cooperation (APEC), and the Organisation for Economic Co-operation and Development (OECD) have developed non-binding but influential cybercrime and cybersecurity frameworks. These guidelines promote harmonised definitions of cyber offences, facilitate cross-border data sharing protocols, and encourage legal convergence across their respective regions, laying the groundwork for broader multilateral adoption of cyber norms and legislative coherence.

2.4 India's Standing and Obligations Under International Law

Despite not being a party to either the Budapest Convention (2001) or the newly adopted United Nations Cybercrime Convention (2024), India remains bound by broader principles of international cooperation under public international law. Articles 1 and 2 of the UN Charter impose a duty on all member states to promote international peace, security, and cooperation

[10] 'Ad Hoc Committee - Home' (*United Nations : Office on Drugs and Crime*) <//www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home> accessed 14 July 2025.
[11] 'Cybercrime' <https://www.interpol.int/Crimes/Cybercrime> accessed 14 July 2025.
[12] 'First Additional Protocol - Cybercrime - Www.Coe.Int' (*Cybercrime*) <https://www.coe.int/en/web/cybercrime/first-additional-protocol> accessed 14 July 2025.

including in the suppression of transnational crime.[13] India's participation in INTERPOL, its adherence to certain Mutual Legal Assistance Treaty (MLAT) frameworks, and recent negotiations with global cloud service providers for data access mechanisms demonstrate a degree of informal alignment with global cyber norms.[14] However, this informal engagement has limitations. The absence of treaty obligations leaves Indian law enforcement without clear legal authority or structured channels for requesting or sharing electronic evidence across borders. The existing MLAT system, which India relies on, is often criticised for excessive bureaucratic delays, inconsistent agency responses, and poor coordination factors that hinder timely investigations. Moreover, India's domestic cyber laws, particularly the Information Technology Act, 2000, lack procedural harmonisation with international instruments, such as standardized data preservation orders, emergency access protocols, and admissibility standards, which are already present in the legal systems of countries that are parties to the Budapest or UN Conventions.

International legal instruments such as the Budapest Convention and the UN Cybercrime Convention (2024) offer comprehensive frameworks for harmonising substantive cyber offences, enhancing procedural cooperation, and facilitating timely cross-border investigations. While the UK and USA benefit from these structured legal alignments, India's absence from such treaties leaves its enforcement efforts fragmented and internationally constrained. To address the rising complexity and transnational nature of cybercrime, India must consider formal accession to these conventions and update its domestic procedures to reflect globally harmonised standards.

3. India's Cybercrime Legal and Institutional Framework

India's legal response to cybercrime is primarily grounded in the Information Technology Act, 2000 (IT Act) and supplemented by relevant provisions of the Indian Penal Code, 1860 (IPC) which has now been repealed and replaced by the Bharatiya Nyaya Sanhita (BNS), 2023. While these laws provide a basic framework for addressing cyber offences, they remain inadequate in addressing the scale, complexity, and transnational nature of modern cybercrime.

[13] United Nations, 'United Nations Charter (Full Text)' (*United Nations*) <https://www.un.org/en/about-us/un-charter/full-text> accessed 14 July 2025.
[14] 'Mutual Legal Assistance in Criminal Matters' (*Ministry of External Affairs, Government of India*) <https://mea.gov.in/mutual-legal-assistance-in-criminal-matters.htm> accessed 14 July 2025.

3.1 Statutory Framework

India's principal statutory foundation for addressing cybercrime is the Information Technology Act, 2000 (IT Act), which was enacted to facilitate electronic governance, regulate e-commerce, and criminalise unauthorised access or misuse of computer systems. Following a major amendment in 2008, the Act introduced several offence-specific provisions including Section 66C (identity theft), Section 66D (cheating by personation using computer resources), Section 66E (violation of privacy), Section 66F (cyber terrorism), and Section 67 (publishing or transmitting obscene material online).[15] While the IT Act provides the core penal provisions, several cyber-related offences continue to be prosecuted under the Indian Penal Code, 1860, which has now been repealed and replaced by the Bharatiya Nyaya Sanhita (BNS), 2023. Under the BNS, corresponding provisions for cyber-enabled offences include Section 318 (cheating), Section 351 (criminal intimidation), and Section 356 (defamation), though these were originally codified under Sections 420, 503, and 499 of the IPC respectively.[16] However, there is still no standalone chapter in the BNS dedicated exclusively to technology-driven offences. This results in dual applicability of the IT Act and BNS for many cases, which frequently causes jurisdictional confusion, poor charge framing, and ambiguities during trial, particularly when procedural safeguards differ across statutes. The absence of harmonisation between general criminal law and specialised cyber legislation creates operational difficulties for both investigators and prosecutors.

3.2 Institutional Mechanisms

India's institutional response to cybercrime has evolved significantly in recent years, with the Indian Cyber Crime Coordination Centre (I4C), launched by the Ministry of Home Affairs in 2020, serving as the national nodal agency for cybercrime investigation and capacity building. I4C manages multiple operational arms, including the National Cyber Crime Reporting Portal and the toll-free cybercrime helpline 1930, and supports the development of state-level cybercrime police units to ensure decentralised enforcement.[17] Complementing I4C's mandate, the Computer Emergency Response Team-India (CERT-IN) operates under the Ministry of Electronics and Information Technology (MeitY). CERT-IN is tasked with real-time threat

[15] Information Technology Act 2000, ss 66C, 66D, 66E, 66F, and 67.
[16] Bharatiya Nyaya Sanhita 2023, ss 316, 351, 354; previously Indian Penal Code 1860, ss 420, 506, 499.
[17] Ministry of Home Affairs, 'Indian Cyber Crime Coordination Centre (I4C)' https://cybercrime.gov.in accessed 25 June 2025.

detection, incident response, vulnerability advisories, and international coordination with other national CERTs.[18] It also plays a regulatory role by issuing sector-specific cybersecurity directives, especially for banking, telecom, and critical infrastructure systems, often mandating log maintenance, breach disclosures, and periodic audits. In terms of investigation, the Cyber Crime Unit of the Central Bureau of Investigation (CBI) handles high-profile and transnational cybercrime cases, particularly those involving data breaches, online fraud networks, and cyber extortion. Several states most notably Telangana and Maharashtra have also established dedicated cybercrime bureaus equipped with digital forensic laboratories, technical experts, and capacity-building initiatives, thereby setting models of institutional best practice for other regions to emulate. Despite these advances, disparities in training, infrastructure, and coordination persist across different jurisdictions, creating inconsistent enforcement outcomes.

3.3 Policy Developments and Limitations

In recent years, India has made visible efforts to modernise its cyber governance framework. The National Cyber Security Policy (2013) laid early groundwork for securing digital infrastructure, while the ongoing proposal for a Digital India Act aims to replace the outdated IT Act with a more adaptive and forward-looking legal instrument. Additionally, CERT-IN has issued critical policy directives, including the 2022 guidelines on data localisation and grievance redressal, as well as sector-specific compliance mandates that require organisations to maintain logs for 180 days and report incidents within strict timelines.[19]

Despite these steps, several policy and operational gaps persist. There is a lack of procedural clarity when it comes to accessing cross-border electronic evidence, which hampers investigations involving foreign tech platforms. India also lacks fast-track cybercrime courts, even as case volumes increase dramatically. Most district police units remain undertrained and under-equipped, particularly in rural areas, making early-stage investigation of digital offences difficult. Critically, India's legal framework has not yet defined emerging cyber offences such as deepfake fraud, sextortion, or cryptocurrency scams, leaving grey areas in prosecution.

These structural and legal gaps reflect in outcomes. As per the National Crime Records Bureau (NCRB), only 1.6% of cybercrime cases resulted in convictions in 2022, despite over 65,000

[18] Ministry of Electronics and Information Technology (MeitY), 'Role and Responsibilities of CERT-IN' https://www.cert-in.org.in accessed 25 June 2025.
[19] Ministry of Electronics and Information Technology (MeitY), 'CERT-IN Guidelines under Section 70B of the IT Act' (28 April 2022) https://www.cert-in.org.in accessed 25 June 2025.

cases being registered that year.[20] The core reason remains the challenge of collecting admissible, jurisdictionally valid digital evidence especially when servers, data, or suspects are located abroad.

3.4 International Cooperation Shortfalls

India's participation in Mutual Legal Assistance Treaties (MLATs) is hindered by delays, lack of trained personnel, and the absence of a cybercrime-specific cooperation framework. The country has not signed the Budapest Convention and, as of mid-2025, has not clarified its position on the 2024 UN Cybercrime Convention, limiting its ability to engage in structured, rule-based collaboration.[21] This leaves Indian agencies without reliable legal pathways for timely cross-border data access. By contrast, the USA's CLOUD Act and the UK's treaty-based systems enable efficient digital evidence sharing and prosecution. India's reliance on bilateral and ad hoc mechanisms is ill-suited to the real-time demands of cybercrime.[22]

Although institutions like CERT-IN and I4C reflect policy progress, the overall architecture remains fragmented and under-resourced. Without a comprehensive cybercrime statute and stronger international treaty participation, enforcement gaps persist. As threats like AI-enabled fraud and ransomware grow, India must modernise its laws and align with global standards.[23]

4. UK Cybercrime Framework: Legal and Policy Approach

The United Kingdom has developed a comprehensive and layered legal framework to combat cybercrime, combining robust legislation, strategic institutional structures, and active international cooperation. As a signatory to the Budapest Convention, the UK is fully integrated into global cybercrime governance systems, making it a valuable comparative model for India.

---

[20] National Crime Records Bureau, *Crime in India 2022* (Ministry of Home Affairs, 2023) https://ncrb.gov.in accessed 25 June 2025.

[21] Council of Europe, 'Chart of Signatures – Convention on Cybercrime (ETS No. 185)' https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures accessed 25 June 2025; UNGA Res 79/243, *United Nations Convention on Cybercrime* (adopted 24 December 2024).

[22] U.S. Department of Justice, 'The CLOUD Act' https://www.justice.gov/cloudact accessed 25 June 2025; UK Government, *National Cyber Strategy 2022–2030* https://www.gov.uk/government/publications/national-cyber-strategy-2022-to-2030 accessed 25 June 2025.

[23] Ministry of Electronics and IT (MeitY), 'Indian Computer Emergency Response Team (CERT-IN)' https://www.cert-in.org.in accessed 25 June 2025; Ministry of Home Affairs, 'Indian Cyber Crime Coordination Centre (I4C)' https://www.mha.gov.in accessed 25 June 2025.

4.1 Legislative Framework

The primary legislation governing cybercrime in the United Kingdom is the Computer Misuse Act 1990, which was enacted to criminalise unauthorised access to computer systems. The Act has evolved through multiple amendments to address new technological threats. Its key provisions include section 1, which penalises basic hacking or unauthorised access to computer material; section 2, which deals with unauthorised access with intent to commit further offences; section 3, which covers unauthorised acts with intent to impair the operation of a computer; and section 3ZA, which targets unauthorised acts causing serious damage, particularly to infrastructure.[24] The Data Protection Act 2018, incorporating the UK General Data Protection Regulation (UK GDPR), further enhances data protection by imposing stringent obligations on data controllers and empowering the Information Commissioner's Office (ICO) to impose penalties for breaches.[25] The Serious Crime Act 2015 expanded the scope of cybercrime by introducing specific offences related to the use of malware and increasing penalties under the CMA.[26] In addition to these core statutes, cyber-enabled offences are also addressed under the Fraud Act 2006 for online fraud, the Sexual Offences Act 2003 for cyberstalking or online grooming, and the Terrorism Act 2006, which addresses the dissemination of terrorist content through digital platforms.[27]

4.2 Enforcement and Institutional Mechanisms

The United Kingdom adopts a multi-agency model for cybercrime enforcement, ensuring a coordinated response across technical, investigative, and public-facing dimensions. The National Cyber Security Centre (NCSC), operating under GCHQ, serves as the lead technical authority, focusing on national cybersecurity resilience, intelligence coordination, and the protection of critical infrastructure.[28] The National Crime Agency (NCA) leads criminal investigations through its National Cyber Crime Unit (NCCU), which specialises in tackling serious and organised cyber offences including ransomware attacks, darknet market operations, and coordinated cross-border cybercriminal activity.[29] The UK also operates Action Fraud, a dedicated national reporting centre for cybercrime and fraud complaints, which works in

[24] *Computer Misuse Act 1990*, ss 1–3ZA.
[25] *Data Protection Act 2018* and *UK GDPR*, retained under the European Union (Withdrawal) Act 2018.
[26] *Serious Crime Act 2015*, s 44, amending the *Computer Misuse Act 1990*.
[27] *Fraud Act 2006*; *Sexual Offences Act 2003*; *Terrorism Act 2006*.
[28] National Cyber Security Centre, 'About NCSC' https://www.ncsc.gov.uk accessed 25 June 2025.
[29] National Crime Agency, 'Cyber Crime' https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime accessed 25 June 2025.

tandem with law enforcement for case triaging and referral. Additionally, local police forces maintain Cyber Crime Units, which are linked and supported through Regional Organised Crime Units (ROCUs) to ensure expertise is pooled and shared across jurisdictions. In recent years, UK enforcement bodies have significantly expanded their capabilities in areas such as digital forensics, threat intelligence, and public–private sector collaboration, particularly in relation to phishing, financial fraud, corporate ransomware, and child sexual abuse material (CSAM). The government also supports public education through national initiatives such as Cyber Aware, which encourages safe online practices and provides guidance on identifying and reporting cyber incidents.[30]

4.3 Policy and Strategic Initiatives

The UK has adopted several strategic frameworks to strengthen its cyber resilience. The UK National Cyber Strategy 2022–2030 aims to establish the country as a global "cyber power" through investment in skills, innovation, and law enforcement.[31] The Cyber Security Breaches Survey, published annually, tracks digital vulnerabilities across sectors. The creation of the UK Cyber Security Council has supported professional standards and capacity building, while the FCDO promotes international cyber norms. Post-Brexit, the UK maintains cyber cooperation through bilateral and multilateral treaties, continues to operate under the Budapest Convention, engages in INTERPOL's cybercrime operations, and remains a core part of the Five Eyes alliance, reinforcing its global cyber diplomacy.[32]

4.4 Legal and Practical Strengths

The United Kingdom's cybercrime framework offers several legal and practical strengths that serve as valuable reference points for India. The presence of dedicated cybercrime statutes, such as the Computer Misuse Act 1990, provides legal clarity and precise classification of offences, reducing ambiguities in prosecution.[33] Specialised enforcement units like the National Cyber Crime Unit (NCCU) and local Cyber Crime Units under Regional Organised

[30] UK Government, 'Cyber Aware' https://www.cyberaware.gov.uk accessed 25 June 2025.
[31] UK Government, *National Cyber Strategy 2022–2030* (15 December 2021) https://www.gov.uk/government/publications/national-cyber-strategy-2022-to-2030 accessed 25 June 2025.
[32] Council of Europe, 'Chart of Signatures – Convention on Cybercrime' https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures accessed 25 June 2025; INTERPOL, 'Cybercrime' https://www.interpol.int/en/Crimes/Cybercrime accessed 25 June 2025.
[33] *Computer Misuse Act 1990*, ss 1–3ZA.

Crime Units (ROCUs) ensure faster, expert-led investigations.[34] The UK's strong alignment with international treaties and norms, particularly the Budapest Convention, facilitates efficient cross-border cooperation and timely access to electronic evidence.[35] Additionally, the government emphasises public engagement and training, including initiatives like Cyber Aware, which promote online safety and awareness among individuals and businesses.[36] Crucially, institutional accountability mechanisms such as the powers of the Information Commissioner's Office (ICO) to investigate and penalise data breaches to ensure that organisations and data controllers remain legally compliant.[37]

5. USA's Cybercrime Framework: Federal and International Dimensions

The United States has developed one of the most comprehensive cybercrime legal regimes globally, combining statutory clarity, institutional strength, and active global leadership. As a founding signatory to the Budapest Convention (2001) and a vocal proponent of the 2024 UN Cybercrime Convention, the USA has consistently shaped international cyber governance norms. Its legal approach integrates federal criminal law, regulatory oversight, and proactive diplomacy.

5.1 Federal Statutes on Cybercrime

At the heart of the United States' cybercrime legislation is the Computer Fraud and Abuse Act (CFAA), 1986, codified under 18 U.S. Code § 1030. The CFAA criminalises unauthorised access to protected computers, computer-related fraud, transmission of malicious code, and extortion through digital threats.[38] Notably, it has extraterritorial application, covering offences involving any computer system affecting interstate or foreign commerce. Recent judicial rulings, however, have limited its interpretation to exclude minor terms-of-service violations.[39] Complementing the CFAA are other critical laws: the Electronic Communications Privacy Act (ECPA), 1986, which regulates state access to stored digital communications; the USA PATRIOT Act (2001), which expanded surveillance powers for national security; the Identity

[34] *National Crime Agency*, 'Cyber Crime Unit' https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime accessed 25 June 2025.
[35] *Council of Europe*, 'Chart of Signatures – Convention on Cybercrime (ETS No. 185)' https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures accessed 25 June 2025.
[36] *UK Government*, 'Cyber Aware' https://www.cyberaware.gov.uk accessed 25 June 2025.
[37] *Information Commissioner's Office (ICO)*, 'Enforcement Action' https://ico.org.uk/action-weve-taken/enforcement/ accessed 25 June 2025.
[38] 18 USC § 1030 (Computer Fraud and Abuse Act, 1986).
[39] *Van Buren v United States* 593 US (2021).

Theft Enforcement and Restitution Act (2008), streamlining prosecution of cyber extortion; and the Defend Trade Secrets Act (2016), which targets online intellectual property theft.

5.2 Enforcement Agencies and Cybercrime Infrastructure

The United States operates a multi-agency cyber enforcement system, with the Federal Bureau of Investigation (FBI) leading both domestic and international cybercrime investigations through its dedicated Cyber Division. The Department of Justice (DOJ) prosecutes cyber offences via the Computer Crime and Intellectual Property Section (CCIPS), focusing on computer intrusion, intellectual property theft, and transnational crime. The Department of Homeland Security (DHS), through the Cybersecurity and Infrastructure Security Agency (CISA), oversees national resilience and protection of critical digital infrastructure.[40] The U.S. Secret Service specialises in financial fraud, identity theft, and counterfeiting, while the National Security Agency (NSA) and Cyber Command manage offensive and defensive cyber operations tied to national security.[41] Public-private collaboration is encouraged through initiatives like InfraGard, a joint FBI-industry platform that promotes cyber threat intelligence sharing and cooperative incident response across sectors.

5.3 International Cooperation and Leadership

The United States plays a leading role in global cybercrime enforcement. It ratified the Budapest Convention in 2006, aligning its domestic laws with international cyber norms.[42] The US has MLATs with over 70 nations and frequently engages in cross-border investigations. Key tools include the CLOUD Act (2018), which permits approved countries like the UK to request data directly from US tech firms, bypassing MLAT delays.[43] The US also participates in the 24/7 network for emergency data preservation. Additionally, it was a major contributor to the 2024 UN Cybercrime Convention, advocating standardised procedures and safeguards for due process.[44]

[40] Cybersecurity and Infrastructure Security Agency (CISA), 'About CISA' https://www.cisa.gov accessed 25 June 2025.
[41] United States Department of Defense, 'US Cyber Command' https://www.cybercom.mil accessed 25 June 2025.
[42] Council of Europe, 'Budapest Convention Status' https://www.coe.int accessed 25 June 2025.
[43] US Department of Justice, 'CLOUD Act' https://www.justice.gov/cloudact accessed 25 June 2025.
[44] UNGA Res 79/243, *UN Cybercrime Convention* (adopted 24 December 2024).

5.4 Key Cybercrime Trends and Challenges

The United States faces a broad spectrum of cyber threats ranging from ransomware attacks on hospitals and schools to state-sponsored espionage and illicit activity on the dark web. In 2023, the FBI's Internet Crime Complaint Center (IC3) received over 880,000 complaints, with reported losses exceeding $12.5 billion USD, the highest recorded to date.[45] Key emerging challenges include jurisdictional disputes over transnational evidence, conflicts between encryption and lawful access, the misuse of AI and deepfakes in scams, and tensions over data sovereignty with allies and platforms abroad. In response, the DOJ's International Strategy on Cybercrime (2022) advocates global legal harmonisation, enhanced technical cooperation, and measures against authoritarian misuse of cyberspace.[46]

6. Comparative Analysis: India, UK, and USA

The contrasting approaches of India, the United Kingdom, and the United States in addressing cybercrime reveal key insights into legal maturity, institutional readiness, and international engagement. A comparative framework helps identify the structural strengths of UK-US models and the gaps India needs to address to become globally interoperable in cybercrime governance.

6.1 Legislative Structure and Offence Classification

India's principal cyber legislation the Information Technology Act, 2000, amended in 2008 remains narrower in scope and less precise than the UK's Computer Misuse Act 1990 and the US Computer Fraud and Abuse Act (CFAA).[47] India follows a hybrid model by using the IT Act alongside provisions from the Indian Penal Code (IPC), often resulting in overlapping charges and procedural inconsistencies. In contrast, the UK and USA rely on clear, standalone statutes that define and criminalise acts like hacking, denial-of-service attacks, identity theft, and online grooming.[48] The CFAA includes extraterritorial application, while the UK's CMA has expanded to address infrastructure and national security threats. Notably, India still lacks

[45] FBI Internet Crime Complaint Center (IC3), *2023 Internet Crime Report* (March 2024) https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf accessed 25 June 2025.
[46] US Department of Justice, *International Strategy on Cybercrime* (April 2022) https://www.justice.gov/ag/page/file/1483516/download accessed 25 June 2025.
[47] Information Technology Act 2000; Computer Misuse Act 1990 (UK); Computer Fraud and Abuse Act 1986, 18 USC § 1030 (USA)
[48] Serious Crime Act 2015 (UK); Defend Trade Secrets Act 2016 (USA).

dedicated statutory provisions for emerging offences such as deepfakes, crypto fraud, and AI-driven phishing, which the UK and USA have begun to address through modernised legislation.[49]

6.2 Enforcement Infrastructure

India's cybercrime enforcement infrastructure remains relatively centralised and under-resourced. Core institutions like the Indian Cyber Crime Coordination Centre (I4C) and CERT-IN lead national efforts but face significant limitations at the state and district levels, where law enforcement personnel often lack adequate training in digital forensics and cyber investigation.[50] In contrast, the UK follows a decentralised model with Regional Cyber Crime Units operating under Regional Organised Crime Units (ROCUs), supported by national agencies such as the National Crime Agency (NCA), National Cyber Security Centre (NCSC), and Action Fraud. The United States maintains a robust multi-agency structure involving the FBI, DOJ, DHS, and Secret Service, working in coordination with the private sector via initiatives like InfraGard and the Cybersecurity and Infrastructure Security Agency (CISA).[51] India's conviction rate for cybercrime remains critically low only 1.7% in 2022, with a charge-sheeting rate of 29.6% indicating systemic enforcement weaknesses less prevalent in the UK and USA.[52]

6.3 International Cooperation and Treaty Participation

A major point of divergence between India and its Western counterparts lies in treaty participation. Both the United Kingdom and the United States are parties to the Budapest Convention on Cybercrime, which allows them to operate within a harmonised legal and procedural framework for cross-border investigations.[53] They also participate in 24/7 cybercrime networks, Mutual Legal Assistance Treaties (MLATs), and real-time access models like the CLOUD Act, facilitating swift exchange of digital evidence. In contrast, India has

[49] Van Buren v United States 593 US ___ (2021); UK Home Office, *Cyber Security Breaches Survey 2024* (Gov.uk, April 2024).
[50] Ministry of Home Affairs, 'Indian Cyber Crime Coordination Centre (I4C)' https://www.mha.gov.in accessed 25 June 2025; CERT-IN, 'About Us' https://www.cert-in.org.in accessed 25 June 2025.
[51] UK Home Office, *Cyber Security Strategy 2022 to 2030* (Gov.uk, 2022); US Department of Homeland Security, 'Cybersecurity and Infrastructure Security Agency' https://www.cisa.gov accessed 25 June 2025.
[52] National Crime Records Bureau (NCRB), *Crime in India Report 2022* https://ncrb.gov.in accessed 25 June 2025.
[53] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime' https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures accessed 25 June 2025.

neither signed the Budapest Convention nor ratified the 2024 United Nations Cybercrime Convention, which limits its legal capacity to engage in structured international cooperation.[54] This exclusion hampers India's ability to access data hosted overseas and contributes to lengthy delays in MLAT responses. Without pre-negotiated protocols, cyber investigations and extradition efforts are often inefficient and inconsistent.

6.4 Institutional and Public Engagement

The United Kingdom and the United States emphasise continuous public engagement, cybersecurity education, and institutional capacity building as integral components of their cybercrime frameworks. Public awareness initiatives such as the UK's Cyber Aware campaign and the US's Stop.Think.Connect. program have significantly improved citizen-level digital hygiene and threat response. India, by contrast, lacks a comparable, government-backed nationwide cyber awareness campaign with consistent reach and funding. Additionally, the UK and US operate under comprehensive national cybersecurity strategies that include multi-year funding plans, defined performance metrics, and cross-sectoral collaboration. India's National Cyber Security Policy (2013) is widely considered outdated, and the proposed Digital India Act remains under consultation as of mid-2025, lacking legislative enactment and implementation frameworks.[55]

6.5 Legal Culture and Case Law Development

The United States and United Kingdom possess well-developed cyber jurisprudence, with landmark rulings that refine the scope of lawful access, digital privacy, and admissibility of electronic evidence. In the US, the Supreme Court's decision in *Van Buren v United States*[56] significantly narrowed the interpretation of "unauthorized access" under the Computer Fraud and Abuse Act (CFAA), clarifying that violations of internal use policies do not constitute criminal offences.[57] In contrast, India's cybercrime case law remains underdeveloped, with

[54] UNGA Res 79/243, *United Nations Convention on Cybercrime* (adopted 24 December 2024) https://www.unodc.org accessed 25 June 2025.
[55] Ministry of Electronics and IT, 'Draft Digital India Act 2023' https://www.meity.gov.in accessed 25 June 2025; UK Cabinet Office, *National Cyber Strategy 2022* https://www.gov.uk/government/publications/national-cyber-strategy-2022 accessed 25 June 2025; US Cybersecurity and Infrastructure Security Agency (CISA), 'Stop.Think.Connect.' https://www.cisa.gov accessed 25 June 2025.
[56] 593 U.S. 374 (2021)
[57] *Van Buren v United States* 593 US (2021) https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf accessed 25 June 2025.

courts frequently applying general criminal law provisions, such as those in the Indian Penal Code, leading to fragmented and inconsistent legal interpretations of cyber offences.

7. Conclusion and Recommendations

The comparative analysis of India's cybercrime framework with that of the United Kingdom and the United States highlights a pronounced divergence in legislative specificity, enforcement capacity, and international legal integration. While India has taken foundational steps to develop cybercrime governance mechanisms through the Information Technology Act, 2000 and the Indian Cyber Crime Coordination Centre (I4C), it continues to grapple with fragmented procedures, low conviction rates, limited treaty participation, and a reactive policy environment.

In contrast, the United Kingdom and the United States exemplify proactive and well-structured responses. Both countries have enacted standalone cybercrime statutes the UK's Computer Misuse Act 1990 and the US's Computer Fraud and Abuse Act 1986 that comprehensively define offences, address critical infrastructure, and enable extraterritorial application. These laws are regularly amended to meet emerging threats, including ransomware, online grooming, deepfakes, and crypto-enabled crimes. India, on the other hand, still lacks explicit statutory coverage of these modern offence types.

Institutionally, the UK and US cybercrime enforcement ecosystems operate through specialised agencies with clear jurisdiction, technical capabilities, and inter-agency coordination. Bodies like the NCSC, FBI Cyber Division, and NCA are supported by legislative mandates and cyber-specific resources. India's enforcement structure, although evolving, remains largely centralised, underfunded at the grassroots level, and often disconnected from global investigative processes. The dismal conviction rate of 1.6% in 2022, coupled with a charge-sheeting rate of under 30%, reflects the need for deep reforms in investigation protocols, digital forensics capacity, and judicial training.

On the international front, India's absence from the Budapest Convention and hesitance in ratifying the 2024 UN Cybercrime Convention severely limits its ability to access cross-border electronic evidence or engage in expedited legal cooperation. In contrast, both the UK and the US actively benefit from these frameworks, using Mutual Legal Assistance Treaties (MLATs), 24/7 networks, and agreements like the CLOUD Act to streamline evidence access and

accelerate prosecutions.

To address these structural and policy shortcomings, several recommendations can be advanced:

1. **Legislative Modernisation**: India must adopt a dedicated and modernised cybercrime law, possibly under the forthcoming Digital India Act, that clearly defines emerging crimes, includes graded penalties, and integrates global procedural standards such as expedited data access and digital forensics admissibility.[3]

2. **Treaty Participation**: India should reconsider its stance and accede to the Budapest Convention, while also supporting the implementation of the UN Cybercrime Convention (2024). Both instruments are crucial for enabling secure and lawful international cooperation in an era of transnational cybercrime.[4]

3. **Enforcement Reforms**: There is an urgent need to decentralise and empower state-level cyber cells with funding, training, and forensic resources. Special cybercrime courts should be created to handle complex digital evidence and fast-track resolution.

4. **Institutional Accountability and Public Engagement**: National campaigns for digital safety akin to the UK's Cyber Aware and the US's Stop.Think.Connect. should be launched in India to build digital hygiene and citizen trust. Law enforcement agencies must also be held accountable through internal audits, transparency mandates, and victim-centric mechanisms.

5. **Capacity Building and Jurisprudential Development**: Continuous training of investigators, prosecutors, and judges on evolving cyber threats and digital laws is essential. In parallel, Indian courts must develop a consistent body of cyber jurisprudence through reasoned decisions, modelled after leading US and UK precedents.

In conclusion, India cannot afford to remain a passive observer in the fast-evolving domain of international cyber law. As one of the largest digital ecosystems in the world, its cybercrime legal framework must be not only reactive but strategic, harmonised, and globally interoperable. Learning from the legislative and institutional models of the UK and USA, and

committing to international cooperation instruments, will enable India to both defend its cyberspace and lead regional legal harmonisation efforts across the Global South.

References

1. M Dasgupta, *Cyber Crime in India: A Comparative Study* (1st edn, Eastern Law House 2016)

2. Pavan Duggal, *Cyber law* (3rd edn, Universal LexisNexis 2023)

3. Anirudh Rastogi, *Cyber Law: Law of Information Technology and Internet* (1st edn, LexisNexis 2024)

4. Jyoti Rattan, *Cyber Laws and Information Technology and Artificial Intelligence* (10th edn, Bharat Law House 2024)

5. Karnika Seth, *Computers, Internet and New Technology Laws* (3rd edn, LexisNexis 2022)

6. Vakul Sharma and Seema Sharma, *Information Technology Law and Practice* (9th edn, Universal LexisNexis 2025)

7. Yatindra Singh, *Cyber Laws* (6th edn, LexisNexis 2023)

8. About the Convention - Cybercrime <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

9. Ad Hoc Committee - Home (*United Nations : Office on Drugs and Crime*) <//www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home>

10. APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice (*APEC*) <https://www.apec.org/publications/2012/03/apec-guidelines-for-creating-voluntary-cyber-security-isp-codes-of-practice>

11. Cyber Frauds Jump 900% in 4 Years: Small Cities like Deoghar, Nuh, Mathura Emerge as New Scam Capitals | India News - The Indian Express <https://indianexpress.com/article/india/cybercrime-sharp-rise-complaints-2024-govt-data-9816845/>

12. Cybercrime <https://www.interpol.int/Crimes/Cybercrime>

13. First Additional Protocol - Cybercrime - Www.Coe.Int (*Cybercrime*) <https://www.coe.int/en/web/cybercrime/first-additional-protocol>

14. Mutual Legal Assistance in Criminal Matters (*Ministry of External Affairs, Government of India*) <https://mea.gov.in/mutual-legal-assistance-in-criminal-matters.htm>

15. Nations U, 'United Nations Charter (Full Text)' (*United Nations*) <https://www.un.org/en/about-us/un-charter/full-text>

16. OECD Policy Framework on Digital Security (*OECD*, 14 December 2022) <https://www.oecd.org/en/publications/oecd-policy-framework-on-digital-security_a69df866-en.html>

17. OECD, *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity* (OECD Publishing 2022) <https://www.oecd.org/en/publications/oecd-policy-framework-on-digital-security_a69df866-en.html>

18. Only 1.6% Conviction Rate in 2 Yrs amid Surge in Cybercrime Cases (*The Tribune*) <https://www.tribuneindia.com/news/india/only-1-6-conviction-rate-in-2-yrs-amid-surge-in-cybercrime-cases-2/>

19. Police Bust Sextortion Racket Using Fake SIM Cards and Synthetic Accounts in Delhi *The Times of India* (18 June 2025) <https://timesofindia.indiatimes.com/city/delhi/police-bust-sextortion-racket-using-fake-sim-cards-and-synthetic-accounts-in-delhi/articleshow/121934480.cms>

20. United Nations Treaty on Cybercrime Agreed by the Ad Hoc Committee - Cybercrime - Www.Coe.Int (*Cybercrime*) <https://www.coe.int/en/web/cybercrime/-/united-nations-treaty-on-cybercrime-agreed-by-the-ad-hoc-committee>