INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBER FRAUD LAWS IN INDIA AND THE UNITED STATES: A COMPARATIVE STUDY

AUTHOR - MR. KANAV BHARDWAJ, LLM STUDENT AT GALGOTIAS UNIVERSITY

BEST CITATION – MR. KANAV BHARDWAJ, CYBER FRAUD LAWS IN INDIA AND THE UNITED STATES: A COMPARATIVE STUDY, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (9) OF 2026, PG. 261-268, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - HTTPS://DOI.ORG/10.65393/IJLRV6I931

ABSTRACT

The compounding growth of online transactions and reliance on network technologies has greatly raised cyber fraud in jurisdictions. India and the United States are two of the largest digital economies globally that have common yet distinct challenges in controlling cybercrimes. In this paper, a comparative study was made on the statutory systems, enforcement strategies, institutional frameworks, and adjudicatory systems of cyber fraud in both countries. Although India mostly employs the Information Technology Act, 2000 and the Indian Penal Code (recovery to the Bharatiya Nyaya Sanhita, 2023), in the United States the combination of the federal statutes (like Computer Fraud and Abuse Act, Wire Fraud Statute, state-based laws) are employed. The convergences noted in the study include criminalisation of unauthorised access, identity theft and financial fraud, whereas divergences occur following different constitutional cultures, enforcement ability and regulatory ideologies. The paper ends with a policy recommendation that will synchronize legal remedies, augment cross-border collaboration or coordination, and perpetuate victim-focused remedies.

INTRODUCTION

Cyber fraud has actually become one of the most common type of crimes that have been developed very fast and likely to keep advancing in the digital age. As the internet gains more and more connectivity globally, e-commerce, cloud computing, and digital banking a person and an institution, now more than ever before, is subjected to a level of online threats never before seen. The cyber fraud realm includes a wide range of fraudsters, such as phishing, vishing, identity theft, ransomware, business email compromise (BEC), one-time password (OTP) fraud, online investment frauds, and cryptocurrency fraud. Cyber fraud, unlike the old models of crime, occurs in an environment that is borderless, anonymous, and complex in terms of technology and as such, this has hampered the ability of domestic law systems to react effectively.

Cyber fraud has been transnational, and has therefore forced countries to reconsider the traditional models of criminal responsibility, jurisdictional capabilities, evidence gathering, and cooperation in law-enforcement. A comparative situation between India and the United States is educative based on their different legal background, economic systems, technological systems, and ability to enforce their laws. India largely depends on the centralized system of laws in the form of the Information Technology Act, 2000, which is supported by the clauses of the Indian Penal Code/ Bharatiya Nyaya Sanhita and directives of regulating bodies, including the reserve bank of India (RBI). The federal-state regulatory model that is used in the United States, on the other hand, is a hybrid one with major federal laws, including the Computer Fraud and Abuse Act (CFAA), the Wire Fraud Statute, identity-theft

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 9 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

regulations, and various cybercrime models on state level.

Although all of this is structured differently, the two countries are susceptible to a comparable form of cyber fraud because of the increase in digital use, data movement across borders, and financial de-banking. This relative analysis is vital in comprehending how various jurisdictions identify cyber fraud, the statutory resources they might employ to prosecute, the enforcement to those, as well as the challenges that are still encountered to deal with technologically advanced criminal activities. It also illuminates on points of convergence that can take place particularly in working as a cross border coalition, capacity development and legal standardization harmonization.

In this connection, this assignment is a critical analysis of cyber fraud law in India and the United States. It examines legal text, institutional reactions, procedure, enforcement issues, law court practices, and the policy debate. It is not just a comparison of the two systems but rather drawing valuable conclusions that can help both jurisdictions in greater regulation of cyber fraud as well as adding to world-wide cyber regulation.

I. GROUND AND CLASSIFICATION OF COMPUTER FRAUD.

Cyber fraud is a broad concept, which may be defined as an attempt at misleading either an individual or an institution using digital systems, networks, or communication technologies to unlawfully acquire money, data, or other valuable resources.[271] It is a highly dynamic type of crime, which can fit the current technological setting and take advantage of the weaknesses in human behaviour and digital infrastructure. A closely related crime is phishing and vishing, whereby perpetrators of fraudulent activities impersonate legitimate businesses or corporations to gain access to sensitive user credentials.[272]Other more closely related is identity theft, whereby user information, such as Aadhaar, Social Security, or online banking, has been stolen and used to steal money, turn into fraudsters, or has been offered as a token in a Ponzi scheme operating using entirely online platforms. Among the most widespread, however, is Business Email Compromise (BEC), where cybercriminals impersonate business executives or vendors to fraudul

II. LAWS IN THE COUNTRY CYBER FRAUD.

The legal basis of the Indian legal approach to combating cyber fraud is heavily based on the Information Technology Act, 2000, which is at the core of the legal and criminal actions against cybercrimes and contains provisions such as the 43C and 43D that deal with identity theft when committed with a malicious motive which involves misuse of digital signatures or passwords and offence of cheating by personation through the use of computer resource, respectively.[273] The grounds of the Indian legal system with regard to cyber crimes are anchored on the Bharatiy Ny Such provisions would guarantee that even non-technical-based financial frauds associated with lying or misappropriation of assets entrusted to them can be prosecuted. Additional reinforcement of the system of regulation is the effective hierarchy provided by the Reserve Bank of India (RBI) that issues the guidelines on disclosing fraud in digital payments and establishing the rules of consumer protection, including the Zero Liability Policy in instances of unauthorized electronic payment .Strict Know Your Customer (KYC) requirements further aim to reduce identity-based financial fraud by ensuring that digital transactions are linked to verified identities.[274] From an institutional standpoint, the Indian Computer Emergency Response Team (CERT-In) plays a central role in monitoring cybersecurity incidents, issuing advisories, and enforcing mandatory reporting of cyber incidents within six hours—a significant regulatory development

[271] Ministry of Electronics & Information Technology, Cybercrime Overview, GOV'T OF INDIA.
[272] Indian Computer Emergency Response Team (CERT-In), Phishing Advisory.
[273] Information Technology Act, 2000 (India).
[274] RBI Master Direction – Know Your Customer (KYC), 2016 (updated).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

introduced in 2022.Complementing these mechanisms are the Adjudicating Officers designated under the IT Act, who possess civil jurisdiction over cyber-related financial disputes up to ₹5 crore, with appeals directed to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).[275] Together, these legal and institutional components form a multilayered framework

III. LEGAL FRAMEWORK GOVERNING CYBER FRAUD IN THE UNITED STATES

On the approach to combating cyber fraud, the United States assumes a multifaceted and multilayered regulatory approach by relying on state legislation, federal laws, and specialized law enforcement authorities. On the federal level, Computer Fraud and Abuse Act (CFAA),1986, is the key legislation criminalizing unauthorized access to secured computers, data theft, digital fraud and purposely causing harm to computer systems but unfortunately its relevance has been limited by judicial interpretation, particularly in the instances of definition of exceeding authorized access. Another law that is utilized most often related to phishing, Business Email Compromise (BEC), and Internet-based investment fraud is the supplementation of the CFAA by the Wire Fraud Statute (18 U.S.C. SS 1343), which punishes schemes to defraud carried out via electronic communications, and it is not an exception.[276]The successful protection against potentially technologically enhanced frauds also encompasses the Electronic Communications Privacy Act (ECPA).

The United States has a blend of federal and state enforcement programs beyond federal law, with individual states having their own cybercrime laws concerning identity theft, online fraud and unauthorized computer access, often in conjunction with federal prosecutes, which have been combined under a dual federal-state enforcement model to effectively reduce fraud-related vulnerabilities to critical infrastructure systems.[277]Lastly, this mixture of distributed and institutionally spread frameworks makes the United States one of the largest cyber enforcement regimes in the world.

IV. CROSSBORDER COMPARATIVE ANALYSIS OF CYBER FRAUD LAWS.

Comparative analysis of the laws of cyber fraud in India and the United States will show considerable differences in the approach to legislature design, enforcement frameworks, and regulatory priorities, as well as reveal those aspects of convergence brought about by the globalisation of cyber crime. This structural difference mirrors wider legal custom habitual: where India adopts a centralized statutory framework based mainly on the Information Technology Act, 2000, where the United States adopts fragmentation and highly localism, with its cyber fraud law provisions spread out over a variety of federal statutes, most famously the Computer Fraud and Abuse Act (CFAA) and the Wire Fraud Statute, supplemented by state-level variations that ensure that U.S. identity theft, computer-related deception, and computer misuse have a written legal formulation. Substantively, the two jurisdictions criminalize illegal access, data theft and illegal online impersonation, but the norms and interpretation of the crimes vary. It has been seen that the IT Act provisions of 43 and 66, India, are generally being used to punish unauthorized access and ill-intentioned use of computer resources, whereas in the U.S. courts have limited the application of exceeding authorized access under the CFAA, most notoriously in Van Buren v. United States, and which confined the liability to violation of technological, rather than contractual, constraint.[278] This proves a comparatively more subdued judicial logic in the United States than the broad statutory phrasing in India.

In identity theft and impersonation, the United States has a more sophisticated structure of fraud schemes than India, aided by its more

[275] Information Technology Act, 2000, § 46; Telecom Disputes Settlement and Appellate Tribunal (TDSAT) Jurisdiction Notifications.

[276] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523.

[277] Cybersecurity & Infrastructure Security Agency (CISA), Cybercrime and Fraud Prevention Guidelines.

[278] Van Buren v. United States, 141 S. Ct. 1648 (2021).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

detailed statutory framework in the form of Identity Theft and Assumption Deterrence Act but has a more traditional varied structures based on levels of technical capabilities to enforce alongside more effectively coordinated across their boundaries and higher rates of investigation by federal agencies and responsiveness (Secretary 2014), and, when a case is undertaken, has the power to investigate consumer frauds more effectively with the added burden of higher rates of offending being met by aggravated identity theft from

Another point of difference is international cooperation. Responding to the issue of sovereignty, the United States is an active signatory to the Budapest Convention on Cybercrime, permitting expedited cross-border exchange of data and investigative support, but India, as a nation, is not, depending on slower Mutual Legal Assistance Treaty (MLAT) systems.[279]This has an impact on the rates at which foreign evidence can be requested in cross-border cybercrimes, which is a more common phenomenon in digital crime. Nevertheless, regardless of these differences, the two nations have similar issues as they struggle with the fast development of technology, the growing use of encryption, the emergence of cryptocurrency-related fraud, and the greater role of transnational criminal organizations. Consequently, both political regimes are in constant stress to revise statutory definitions, improve their investigative abilities, and improve on collaboration between the state and the business sector. All in all, the U.S. system is more institutionally developed and tightly technological, whereas India has a centralized system which is of clarity and coherence, but needs much capacity building before it can attain similar levels of enforcement effectiveness.

V. ENFORCEMENT CHALLENGES IN BOTH COUNTRIES

At this, both the United States and India struggle with the issue of cyber fraud incapability even with well-developed statutory frameworks, and much of it is due to the transnational and technologically intensive essence of online crimes. Jurisdictional ambiguity is one of the major challenges. Cyber fraud regularly involves perphenazine, victims, servers, and financial liaisons across several states or countries, making the investigation and prosecution complicated in both nations.[280]The second challenge is the technical knower and forensic ability, which is experienced in India, as jurisdiction is duplicated between state police cyber cells and the national authorities like the CBI, and this delays the investigation or inconsistency in the results of various investigations. Granted that the United States has a sophisticated digital forensics infrastructure, such as the FBI and Secret Service, nevertheless even the United States has capacity bottlenecks in controlling the level of malware, encryption, and anonymization advances, as well as challenges in preserving the evidence chain on electronics, which calls into question low conviction rates in passing cyber fraud cases through the courts.

Under-reporting by the victims is another significant barrier, as it occurs because of the fear of stigma, the lack of enlightenment, or the distrust in the results of the investigation. Although some, such as the Internet Crime Complaint Center (IC3) created by the FBI, offer the simplicity of reporting in the United States, the National Cyber Crime Reporting Portal available in India is unevenly used because of the lack of digital literacy and unequal follow-up implementation at the state level.[281] The emergence of cross-border data storage only complicates the process of enforcement. The US, by being involved in the Budapest Convention and due to the legal structures like CLOUD Act,

[279] Council of Europe, Budapest Convention on Cybercrime.

[280] Council of Europe, Budapest Convention on Cybercrime (Jurisdictional Guidelines).

[281] Federal Bureau of Investigation, IC3 Annual Report; National Cyber Crime Reporting Portal, GOV'T OF INDIA.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

can more effectively access evidence that is held abroad, whereas India still relies on the slow mechanisms of the Mutual Legal Assistance Treaty (MLAT), which leads to us delays in gaining access to vital digital evidence.[282]

Furthermore, technological evolution is typically outpaced by legislative change in both countries: in the United States, the system of multi-competent response has been well-funded to legally enforce and legally aligned to respond, whereas in India, mandatory reporting remains an unfinished mandate split across multiple agencies, with limited resources, and requiring bureaucratic coordination to compel its counterparts to comply with the process.[283]

VI. JUDICIAL TRENDS

The similarities in judicial tendencies in India and the United States suggest the increasing awareness of the intricacy of cyber fraud and the necessity of adjusting the historical legal principles to the technology mediated crime. Courts in India have increasingly now found the Information Technology Act, 2000, to be construed in a fashion that reflects the current trends of Internet fraud, with stress put on unauthorized access and identity abuse and deceptive ways of doing business over the Internet. Such cases as Shafhi Mohammad v. State of Himachal Pradesh, the Supreme Court emphasized that due care should be made to accommodate new approaches of generating electronic evidence representing judicial goodwill to overcome procedural obstacle in the prosecution of cyber crimes, such that inconsistent application of e-custodial regulations among states, lack of evidentiary basis, and delays in obtaining forensic certification each undermines the overall deterrence impact of cyber fraud cases.[284]

The interpretation of cyber fraud laws by the United States courts has been marked by a more subtle interaction with constitutional values, in particular those of due process, overcriminalization and the boundaries of federal power. The landmark ruling by the Supreme Court on Van Buren v. United States The Computer Fraud and Abuse Act (CFAA) was narrowed considerably, with the court holding that the term exceeding authorized access should not be applied in instances that do not involve a user of information wrongly obtained via the computer interface but instead in cases in which the user of the information is already technically barred from accessing information but is just misusing their already available access. The lower federal courts have also examined government interpretations of the wire fraud and identity theft laws, with a consistent emphasis on balancing between strong enforcement and protection against over- broad discretion in prosecution.[285] The U.S. judiciary has also developed doctrines regarding the admissibility and integrity of flattened evidence, often with an insistence on the strict adherence to the forensic standards in order to prevent over-reach through over-liberal prosecution.

One of the greatest areas of separation between the two jurisdictions as far as the courts are concerned is the fact that the U.S courts tend to stick to more technologically informed and doctrine written approaches whilst the Indian courts address more often entitled to cyber fraud in terms of statutory purpose and public policy. However, both systems have an identical course: legal acceptance that cyber fraud requires liberalistic treatment of the law, the transformation of the evidentiary methods, and ongoing involvement with new variants of digital crimes. Under this, therefore, judicial involvement in both states is continuously defining the boundaries of the cyber fraud jurisprudence, despite the legislative and enforcement dilemma.

[282] U.S. CLOUD Act, 18 U.S.C. § 2713; Ministry of External Affairs (India), MLAT Procedures.

[283] Standing Committee on Home Affairs (India), Review of Cybercrime Infrastructure and Preparedness.

[284] National Crime Records Bureau (India), Crime in India: Cybercrime Statistics.

[285] Cybersecurity & Infrastructure Security Agency (CISA), Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Guidelines.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

VII. POLICY RECOMMENDATIONS

Since the prevention, investigation, and controls context are constrained by various weaknesses outlined in the enforcement systems of both India and the United States and the cyber fraud is becoming more sophisticated, it requires a combination of specific policy changes, which would enable the countries to improve their preventive measures against cyber fraud as well as investigate and fix the damages caused by the cyber crimes. In the case of India, one of the key suggestions is to modernize the Information Technology Act, 2000, to fill the gaps concerning artificial intelligence-driven fraud, deepfake impersonation, and cryptocurrency scams, as well as, the manipulation of data across platforms, which were not envisioned when the law was introduced in 2000.Improving national digital forensic capacity is also important; with the support of constant training of law-enforcement personnel, a system of regional cyber forensic laboratories with uniform standards should be established, which would significantly enhance the reliability of the evidences and enable quicker investigations in cross-border cases, despite the lack of agreement on the participation in the Budapest Convention, which would simplify access to the evidence abroad and improve the use of the slow process of signing the Mutual Legal Assistance Treaty (MLAT).5 On the consumer-protection aspect, the Zero Liability Policy of Even the more advanced enforcement ecosystem of the United States needs some sharpening of aspects of its legal and regulation structure. A key suggestion includes revising laws that are unclear in the Computer Fraud and Abuse Act (CFAA), particularly following judicial reduction questions in Van Buren, to eliminate that cybersecurity research, audit in policy, and good-faith digital behavior may accidentally become a criminal act. Unifying differing state-based cybercrime jurisprudence with a federal minimum might also be a way of reducing differences in the prosecution level and facilitating interagency cooperation between federal and state law enforcement agencies. Mandatory reporting of data breaches, ransomware attacks and digital financial fraud, especially those involving private firms providing key infrastructure would also be enhanced in the United States as this would improve the collection of threat intelligence and respond more swiftly to systemic consequences. Lastly, the two jurisdictions should focus on the idea of the collaboration between states and corporations as most digital infrastructures belong to the latter; joint cyber-drives, synchronized threat notifications, and mutual cyber-drills have the potential to be highly resilient to transnational fraud-related activities.

The common feature of these policy recommendations is based on the requirement of an adaptable legislation on the technological aspect, higher forensic and investigative capacity, increased international cooperation, and a regulatory philosophy focused on victims. As the cross-border evolution of cyber fraud cases continues, India and the United States need to continue allowing reforms between innovation and security where legal frameworks can be responsive, enforceable and adaptive to the new threats they face.

VIII. CONCLUSION

The comparative analysis of cyber fraud legislation on the Indian and the United State reveals that both nations have come quite a long way in establishing legal and institutional structures to deal with more and more sophisticated versions of digital crime. The centralized statutory regime of India with the centre being the Information Technology Act, 2000 does give a unified set of laws but has significant issues with both enforcement capacity as well as digital forensics as well as with synchronization between agencies. The US, however, has a more decentralized but more specialized enforcement apparatus with the help of several federal laws and technologically sophisticated investigation departments. This model is efficient and it is a model of specialization but it leads to differences between states and individuality in the regulation process. Nevertheless, such differences do not cause the

nations to avoid similar challenges, such as quick technological advances, cross-border crime, and the increase of new threats involving crypto-related fraud, AI-driven impersonation, and deepfakes-based ones.

The comparison of the analysis helps bring out areas that the various jurisdictions can enhance. India needs to advance investigative proficiency, collaborative inter-agency abilities, improve forensics hardware, and develop overseas collaboration to improve the implementation of trans-regional cyber felony. In the meantime, the United States could also use a more federalized system of data security laws at the state level and a more precise wording of the existing statutes to make cybercrime areas less ambiguous and they are more uniformly applied. After all, cyber fraud is a truly international menace to both the legislation and the law itself, which requires collaboration, flexibility, and active change of the policies and law enforcement in order to stay up to date with emerging technologies. India and the United States should therefore embrace pliant, technologically receptive and globally synchronized legal measure to be defiant of the transforming circumstances in cyber frauds.

IX. REFERENCES

Ministry of Electronics and Information Technology (India) — https://www.meity.gov.in

Information Technology Act, 2000 (India) — https://www.indiacode.nic.in

Indian Computer Emergency Response Team (CERT-In) — https://www.cert-in.org.in

Reserve Bank of India — https://www.rbi.org.in

National Cyber Crime Reporting Portal (India) — https://cybercrime.gov.in

Federal Bureau of Investigation (IC3 Reports) — https://www.ic3.gov

U.S. Department of Justice — https://www.justice.gov

Cybersecurity and Infrastructure Security Agency (CISA) — https://www.cisa.gov

Federal Trade Commission (FTC) — https://www.ftc.gov

United States Secret Service — https://www.secretservice.gov

Council of Europe: Budapest Convention on Cybercrime — https://www.coe.int/cybercrime

U.S. Securities and Exchange Commission (Crypto Fraud Alerts) — https://www.sec.gov

Ministry of Electronics and IT, Government of India – IT Act, 2000

CERT-In Guidelines and Cyber Incident Reporting Framework

Reserve Bank of India – Consumer Protection & Digital Payment Guidelines

U.S. Department of Justice – Computer Fraud and Abuse Act

Federal Trade Commission – Identity Theft and Consumer Fraud Reports

FBI – Internet Crime Complaint Center (IC3) Reports

U.S. Code: 18 U.S.C. § 1343 (Wire Fraud Statute)

CISA – Cybersecurity Regulations and Advisories

BIBLIOGRAPHY

Books and Articles

Brian Craig, Cyberlaw: The Law of the Internet and Information Technology.

Jonathan Clough, Principles of Cybercrime.

Gerald R. Ferrera et al., CyberLaw: Text and Cases.

Pavan Duggal, Cyberlaw in India.

Vivek Sood, Cyber Crimes, Electronic Evidence & Investigation.

Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes.

Statutes and Government Regulations – India

Information Technology Act, 2000.

Bharatiya Nyaya Sanhita, 2023.

Reserve Bank of India, Customer Protection in Unauthorized Electronic Banking Transactions.

RBI Master Directions on Know Your Customer (KYC), 2016 (updated).

Ministry of Home Affairs, National Cyber Crime Reporting Portal Guidelines.

CERT-In, Directions on Cybersecurity Incident Reporting, 2022.

Reports and Institutional Documents

Federal Bureau of Investigation (FBI), Internet Crime Complaint Center (IC3) Annual Reports.

Cybersecurity & Infrastructure Security Agency (CISA), Cyber Threat Intelligence Reports.

National Crime Records Bureau (India), Crime in India: Cybercrime Statistics.

Ministry of Electronics & Information Technology (India), National Cyber Security Policy.

Standing Committee on Home Affairs (India), Report on Cybercrime Preparedness.

Federal Trade Commission (USA), Identity Theft & Consumer Fraud Reports.

Web Resources

https://www.meity.gov.in

https://www.cert-in.org.in

https://cybercrime.gov.in