INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

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

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

Copyright © International Journal for Legal Research & Analysis

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

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

Dr. Namita Jain

Head & Associate Professor

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

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

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

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

Avinash Kumar

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

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

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

ISSN: 2582-6433

UNRAVELLING CYBERSPACE: LEGAL CHALLENGES AND THE BATTLE AGAINST CYBER ECONOMIC OFFENCES IN INDIA

AUTHORED BY - DEEPTHI SOMAN
Assistant Professor of Law
Government Law College, Thiruvananthapuram

Abstract

Unravelling Cyberspace: Legal Challenges and the Battle Against Cyber Economic Offences in India

As India rapidly embraces digital transformation, cyberspace has become central to communication, commerce and governance. However, the expansion of digital infrastructure and financial technologies has also given rise to a growing number of cyber economic offences, including online fraud, identity theft, phishing, ransomware attacks and unauthorised access to sensitive financial data. These offences exploit the borderless and anonymous nature of the internet, creating unique challenges for law enforcement, regulators and the judiciary. Traditional legal frameworks are often ill-equipped to address the jurisdictional ambiguities, evidentiary complexities and technological sophistication associated with such crimes.

This article critically explores the emerging jurisprudence of cyberspace in India with a specific focus on cyber economic offences. It traces the evolution of cyberlaws, examines judicial approaches to determine jurisdiction on the virtual realm and identifies the pressing legal and procedural barriers that hinder effective enforcement. By analysing both domestic legislation and international instruments, the article highlights the need for harmonised legal standards, improved investigative capabilities and robust cross-border cooperation.

The article also discusses the institutional and infrastructural shortcomings, such as the lack of specialised cybercrime courts and limited technical expertise within law enforcement agencies. It argues that legal reform must be accompanied by capacity building, public awareness and strategic international partnerships. In conclusion, the article calls for a proactive and integrated legal framework to confront the rising threat of cyber economic offences and to secure India's digital future through an adaptive, well-resourced and technologically aware cyber

ISSN: 2582-6433

jurisprudence.

Key Words

Cyberspace, Cyber economic offences, Cybercrime in India, Cyber Jurisprudence, Digital Governance, Financial Data Security, Jurisdiction in Cyberspace, Cross-border cybercrime, Cyber law enforcement, Judicial approach, Data protection, legal reforms.

Introduction

In the digital age, cyberspace plays a vital role in daily life, influencing how people interact, carry out business activities, utilise services and handle financial operations. India with its rapidly growing digital infrastructure and over a billion internet users, is at the forefront of this transformation. However, this digital revolution has also brought with it a troubling rise of cyber economic offences.

These crimes, which include online financial fraud, phishing scams, Identity theft, ransomware attacks, and unauthorised access to financial data, pose significant threats to individuals, businesses and national security.

Unlike conventional crimes, cyber economic offences exploit internet's anonymous, constantly evolving and transnational nature. These offences often extend across countries and outpace the legal and regulatory frameworks designed to combat them. This creates complex legal and enforcement challenges related to jurisdiction, evidence collection, data privacy and international cooperation.

This article aims to examine the evolving contours of cyber jurisprudence in India with special focus on economic offences in the digital realm. It analyses the key legal, procedural and infrastructural challenges faced by law enforcement and the judiciary and explores how India's legal system can adapt to safeguard its digital ecosystem. As we unravel the complexities of cyberspace, it becomes imperative to not only reform legal provisions but also enhance institutional capacity, foster international cooperation, and build public trust in digital governance.

ISSN: 2582-6433

Evolution of cyberspace jurisprudence

The word 'cyber' traces back to Norbert Wiener's concept of 'cybernetics' in 1948, which he described as "control and communication in the animal and the machine."[1] Later he added society as the third object to this concept. Building on this concept, the belief that humans can interact with machines to create an entirely new kind of environment laid the groundwork for how we understand cyberspace today.

The concept of "cyberspace" was introduced by science fiction writer William Gibson in his short story 'Burning Chrome', where he envisioned a network of connected digital systems. He later brought the idea to wider attention the 1984 seminal novel 'Neuromancer', portraying it "a consensual hallucination experienced daily by billions of legitimate operators… a graphic representation of data abstracted from the banks of every computer in the human system"[2]

Although this description highlights how cyberspace is perceived as a unique environment by users, it continues to hold relevance today, especially in demonstrating the possibilities of developing immersive digital experiences. Notably it also highlights complexity as a defining feature of cyberspace, a characteristic that continues to shape how we interact with digital systems. Overtime, numerous definitions of cyberspace have emerged, reflecting its evolving nature and the diverse ways in which it is conceptualised across disciplines.

The UK Cyber Security Strategy defines cyberspace as a dynamic digital domain used to store, alter and exchange information. This digital realm extends beyond the internet to include a wide range of information systems that enable essential sectors, operational networks and public utilities.[3]

In the United States, cyberspace is acknowledged as a vital component of the broader digital ecosystem. The U.S.Department of Defense describes it as a "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks,

[1] D.A.Novikov, Cybernetics: *From Past to Future*(Springer,2016), available at https://www.researchgate.net/publication/287319297_Cybernetics_from_Past_to_Future (last visited July 10,2025)
[2] Carmen Moldovan, On the Normative Equivalence Paradigm in Cyberspace,177 *SHS Web of Conf.*02002 (2023), https://doi.org/10.1051/shsconf/202317702002
[3] U.K. Cabinet Ofifce, *Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (Nov.2011), https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf

ISSN: 2582-6433

computer systems, and embedded processors and controllers."[4]

According to Canada's Cyber Security Strategy (2010), cyberspace is described as "an electronic domain formed by interconnected information technology networks and the data they carry. It is portrayed as a global common, a shared virtual environment where billions of users engage in sharing ideas, accessing services and forming social networks" [5]

The European Commission, in its conceptual framework for safeguarding EU cyberspace, defines cyberspace as " the virtual global and common domain within the information environment consisting of all interconnected and interdependent networks of global, organisational and national information infrastructure, based on the Internet and telecommunications networks, to be extended by other networks of global, organisational and national information infrastructure, based on the Internet and telecommunications networks to be extended by other networks, computer systems and embedded processors, and also containing stand-alone systems and networks."[6]

Cyber space does not have one clear or universally accepted definition. While it is often described as the place where the computer networks and online communication take place, such descriptions do not fully capture its complex and constantly changing nature. A more inclusive way to define cyberspace is to see it as a network of connected information systems, including hardware, software, data and the media that link them, combined with the people who use and interact with these systems. This approach recognises thar cyberspace is not just made up of machines, but also depends heavily on human users. It is always changing, as the computers and users join and leave the network, connections shift and the data being shared and stored is constantly updated. This ongoing movement makes cyberspace very complex. As a result, it cannot be fully understood using physical space alone. Instead, it can be thought of as a kind of map or digital space, where the connections between the users and systems are more important than physical distance. Cyberspace would not exist without human involvement. It is a manmade space, created and maintained for human use whether for

[4] U.S.Dep't of Def., *Joint Pub. 1-02: Dep't of Defence Dictionary of Military and Associated Terms,* https://irp.fas.org/doddir/dod/jp_1_02.pdf (last visited July 10,2025)
[5] Gov't of *Can.*, Cyber Security Strategy: For a stronger and More Prosperous Canada*(2010),* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf (last visited July 11,2025)
[6] Grzegorz Pilarski, Tackling Cyberspace Threats-The International Approach, Sec.& Def. Q., War Studies U., https://securityanddefence.pl/pdf-103238-36118?filename=36118.pdf (last Visited July. 10,2025)

ISSN: 2582-6433

communication, business entertainment or governance. If individuals ceased to use or support its infrastructure, cyberspace would slowly deteriorate. Therefore, it is important to consider not just the technological aspects of cyberspace but also the people who create and engage with it. Understanding this balance between humans and machines is essential for building effective laws and policies to manage cyber space responsibly.

According to Black's Law Dictionary, "Jurisprudence is the philosophy of law or the science which treats the principles of positive law and legal relations."[7] In today's digital age, the growth of electronic communication and the broad expansion of internet use have created a necessity for a new kind of legal framework commonly called Cyber Jurisprudence.This area of law looks at the rules and challenges that come with living and interacting in cyber space, a world that exists beyond physical borders. This emerging field provides a legal framework for a domain that transcends physical borders and traditional territorial boundaries. Unlike the tangible world, the cyberspace operates through virtual structures, where elements such as contracts, property, disputes and even judicial mechanisms exist in digital forms.

Cyber jurisprudence focuses on the legal aspects of activities carried out in cyberspace, particularly issues like cyber jurisdiction and the conceptual development of virtual courts. It aims to build a consistent set of legal standards that can be applied across nations to manage conduct in this borderless environment.

Some of the recent court decisions indicate a growing trend of applying existing laws from the physical world to cases in the virtual domain. This approach has led to the idea of developing principle often referred to as the "Primacy of Meta Space", which suggests that unless specific cyberlaws are established, real world legal systems will continue to dominate the regulation of cyber space. [8]

A landmark case, Bragg Vs Linden lab, highlights this reality. The court in this case observed that "although the facts of the case are virtual, the dispute is real."[9] This reflects the need for a

[7] Black's Law Dictionary 854 (6th ed. 1990) , https://ia600308.us.archive.org/34/items/table-of-authorities/references/BLD_6th.pdf (accessed May 16, 2025)
[8] P. Vasantha Kumar, Cyber Jurisprudence: Jurisprudence of the 21st Century, 3(1) Int'l J.Advances in Eng'g & Mgmt, 790 (2021) , https://www.ijaem.net/issue_dcp/Cyber%20Jurisprudence%20the%2921st%20Century.pdf (last visited Apr. 15, 2025)
[9] Bragg Vs Linden Research, Inc.,487 F.Supp.2d 593(E.D.Pa.2007), https://www.lexology.com/library/detail.aspx?g==e2167f3f-ecff-4df3-9a74-248880064025 (last visited on June

ISSN: 2582-6433

clearer legal foundation in dealing with disputes arising from the digital world.

Cyber jurisprudence may be understood as the body of legal principles specifically developed to govern matters arising within cyberspace and the internet.

Cyber jurisprudence and the tests for jurisdiction in cyberspace

In the realm of cyber jurisprudence, determining jurisdiction in cross-border cybercrime matters poses significant challenges. To address these, courts have developed several legal tests to ascertain whether they can exercise personal jurisdiction over defendants operating in cyberspace

1. Minimum Contacts Theory

The concept was laid down by the U.S. Supreme Court in International Shoe Co. Vs Washington.[10] Under this test, a court can exercise jurisdiction if the defendant has purposefully established significant ties with the concerned jurisdiction, such as engaging in business activities or entering into contractual relationships. The test is later extended to cyber contracts in CompuServe Inc. Vs Patterson[11], recognising that digital interactions can establish sufficient 'minimum contacts".

2. Sliding Scale Theory (Zippo Test)

This test is most widely used in internet related cases and the most accepted test in deciding personal jurisdiction in cyber space. The Zippo case, formally known as Zippo Manufacturing Co. Vs Zippo Dot Com, Inc.,[12] introduced framework for determining jurisdiction based on website's interactivity. This approach analyses how actively a website engages with users in a particular forum to decide whether exercising jurisdiction is appropriate. Passive websites that merely provide information do not attract jurisdiction, while highly interactive sites that conduct business and engage users across borders are likely to be subject to judicial authority in those jurisdictions. This approach highlights how online activities such as subscriptions and targeted services can subject foreign entities to the jurisdiction of domestic courts.

15, 2025

[10] International Shoe Co. v. Washington, 326 U.S. 310 (1945)

[11] CompuServe Inc. v. Patterson,89 F.3d 1257(6th Cir.1996)

[12] Zippo Mfg.Co. v. Zippo Dot Com, Inc., 952 F. Supp.1119 (W.D. Pa.1997)

ISSN: 2582-6433

3. Effects Test

This test is derived from the landmark case Calder Vs Jones.[13] The U.S. Supreme Court established the "effects test" to determine personal jurisdiction in cases involving defamation and related intentional torts, where the defendant's actions were specifically aimed at the forum state. This case serves as a cornerstone in cyber jurisprudence, as it laid a foundation for determining personal jurisdiction in cyberspace, where harmful digital content may be created in one location but causes injury elsewhere. It highlights how intentional online actions with foreseeable consequences in another jurisdiction can establish a sufficient nexus for courts to assert jurisdiction even across borders.

All these tests reflect the ongoing evolution of cyber jurisprudence, which seeks to adapt traditional legal concepts to the unique realities of cyberspace. As digital interactions increasingly transcend national borders, these jurisdictional framework helps courts to balance technological innovations with the enforcement of justice in the virtual realm.

Cyber jurisprudence and the rising threat of Cyber Economic offences

As cyberspace becomes an integral part of our daily lives, the need for a legal framework to understand and regulate behaviour in the digital world is increasingly important. With the evolution of cyberspace, it is clear that legal frameworks must adapt accordingly. Cyber jurisprudence addresses key issues such as digital identity, virtual property and the challenges of cross-border jurisdiction, all of which are essential for regulating behaviour in the online world. However, with the growing reliance on digital platforms for personal, corporate and governmental activities, cyberspace has also become a breeding ground for cybercrimes, especially economic offences. These crimes have evolved from technical challenged into serious legal concerns highlighting gaps in the current laws. The borderless nature of online transactions complicate enforcement as perpetrators often operates from jurisdictions far removed from their victims. Consequently, cyber jurisprudence must adapt to not only govern online conduct but also to create robust mechanisms for detecting, attributing and prosecuting cyber economic offences. Developing legal standards that can navigate both the technological and geographical complexities of these offences is crucial to safeguarding the digital economy and ensuring justice in the cyber space.

[13] Calder V. Jones, 465 U.S.783(1984), https://www.oyez.org/cases/1983/82-1401 (last visited June 25,2025)

ISSN: 2582-6433

Legal and jurisprudential challenges in tacking Cyber economic offences in cyber space

The rise of cyberspace has given birth to new forms of criminal behaviour that are often transnational, anonymous and technologically sophisticated. Certain criminological theories help in explaining the reasons behind the commission of cybercrimes. The Routine activity theory, proposed by Cohen and Felson, states that "a crime occurs when a motivated offender, a suitable target, and lack of capable guardianship converge." [14] This theory holds strong in cyberspace, as the absence of physical boundaries increase opportunity for cyber criminals. The theory highlights the importance of monitoring, awareness, and prevention in digital space. Another theory is rational choice theory introduced by Clarke and Cornish (1986) which suggests that people commit cybercrimes when they perceive the rewards as high and the risks as minimal.[15] In the digital world, low risk of detection and high potential reward often encourage cyber offences. Crime displacement theory advanced by Felson and Clarke [16]in their collaborative work on situational crime prevention explains that crime prevention in one area may shift crime to another. Blocking one cyber route may lead criminals to try new tactics and targets. Displacement can be positive, neutral or even harmful.[17]According to Rober Agnew's General Strain theory, individuals under pressure, whether from financial struggles, social isolation or other forms of hardship may resort to cybercrime as a way to cope, feel empowered or gain control.[18] Another theory specific to cybercrime is, Jaishankar's Space Transition theory, which says that people who would not break the law in real life may commit crimes online because they feel anonymous and unafraid of consequences. People from closed societies may find cyber space a safe outlet for behaviour they supress offline. The theory also suggests that online and offline behaviours can influence each other.[19] These theories collectively offer insight into the motivations, circumstances and behavioural patterns that lead

[14] Lawrence Cohen & Marcus Felson, Social Change and Crime Rate Trends : A Routine Activity Approach, 44 Am.Sociol.Rev.588(1979), https://doi.org/10.2307/2094589 (last visited July 20, 2025)
[15] Maude Beaudry-Cyr, Rational Choice Theory, The Encyclopedia of Criminology and Criminal Justice (2014), https://doi.org/10.1002/9781118519639.wbecpx038 (last visited July 20,2025)
[16] Marcus Felson and Ronald V. Clarke, Opportunity Makes the Thief: Practical Theory for Crime Prevention, Police Research Series, Paper No.98 (Research, Development and Statistics Directorate, London, 1998), available at https://popcenter.asu.edu/sites/default/files/oppurtunity_makes_the_thief.pdf (last visited July 20,2025)
[17] Shane Johnson, Rob Guerette and Kate Bowers, Crime Displacement: What We Know, What We Don't Know, and What It Means for Crime Reduction, 10 J.Experimental Criminology 549 (2014), available at https://doi.org/10.1007/s11292-014-9209-4 (last visited July 20, 2025)
[18] Robert Agnew, Foundation for a General Strain Theory of Crime and Delinquency, 30(1) Criminology 47(1992), https://archive.org/details/criminology-february-1992-agnew-foundation-for-a-general-strain-theory-of-crime-and-delinqency/page/48/mode/2up (last visited July 16, 2025)
[19] Jayashankar Karuppannan, Cyber Criminology and Space Transition Theory: Contribution and Impact(2019), available at https://doi.org/10.13140/RG.2.18087.80806 (last visited July 20, 2025)

ISSN: 2582-6433

to digital crimes.

Cybercrimes include a wide range of harmful activities carried out using computers or online platforms. This includes economic offenses which exploit digital vulnerabilities. These cyber economic offences which includes a wide range of financially motivated crimes conducted through or against information systems, are emerging as one of the most pressing challenges in the realm of cyber jurisprudence. These growing threats highlight the urgent need to rethink and expand traditional legal principles to effectively respond to the complex realities of the digital age.

Cyber economic offences can be broadly categorised into three main types,
(i) Fraud based offences
(ii) Data-centric offences and
(iii) High-tech financial crimes

(i) Fraud based cyber economic offences

Fraud based offences involve deceit and misrepresentation to unlawfully acquire financial assets
(a) Phishing
(b) Online banking fraud and
(c) Credit card cloning

(a) Phishing

Phishing constitutes a form of cyberattack where individuals are deceived into revealing sensitive information, downloading harmful software, or clicking on deceptive links. Cybercriminals typically pose as reputable organisations, like banks or delivery services and send messages that appear genuine through email, text messages, or social media platforms.

There are several variants of phishing like:
Spear phishing**,** which involves highly targeted attacks tailored to specific individuals, often incorporating personal details like interests, recent transactions or online behaviour to enhance credibility. Whaling targets high ranking officials, such as CEO's or senior executives, aiming to access critical organisational information due to their authority and privileged access. Smishing is another phishing technique conducted through SMS messages, where attackers

ISSN: 2582-6433

pose as acquaintances or service providers to solicit payments or updates. In quishing or QR code phishing QR codes embedded in emails are utilized. Scanning these codes redirect victims to malicious websites, often evading traditional email security filters. Vishing (voice phishing) involves telephone calls where scammers use spoofed caller ID's, often through Voice over Internet Protocol (VoIP) services, to impersonate legitimate organizations and extract sensitive information from victims.

These evolving forms of phishing highlight the sophisticated strategies employed by cyber criminals to perpetrate economic offenses in the digital environment

(b) Online banking Fraud

Online banking fraud involves unlawful actions conducted through internet based financial platforms, typically involving unauthorised access, data manipulation or fund diversion. These schemes exploit the user's limited awareness of digital security and often rely on impersonation, malware deployment and advanced social engineering techniques.

The primary types of online banking fraud are

Unified Payments Interface fraud (**UPI Fraud)** have seen a significant rise in countries like India, where digital payment systems are widely used. Fraudsters often impersonate bank representatives or trusted service providers to send phishing links or make deceptive calls, tricking users into revealing their UPI credentials or PIN's. These credentials are then exploited to perform unauthorised fund transfers.

Lottery/ Gift Scams involves deceiving victims into transferring money under the false promise of receiving prizes, foreign shipments or inheritances. Fraudsters frequently impersonate customs or courier officials to extract processing fees for releasing non- existent prizes. Such schemes exploit psychological manipulation and lack of verification protocols.

Card skimming and Credit card fraud involves unauthorised transactions using stolen or duplicate credit card information. In card skimming, fraudsters install covert devices on ATM's or point of sale terminals to extract card data, which is then cloned for unauthorised transactions. In a major incident reported in Europe in 2022, hackers exploited security loopholes in ecommerce websites to steal thousands of card credentials, later using them to

ISSN: 2582-6433

make fraudulent purchases.[20]

Fake loan offers involve scammers leveraging leaked personal data to impersonate legitimate lending agencies and promise quick loans in exchange for advance fees. Once the payment is made, the fraudster disappears, resulting in financial and identity loss for the victim.

Electronic Fraud includes fraud conducted through electronic devices such as computers, smartphones or ATMs to execute unauthorised financial activities. Common methods include malware attacks, SIM swap schemes and ATM skimming, all aimed at compromising user's sensitive banking information.

Money Transfer Scams involves coercing the victims to transfer money through untraceable services like Westen Union or MoneyGram, usually citing fabricated emergencies or impersonating relatives in distress. These scams offer no practical avenue for fund recovery.[21]
Internet Banking Fraud involves unauthorised access to the user's online banking account. Common methods include phishing emails, keyloggers and man in the middle (MITM) attacks[22], that allow attackers to intercept and manipulate data exchanges between users and banks. The hackers may redirect legitimate transactions to fraudulent accounts.

OTP and SIM Swap fraud occurs when One-Time Passwords (OTPs), commonly used for transaction authentication, are compromised through social engineering or SIM card duplication. Attackers request telecom providers to duplicate SIMs using falsified documents enabling them to intercept OTPs and access accounts.

(c) Credit card cloning

Card cloning, also known as skimming, involves duplicating the information from a stolen credit or debit card and transferring it into another card. This process typically requires capturing the card data using an electronic device or software at a payment terminal. Once the

[20] Shreya Shivkumar Mathpati & Pratibha C. Kaladeep-Yalagi, A Comprehensive Analysis of Modern Approaches to Fraud Prevention and Detection in Online Banking and Credit Card Transactions, 44 Libr. Progress Int'l 225 (2024), https://www.bpasjournals.com (last visited June 29 ,2025)
[21] Warangal City Police ,Cyber Awareness: Online Banking Fraud, https://warangalpolice.telengana.gov.in/online-banking-frauds (last visited June 29, 2025)
[22] Avijit Mallik, Abid Ahsan, Mhis Shahadat and Jia-Chi Tsou, Man-in-the-Middle-Attack: Understanding in Simple Words, 3 International Journal of Data and Network Science 77-92(2029) available at https://doi.org/10.5267/j.ijdns.2019.1.001 (last visited June 29,2025)

ISSN: 2582-6433

information is obtained, it can be encoded into a blank card or used to overwrite the data on an existing card, effectively creating a replica of the original for fraudulent use.[23]

(ii) Data Centric offences

Data centric cyber economic offence refers to criminal activities in cyberspace that revolve around the unauthorised access, manipulation or exploitation of data which may be personal, financial or institutional information for economic gain. These offences target the very foundation of the digital world, treating data as the primary asset to be exploited, manipulated or stolen. This include crimes that focus on the theft, misuse or unauthorised access of data, especially personally identifiable information (PII), which is the core element that supports digital communication and online interactions.

(a) Identity theft

Identity theft is a serious and growing data-centric cyber economic offence, which occurs when a fraudster unlawfully obtains and uses another's personally identifiable information (PII) like his name, addresses, banking credentials or government issued identification to commit fraud or other offences for financial gain or nonfinancial gain. This offence targets the informational foundation of cyberspace, exploiting digital systems to commit fraud in increasingly complex ways. Common methods used to commit identity theft include social engineering, phishing emails, spoofed messages and system hacking.

Types of identity theft include financial identity theft where a person's PII is used to steal money or to open unauthorised financial accounts such as credit cards, loans and mortgages. With the rise of digital services like online mortgages, fraud can occur with minimal human interaction, placing the burden of proof on the victim. Another type is Synthetic Identity Theft where fraudsters combine real PII like Social Security numbers (SSN) with fake details to create entirely new identities. Offenders may use valid SSN alongside invented names, addresses, and other personal details. This mix of genuine and false data helps synthetic identities appear credible to financial institutions, making them difficult to detect. Often fraudsters slowly build credit histories under these fake identities, increasing their creditworthiness overtime. This gradual progression enables fraudsters to carryout significant

[23] Sathyendra Sharma & Triveni Singh, Rising Cyber Fraud through Card Cloning : Global Concern in the Banking Industry 3(8) Int'l J.Sci.Res.Comput.Sci., Eng'g & Info.Tech.357 (2018), https://doi.org/10.32628/CSEIT1838100 (last visited June 30,2025)

ISSN: 2582-6433

financial crimes while remaining undetected, making it difficult to identify the fraud in its early stages.[24] Non-financial identity theft includes unauthorised access to medical services, utilities or telecommunications using someone else's PII. Medical identity theft is an increasingly serious issue in the healthcare sector. It occurs when someone unlawfully uses another person's personal information such as health insurance ID or social security number to medical records for financial gain. While it harms healthcare providers and insurers, the most severely impacted party is the patient. Victims may receive incorrect or even dangerous treatments based on falsified records, and they often face significant financial burdens from unauthorised medical bills charged to them or their insurance.[25]

(b) Criminal record fraud

This occurs when offenders use another individual's PII while committing crimes, causing legal and reputational damage to the victim. When a person's personally identifiable information is misused for fraudulent activities, they often face a long and difficult journey to prove their innocence and restore their reputation with institutions. In serious cases, if victims are unaware of debts occurred through identity theft, they may unknowingly face legal consequences, including potential criminal records. Victims may also be drawn into complicated procedures to demonstrate they were not responsible for unauthorised financial transactions involving stolen funds or credit card misuse.[26]

(c) Account Takeover fraud

Account takeover fraud is a frequent outcome of identity theft; wherein cyber criminals use stolen credentials to infiltrate a victim's online banking or financial accounts. After gaining access, they may alter account details, deny access to the rightful owner, and carryout unauthorised financial transactions.

(iii) High-tech Financial Crimes

High-tech financial crime refers to the use of advanced digital technologies to infiltrate computer systems, unlawfully access data, and execute cyber offenses motivated by financial

[24] Okunola Orogun et al., Strategies for Combating Synthetic Identity Fraud: The Role of Machine Learning and Behavioral Analysis in Enhancing Financial Ecosystem Security, 12 Int'l J. Res. Eng'g & Sci.280 (Apr.2024), https://www.ijres.org/vol12-issue4/1204280292.pdf (last visited June 29, 2025)
[25] M. Mancini, Medical identity Theft in the Emergency Department: Awareness Is Crucial, 15(7) W.J.Emerg. Med. 899 (2014), https://doi.org/10.5811/westjem 2014.8.22438 (last visited June 30, 2025)
[26] C S Kayser, S Back & M M Toro-Alvarez, Identity Theft: The Importance of Prosecuting on Behalf of Victims, 13(6) Laws 68 (2024), https://doi.org/10.3390/laws13060068 (last visited July 10, 2025)

ISSN: 2582-6433

gain. These crimes are typically carried out using sophisticated tools such as malware, phishing schemes, ransomware and other malicious software designed to infiltrate systems, steal information or disrupt digital operations.

Malware (malicious software) plays a central role in these attacks. Once installed, it can take control of devices, stealing sensitive financial data or cause damage to files and systems.

High-tech financial crimes such as ransomware attacks, crypto currency frauds and cyber extortion are becoming more common and dangerous. These crimes use advanced technology to cause serious financial damage to individuals, companies and even entire financial systems.

(a) Ransomware attacks

Ransomware is a type of malicious software that prevent users from accessing their devices or data by locking systems or encrypting files. Victims are then asked to pay a ransom, usually in cryptocurrency to regain access. This form of digital extortion has been in existence since late 1980's, with early cases involved payment through traditional mail.

These attacks can target individuals, organisations or geographic regions. The attackers are refining their techniques day by day to maximise impact and financial gain.

Some common types of ransomwares include scareware, which delivers fake malware warnings through popups to pressure users into paying for a non- existent fix without causing actual harm to files. Screen lockers block access to the system by displaying a full screen message often impersonating law enforcement and demand payment for alleged illegal activities. Encrypting ransomware or crypto ransomware, locks user's data by encrypting it and then demands payment in exchange for the key to decrypt the files. Mobile ransomware specifically targets smartphones through malicious apps or websites, locking the device and falsely claiming legal violations to extort payment from the victim.

Ransomware commonly spread through multiple channels that take advantage of both human and system vulnerabilities. One of the most prevalent methods is phishing and social engineering, where users are deceived into downloading malicious software through fraudulent emails or messages that often appear to be from legitimate sources. Another technique involves malvertising and automatic downloads that can infect a user's device with the silent installation

ISSN: 2582-6433

of ransomware without any further action beyond accessing a compromised or malicious webpage.

Cyber criminals also exploit unpatched software vulnerabilities in operating systems or applications, using these weaknesses as gateways to infiltrate systems. Furthermore, the theft of user credentials, especially those for remote desktop services, allow attackers to gain direct access and install ransomware. In several instances, ransomware is distributed in collaboration with other types of malwares. For example, the banking trojan, Trick Bot has been used to deliver ransomware such as Conti, emphasising the interconnected and continually evolving nature of cyber threats.

(b) Cryptocurrency fraud

Cryptocurrency is a form of digital money that exists as tokens or coins, which can be bought as an investment or used to pay for goods and services from vendors that accept it. Although its use as a regular payment method remains limited, its popularity as a speculative investment has grown significantly. Many investors are drawn to cryptocurrency like bitcoin, not for their practical use, but for the hope of profiting by selling them at higher prices, often based on market trends rather than any intrinsic value. Transactions involving cryptocurrency take place over decentralised, peer to peer networks and are recorded on block chains which are digital ledgers maintained by computers across the globe.[27]

Cryptocurrency fraud has emerged as a pressing concern in the digital economy, marketed by a rise in both the frequency and sophistication of scams. These fraudulent schemes exploit the decentralised and often unregularized nature of crypto market leveraging cyber-enabled methods to deceive investors. Rug pulls have emerged as a prevalent form of cryptocurrency fraud. It is a type of cryptocurrency scam in which the developers or promoters of a digital asset or blockchain project abruptly abandon it after securing significant investments, effectively disappearing with the investor's funds.

Rug pull scams manifest in several forms. In fake token launches or fraudulent initial coin offerings (ICOs), promoters create and aggressively market a new cryptocurrency, typically via social media and online forums, before vanishing with the raised funds. Exit scams follow

[27] David Kerr et al., Cryptocurrency Risks, Fraud Cases, and Financial Performance, 11 Risks 51(2023), https://doi.org/10.3390/risks11030051 (last visited July13, 2025)

ISSN: 2582-6433

a similar path with projects or exchanges operating legitimately for a period to build investor trust, only to shut down unexpectedly and abscond with user assets. In the decentralised finance (DeFi) space, malicious actors often develop yield farming platforms promising unrealistically high returns; once significant liquidity is deposited, the operators withdraw the assets and disappear. Another approach involves exploiting smart contract vulnerabilities in DeFi protocols, enabling developers to extract investor funds. Additionally, the Ponzi schemes, though not unique to digital assets, have become more common in cryptocurrency markets. These schemes typically offer high returns to early investors using the capital of newer participants. They inevitably collapse once the inflow of the new funds diminishes, resulting in significant financial losses.

These fraudulent practices exploit investor's enthusiasm and the lack of comprehensive regulatory oversight in the crypto currency space.

(c) Cyber extortion

Cyber extortion refers to a category of cybercrime in which offenders leverage digital threats to unlawfully compel individuals, corporations, or institutions to surrender money or confidential information. The coercion typically involves threats to damage data, reveal sensitive material or interrupt essential operations, often by exploiting vulnerabilities in digital infrastructure. With the increasing integration of technology into both personal and professional spheres, cyber extortion has emerged as a significant legal and cybersecurity concern.

Ransomware has emerged as one of the most prominent and rapidly evolving form of cyber extortion. Initially limited to locking systems or encrypting files in exchange for a ransom, known as single extortion, these attacks have since become more complex and coercive. Double extortion attacks involve cybercriminals extracting sensitive data prior to encrypting it and then threatening to expose the stolen information publicly if their ransom demands are not fulfilled. This tactic significantly raises the stakes, especially for organisations handling confidential or regulated data. Triple extortion further escalates the pressure by adding additional threats, such as launching distributed denial of service 9DDoS) attacks or contacting clients, customers or partners to expose the breach and inflict reputational damage. As a result, ransomware is no longer just a disruptive malware but a central tool in a broader extortion strategy, contributing to the growing complexity and danger of high-tech financial crimes in

ISSN: 2582-6433

the digital economy.

Beyond ransomware, cyber extortion can also occur through data theft followed by demands for payment under the threat of disclosure. Offenders may unlawfully access financial records, personal data, or proprietary information and threaten exposure unless a payoff is made. Another prevalent tactic is the publication of threat of publication of personal or damaging information, often referred to as doxing. Victims in these cases can range from private individuals to high-profile public figures and entities, with attackers frequently using social media platforms to exert pressure or maximise reputational damage.

These offenses are facilitated by a range of technical methods, including phishing campaigns, exploitation of software vulnerabilities and unauthorised access to digital systems. The increasing use of anonymizing tools and cryptocurrency transactions further complicates enforcement, as perpetrators can obscure their identities and operates across jurisdictions

Challenges in tackling cyber economic crimes in cyberspace

Cyber economic crimes have become one of the biggest challenges for today's legal systems. These offences use digital technologies to carryout financial crimes quickly and often without being detected. Criminals take advantage of weak points in digital infrastructure and outdated legal systems that were not designed to handle modern, high-tech crimes. Traditional laws based on ideas from the physical world, like property ownership or personal harm and now struggling to keep up with how crimes happen in the digital world

One reason for this gap is the way the internet was originally built. It was designed for sharing information, not for secure business transactions. As a result, the internet is open and not very secure, which makes it easy for criminals to steal data or commit fraud. With most banking and business transactions are taking place online, these weaknesses have become major risks.

Criminals today exploit darknet markets, fake investment platforms, and money laundering schemes to commit economic offences on a global scale. Tools such as VPNs and Tor browsers obscure their identities and locations, making it difficult for law enforcement to trace them. These digital tools make law enforcement less effective and reduce the fear of getting caught.

In India, the rise in cyber economic crimes has revealed critical gaps in the existing legal and enforcement frameworks. Although the Information Technology Act, 2000, Bharatiya Nyaya Sanhita and the Bharatiya Nagarik Suraksha Sanhita forms primary structure for regulating

ISSN: 2582-6433

cybercrimes, its enforcement faces serious limitations.

One major challenge is the lack of specialised training among law enforcement officials, including police, prosecutors and judges, in cybercrime investigation and digital forensics. This makes it challenging to effectively deal with cases that involve digital evidence and complex technological tools

The transnational nature of cybercrime further complicates enforcement by raising complex jurisdictional issues. Traditional rules based on geography will not work well when a criminal can commit a crime from another country, using servers in a third country, and target someone in yet another. To address this, Indian law incorporates doctrines such as subjective territoriality (where the act occurs), objective territoriality (where the consequences are experienced) and jurisdiction based on nationality(which considers the citizenship of either the accused or the victim).Provisions like Sec 3 of the Bharatiya Nyaya Sanhita and Sec 75 of the Information Technology Act extend India's jurisdiction to offences committed by Indian nationals or involving systems located within India, even if the act takes place abroad.[28]

Despite these provisions, enforcement remains problematic due to limited international cooperation and outdated legal frameworks. Many modern cyber threats such as crypto currency scams, phishing and ransomware are either inadequately covered or not addressed at all under current laws. The lack of well-defined legal frameworks hinders law enforcement agencies from effectively investigating, prosecuting and penalising offenders involved in these complex and often transnational crimes. To make the matters worse, delays in legal proceedings further weaken the enforcement mechanism. Data from the National Crime Records Bureau (NCRB)[29] indicates that, many cybercrime cases are pending for years or are closed due to lack of evidence.

In its decisions in Ajay Agarwal Vs Union of India[30] and Lee Kun Hee Vs State of UP[31], the apex court acknowledged that Indian jurisdiction may extend to criminal conducts with

[28] Mr. Justice A . Muhammed Mustaque, Jurisdictional Issues in Adjudication of Cyber Crimes, High Ct. of Kerala, Nat'l Judicial Acad., https://nja.gov.in/Concluded_Programmes/2022-23/P-1299_PPTs/2.Jurisdictional%20Issues%20in%20Adjudication%20of%20Cyber%20Crimes.pdf, (last visited July16,2025)
[29] Ministry of Home Affairs, Steps to Curb Cyber Crime, Press Info.Bureau (March 18, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=211244 (last visited July16, 2025)
[30] Ajay Agarwal Vs. Union of India, A.I.R. 1993 S.C. 1637
[31] Lee Kun Hee Vs State of U.P, A.I.R. 2012 S.C. 1007

ISSN: 2582-6433

transnational dimensions. At the international level, decisions such as the Microsoft Ireland Case[32] and Yahoo! INC Vs LICRA [33]reflect the growing complexity faced by courts in addressing issues of jurisdiction in cyberspace. In the absence of a comprehensive international legal framework, mechanisms such as Mutual Legal Assistance Treaties (MLATs) and bilateral Memoranda of Understanding (MoUs) remain essential instruments for facilitating transnational cooperation in cybercrime enforcement.

Although Conventions like the Budapest Convention on Cybercrime[34] aim to establish common international standards, India has not yet become a signatory, citing concerns over sovereignty and unequal obligations. As a result, enforcement still relies heavily on bilateral frameworks, which are often slow and ineffective.

Conclusion and Suggestions

The rapid growth of digital infrastructure and internet usage in India has led to a significant rise in cybercrimes, particularly those involving financial and economic harm. These offences pose complex challenges for law enforcement agencies, which must navigate legal and procedural hurdles, technological shortcomings and a shortage of trained personnel.

A key priority is enhancing the capacity of law enforcement through continuous investment in training and skill development. Many officers still lack the expertise needed to handle the complexities of cybercrime, especially in areas such as digital forensics and online financial fraud. Establishing specialised cybercrime units and offering regular training sessions, workshops and conferences can improve investigative and prosecutorial competence across criminal justice system Modernising technological infrastructure is equally important. Conventional tools and investigative methods are inadequate for dealing with sophisticated cybercrimes. Upgrading digital forensic labs, adopting AI-driven analytics and integrating databases across departments can make investigation more faster and more accurate. Ensuring that different systems work well together will help avoid delays and make it easier to share information efficiently.

Due to the global nature of cyberspace, cybercrimes frequently involve individuals and impacts

[32] Microsoft Corp Vs United States,829 F.3d 197(2d Cir.2016)
[33] Yahoo! Inc. Vs. La Lique Contre Le Racisme Et L'Antisemitisme, 433 F.3d 1199(9th Cir.2006)
[34] Council of Europe, Convention on Cybercrime, Eur.Treaty Ser.No.185,Budapest,Nov.23 2001, https://rm.coe.int/1680081561 (last visited July16,2025)

ISSN: 2582-6433

that stretch across national borders. Strengthening international cooperation is therefore essential, particularly through strong bilateral and multilateral frameworks that support information sharing and legal collaboration. India should also consider engaging with global instruments like the Budapest Convention on Cybercrime. Although not a signatory aligning domestic practices with international standards would enhance India's capacity to address transnational cyber threats more effectively Public engagement also plays a crucial role in improving cybercrime response. Many incidents go unreported due to fear, lack of awareness or mistrust in the system. Well-designed public awareness campaigns can empower individuals with knowledge about prevention and reporting mechanisms, while also building trust in the legal process. Outreach through media, community programmes and social influencers can broaden reach and impact.

Addressing cyber economic offences in India requires a collaborative and future oriented strategy. Strengthening enforcement capabilities, upgrading infrastructure, enhancing international partnerships, promoting public participation and reforming legal frameworks are interlinked steps that together create a resilient ecosystem for investigating and prosecuting cybercrimes.

At a broader level, the legal system must evolve in step with the expanding digital economy, especially to address the growing threat of cyber economic offences. These offences ranging from online financial fraud to identity theft and data breaches demand clear legal recognition of concepts such as digital property, virtual harm, and data rights, all of which currently lack comprehensive legal definitions and consistent judicial interpretation. While the Information Technology Act, 2000, provides the foundational framework for addressing cybercrime, it was originally designed for a different technological context and does not adequately cover many complex forms of economic offences committed in the cyberspace. Although recent initiatives such as the introduction of Digital Personal Data Protection Act, 2023[35] and sector-specific regulations issued by institutions such as Reserve Bank of India represent positive progress , significant gaps remain. These deficiencies highlight the urgent need for a more comprehensive and modernized legal framework capable of effectively tackling the financial and economic dimensions of cybercrimes.

[35] Digital Personal Data Protection Act,2023,No.22 of 2023, Acts of Parliament,2023 (India), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9fb4f8fef35ef35e82c42aa5.pdf (last visited July 16,2025)

ISSN: 2582-6433

India's criminal justice reforms, such as the BNS[36] and BNSS[37] represent steps in the right direction, but jurisdictional and enforcement challenges persist especially in the context of cross-border crimes. Strengthening protocols for international legal cooperation and exchange of digital evidence is crucial for successful prosecution.

To effectively combat the rising challenges of cyber economic offences, it is important to establish a legal framework that is progressive and capable of adapting to change. This includes introducing comprehensive laws that clearly define emerging forms of cybercrime, while also incorporating provisions in ethical hacking, digital privacy and data protection. The establishment of specialised cybercrime courts with trained judicial officers can significantly improve the speed and quality of case resolution.

In conclusion, the fight against cyber economic offences in India cannot succeed without a robust, well equipped and technologically informed legal system. As cyberspace continues to evolve, our legal and institutional systems must adapt. Without consistent and well-planned reforms, our efforts to tackle cybercrimes will stay incomplete and less effective. Strong steps are to be taken to develop comprehensive legal mechanisms capable of addressing the complexities of the digital world.

[36] Bharatiya Nyaya Sanhita,2023, No.45 of 2023,Acts of Parliament,2023 (India), https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf (last visited July 16,2025)
[37] Bharatiya Nagarik Suraksha Sanhita,2023, No.46 of 2023,Acts of Parliament,2023 (India), https://www.mha.gov.in/sites/default/files/2024-04/250884_2_english_01042024.pdf (last visited July 16,2025)