IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

E-commerce: Contributor to Cybercrimes

[1]Isabell Manoj, [2]Dr. Vidya Ann Jacob

[1] Student, LLM(Corporate and Commercial Law), Christ (Deemed to be University), Bengaluru

[2] Assistant Professor, School of Law, Christ (Deemed to be University), Bengaluru

Abstract: E-commerce has rapidly transformed the retail and commerce landscape in India. While e-commerce has made shopping more convenient for consumers, providing wider selections and competitive pricing, its growth has also been accompanied by increased cybercrime. This paper investigates the relationship between the rise of e-commerce and cybercrime rates in more comprehensive selections in India by examining existing literature and statistical analysis of government and industry data. The anonymity afforded by the Internet, coupled with jurisdictional ambiguities across international boundaries, constrain efforts to identify these fraudsters and investigate cross-border cybercrimes. Demands for reform include expanding definitions of cybercrimes, increasing penalties, enabling faster trials and granting law enforcement access to digital forensics and surveillance tools while protecting citizen privacy. Acute jurisdictional complexities arise in investigating cross-border e-commerce cybercrimes spanning multiple nations with divergent legal protocols. Despite the benefits of online financial transactions, people started highlighting the fear of financial cybercrimes among the top concerns that impact their daily lives. It concludes that optimised regulation is imperative to enhance India's cyber readiness, leveraging the digital public goods generated by e-commerce innovations while safeguarding citizen rights and cyber-physical security. Recommendations encompass reforming legal frameworks, strengthening law enforcement capabilities, augmenting cybersecurity protocols, enhancing public awareness, and fostering greater public-private collaboration focused on the prevention, detection and deterrence of emerging e-commerce-related cyber threats.

Keywords: E-commerce, Cybercrimes, Financial fraud, Identity theft, IT Act 2000, Cybersecurity

1. INTRODUCTION

Cybercrimes are rising in the country due to the emergence of technological developments that have made the common man's life smooth and easy-going. E-commerce enhanced consumers' purchasing power, thereby changing citizens' lifestyle patterns. From the newest idea of ordering food online to bringing the entire salon to your doorstep, it is possible due to the intervention of E-commerce in our daily lives. As it is said that everything that comes easy also goes easy, e-commerce was a boon to the fraudsters who were constantly

vigilant over newer modes of looting from the public. The types of cybercrimes include online financial fraud, hacking, identity theft, phishing scams, and other cyber-enabled offences involving deceit to obtain personal data or money.[1]

E-commerce has facilitated access to wider arrays of goods and services, reduced transaction costs for buyers and sellers, bridged geographic divides between demand and supply, and enhanced financial inclusion. India's e-commerce market has witnessed exponential growth, evidenced by its considerable contribution to economic growth and employment generation. Greater dependence on digital payments, online data collection, remote transactions, and integration with social media expand the attack surface for potential misuse by cyber criminals, ranging from petty fraudsters to organised cyber-criminal networks.[2]

The criminals had co-evolved and adapted in response to the socio-technical environmental advancements. The criminals found ways to commit crimes remotely without being tracked or caught. The criminal activities evolve more rapidly than the advancements adopted by the Indian Cybercrime Coordination Centre (I4C)[3] . The Information Technology Act 2000, enacted before the e-commerce revolution, contains critical lacunae in addressing related offences. In 2017, consumers in India collectively lost over 18 billion U.S. dollars due to cybercrimes[4]. These were merely estimations, though, based on numbers that had been released. The statistics may be underreported in a nation like India since there are insufficient systems to categorise or raise awareness of cybercrime.

The primary cause of the unexpected increase in online crimes starting in 2017 may be recent government actions, such as creating a unique online platform for reporting cybercrimes.[5] This research applies an interdisciplinary approach combining insights from cyberpsychology, criminology and socio-legal studies to probe the complex dichotomy posed by e-commerce, enriching commerce and empowering consumers while simultaneously spawning unintended risks and harms.[6]

2. LEGAL FRAMEWORK INVOLVING CYBERCRIMES

The significant and primary framework for cybercrimes in India is the Information Technology Act of 2000[7], enacted by the Indian parliament. The IT Act stated that only computer systems and networks should be exempt from the legality in cases involving electronic communications, commercial transactions, trade, and commerce. The Act addresses several topics, including the legal acceptance of digital signatures and electronic documents, cybercrimes and their violations, and the mechanisms for distributing justice in these cases. Due

[1] *What is Cyber Crime?,* Proofpoint (Mar. 20, 2024, 11:57 PM), https://www.proofpoint.com/us/threat-reference/cybercrime#:~:text=In%20a%20digital%20context%2C%20identity,identity%20to%20conceal%20their%20own.
[2] Munjal, Sourabh & A., Anooja, *Cyber Crimes Threat for the E-Commerce*, SSRN Electronic Journal, 10.2139/ssrn.2767443.
[3] The MHA founded the Indian Cybercrime Coordination Centre (I4C) in New Delhi to give Law Enforcement Agencies (LEAs) a framework and ecosystem for addressing cybercrime in a coordinated and all-encompassing way. It is intended for I4C to serve as the focal point for reducing cybercrime in the nation.
[4] Cybercrime in India, Statistics report on cybercrime in India, Statista, 2022, https://www.statista.com/study/59177/cyber-crime-in-india/.
[5] Harikishan Sharma, *NCRB data: Cybercrime jumped by 77% in 2017*, The Indian Express, Oct. 23 2019, https://indianexpress.com/article/explained/ncrb-data-cyber-crime-jumped-by-77-in-2017-6082779/#:~:text=(NCRB)%20show.-,A%20total%2021%2C796%20instances%20of%20cyber%20crime%20were%20recorded%20in,the%202015%20number%20of%2011%2C592.
[6] *id.*
[7] The Information Technology Act, 2000, No.21, Acts of Parliament,2000 (India).

to the rising technological development and increased data stealing, The Act was amended in 2008. However, neither act mentions the definition of cybercrime and is vague. Priority was mostly given to privacy issues. [8]

Section 66[9] of the Act defines hacking, and Section 63-74[10] gives the government the power to take action against any cybercrime in the country. Besides the Act, India's legal framework contributes to cybercrime through the Indian Penal Code (IPC)[11], Criminal Procedure Code (CrPC)[12] and Indian Evidence Act[13]. Cybercrime is treated as any other crime in India; therefore, using the said Acts is also valid. The only problem that the authorities face is jurisdiction as cybercrimes do not confine themselves to any physical boundaries, nor can the effect be felt unless and until it turns into a crime that society faces difficulty with.

The IPC's Sections 406, 408, 420, and 468 address offences about online fraud and cheating[14]. Cyberbullying and stalking offences are included under Section 509[15]. CrPC is the primary procedural law on criminal behaviour in India. It establishes the protocols for examining, prosecuting, and sentencing criminal acts, including cybercrime. The guidelines for arrest, search, seizure, and bail are also outlined in the CrPC. Cybercrime cases are also subject to the Indian Evidence Act. It establishes the guidelines for the admissibility of evidence in criminal prosecutions, including digital evidence from social media, chat logs, and emails. Evidence Act sets forth the kinds of evidence that are admissible in court, how they are presented, and how they are assessed.[16]

3. RISE IN CYBERCRIME RATES THROUGH E-COMMERCE

3.1 The Development

E-commerce has been an adding factor to the extensive cybercrime rates throughout our country. The various incidents of fraudsters asking for a one-time password (OTP) through mobiles to spam our E-mail all come under cybercrime. E-commerce has also been a method to contribute to these crimes due to the need for more security.[17] All of us, being in the realm of e-commerce and constantly using e-commerce to get our necessities fulfilled quickly, surely know the procedure involved, the extent of data collected from the consumers, and the legal consent consumers are forced to give to avail the services. The immense amount of data procured by these online businesses is a source of income by selling it to hackers who misuse it to extort money or other purposes.[18]

[8] Raagini Sharma, *Legal Framework for Cyber Crimes in India and Beyond*, Research Institute for European and American Studies, 24th July 2021.
[9] The Information Technology Act, 2000,§66, No.21, Acts of Parliament,2000 (India).
[10] The Information Technology Act, 2000, §63-74, No.21, Acts of Parliament,2000 (India).
[11] Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).
[12] The Code of Criminal Procedure, 1974, No.2, Acts of Parliament, 1974 (India).
[13] The Indian Evidence Act, 1872, No.1, Acts of Parliament,1872 (India).
[14] Indian Penal Code, 1860, §406,§408,§420,§468, No. 45, Acts of Parliament, 1860 (India).
[15] Indian Penal Code, 1860, §509, No. 45, Acts of Parliament, 1860 (India).
[16] Dhanashree Chowdhury, Mahua Roy Chowdhury, *The Indian Penal Code (IPC), the Criminal Procedure Code (CrPC), and the Indian Evidence Act to be revamped*, Lexology, Sept. 6 2023 https://www.lexology.com/library/detail.aspx?g=c84a6d2d-d128-4ad4-b8ef-cac874bbdbd8.
[17] Adv. Rupa K.N, *What Kind of Cybercrime exists in E-Commerce?* , Ezy legal (Mar. 21 2024), https://www.ezylegal.in/blogs/what-kind-of-cybercrime-exists-in-e-commerce.
[18] *How do Malicious Hackers Earn Income?,* Packetlabs (Mar.21 2024), https://www.packetlabs.net/posts/hacker-income/.

Analysing the development of e-commerce in the country, it is proved that if there has been a decline in e-commerce activities, it is due to issues with privacy and security in the systems. Even though the number of e-commerce providers has risen in the last few years, the development of the security of the data collected is invisible.[19] The popularity of a website depends on the trust its consumers have in data protection. The giant development of e-commerce is another risk towards cybercrimes. Although the world has become more digital, business ties have remained the same to support efforts to combat cybercrimes. Advanced technology may be unavailable to other organisations due to the influence of a few large, technologically-savvy firms. As a result, network creation, deployment, and use are determined by organisational structure. Therefore, it is necessary to include the digital economy in inter-organizational networks and partnerships. The establishment of these interdependencies and linkages is crucial to the expansion of e-commerce.[20]

Cybercrime, whether related to e-commerce or not, is the threat created by dishonest or careless computer users who take advantage of the pervasive use of computer networks. It jeopardises most business information systems' integrity, safety, and quality; hence, developing strong security measures is paramount. Cybercrime in e-commerce is generally understood as the unlawful or illegal use of computer resources for online business-related activity.[21]

3.2 Cybercrime and E-commerce Transactions

Cybercriminals use malware to inflict damage or disable machines, erase or pilfer data, and launch denial-of-service (DoS) assaults. Cybercrime related to e-commerce entails using computers for offences such as disseminating viruses, unlawful data, or illicit photos. Malware is frequently installed on computers by cyber criminals, and several nations have recognised computer use as an accomplice.[22] Cybercrimes stand in the way of e-commerce and online business growth. Clever criminals are using cybercrime to expand their rapidly expanding underground companies. They buy and sell highly classified financial data from several web clients in an online bootleg market. These cyber specialists are incredibly skilled at regularly breaking into many PCs and involve vast sums of money.[23] The most common way harmful malware infiltrates our computer systems is through cyberattacks. After that, this malware completely takes over our system, giving the crooks access to all the data on our computer system. Neither the owner nor the user is aware of the entire process.

Cybercrimes have escalated in tandem with the growth of the internet industry, affecting global e-commerce as well as people. While total eradication of cybercrimes may not be possible, the complexity of cybercrimes

[19] Cynthia Ruppel, Linda Underwood-Queen and Susan J. Harrington, *e-Commerce: The Roles of Trust, Security, and Type of e-Commerce Involvemen*t, E-Service Journal, Vol. 2, No. 2, Winter,2003, pp. 25-45.
[20] Dorothy Leonard-Barton, William A. Kraus, *Implementing New Technology*, Harvard Business Review (Mar 21 2014) https://hbr.org/1985/11/implementing-new-technology.
[21] Rajkumar Dubey, *Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both" – In Indian Legal Perspective*, Mondaq, Sept. 24 2024, https://www.mondaq.com/india/technology/28603/cyber-crimes-an-unlawful-act-where-in-the-computer-is-either-a-tool-or-a-target-or-both.
[22] N. Leena, *Cyber Crime Effecting E-commerce Technology*, Oriental Journal of Computer Science & Technology, Vol. 4(1), 2011, pp 209-212.

[23] Sood, Aditya, Bansal, Rohit, Enbody, R.J., Cybercrime: Dissecting the State of Underground Enterprise, Internet Computing, IEEE, Vol 17, pp 60-68, 10.1109/MIC.2012.61.

in e-commerce requires both technological and non-technical measures to manage hazards.[24] Businesses like banking and retail are becoming more dependent on electronic media and the internet, which leaves them open to cybercriminals. Businesses that are going online are happy about the growth potential, but they are also worried about security because their money and confidential data are at danger. Due to its virtual nature, e-commerce presents certain difficulties and dangers that exacerbate fraud and criminality. Uncontrolled e-commerce cyber frauds in India can be attributed to a number of factors.[25] As more company operations go online, the cost of cybercrime is expected to increase. Theft of intellectual property is a serious issue that costs parent companies money. Governments must act decisively to prevent cybercrime because it has the potential to negatively impact enterprises. Annual losses from cybercrime surpass 400 billion dollars worldwide.[26]

3.3 Statistical Analysis of Cyber Crime in E-commerce Transaction

The rates of cybercrimes in the country speak for the increasing cyber-attacks and prove now and then that initiatives to tackle this issue were left long back.

As per the National Crime Records Bureau (NCRB) report, India had 52,974 incidences of cybercrime in 2021. This rose more than 15% from 2019 and more than 5% from 2020.

According to the Ministry of Home Affairs, between January 1, 2020, and December 7, 2022, over 16 lakh cybercrime occurrences and over 32,000 FIRs filed. During the examined period, the largest percentage of cybercrimes were reported in Uttar Pradesh and Karnataka.[27]

According to the open data source provided by the Indian Government, the total number of crimes reported as of 2020 is around 50035 cases. The table below shows the total number of cases related to e-commerce:

Violation of privacy	742
Data theft	98
Fraud	10395
Credit /Debit card	1194
Online banking fraud	4047
OTP frauds	1093

Around 17600 cases are related to e-commerce, proving that e-commerce contributes to cybercrime in the country. [28] If we look at it on a global level, A report calculating the global cost of cybercrime, cybercrime is

[24] Sujoy Kapoor, *Cybercrimes in E-commerce*, International Journal of Scientific & Engineering Research, Vol 11, Issue 7, July 2020.

[25] Sourabh Munjal, Anooja A., *Cyber Crimes Threat for the E-Commerce,* Jan. 2016, SSRN Electronic Journal, 10.2139/ssrn.2767443.

[26] Net Losses: Estimating the Global Cost of Cybercrime, Centre for Strategic and International Studies, June 5th 2014, https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime#:~:text=The%20Center%20for%20Strategic%20and,is%20more%20than%20%24400%20billion.

[27] National Crime Records Bureau, *Crime In India*, https://ncrb.gov.in/crime-in-india.html.

[28] Crime Head-wise & State/UT-wise Cyber Crimes during 2020, Open Government Data (DGD) Platform India, https://data.gov.in/resource/crime-head-wise-stateut-wise-cyber-crimes-during-2020.

expected to cost the world economy more than $400 billion annually.[29] India has had a 107% common annual growth rate in the number of cybercrime incidents reported in the past several years. The annual growth in cybercrime cases demonstrates the gravity of the escalating abuse of computer resources and the internet.[30]

Over 14 billion data records have been stolen from e-commerce businesses since 2013, according to the Gelmato Breach Index[31].Furthermore, research indicates that online businesses which lose less than 1% of their customer base might potentially lose $2.8 million in actual income annually. To understand the extent of cybercrimes in the e-commerce industry, we must realize that 95% of compromised records in 2016 originated from the government, retail, and technology sectors.[32] A research by the University of Maryland Clark School quantified the frequency of hacker attacks. They determined that there is a hacking attack on average every 39 seconds.[33] According to the Bank of Ghana's 2018 banking cyber fraud report, cybercriminals have taken or tried to take 325.9 million Ghana Cedis, or 61.5 million US dollars, from the country's financial institutions.[34]

Since e-commerce's inception, fraud has existed. However, the COVID-19 pandemic's surge in online sales and purchases gave fraudsters a new window of opportunity. Prior to the pandemic, only 24% of scams recorded worldwide were related to internet purchasing; by 2020, this percentage had increased to 38%. Even while that number has decreased as the crisis has passed, security lapses still have a significant negative impact on the sector, with losses from online payment fraud reaching over 40 billion dollars in 2022. Given these circumstances, it is anticipated that the market for e-commerce fraud detection and prevention will surpass $100 billion in sales by 2027, which is two times growth between 2023-2027.[35]

4. CONCLUSION AND SUGGESTIONS

Global cybercrime is spreading and negatively impacting international trade, either directly or indirectly. Governments and organisations are implementing measures to protect consumers and foster e-commerce free from cybercrime. Customers should be knowledgeable of cybercrimes and assist in preventing them. The expectation that the growth of online markets will be slower may result from the variety of hazards and the novelty of crime, and the fall in confidence may have favoured other causes. That being said, this perspective

[29] Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies (CSIS), McAfee, June 5 2014.
[30] Lallmahamood, Muniruddeen. "An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of this on their Intention to Use E-commerce: Using an Extension of the Technology Acceptance Model." Journal of Internet Banking and Commerce 12 August (2007)
[31] Julie Olenski, *New Gemalto Breach Level Index Reports Nearly Two Billion Records Were Either Lost or Stolen Between January and June*, GlobalSign Blog, October 11 2017.
[32] *Cybersecurity: A Global Priority and Career Opportunity*, University of North Georgia, https://ung.edu/continuing-education/news-and-media/cybersecurity.php
[33]Michel Cukier, *Study: Hackers Attack Every 39 Seconds*, University of Maryland, Feb. 9th 2007, https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds#:~:text=A%20Clark%20School%20study%20is,attackers%20more%20chance%20of%20success.
[34] Bank of Ghana Report, 2019.
[35] Stephanie Chevalier, *E-commerce fraud- Statistics and facts*, Statista, June 7 2023.

is not grounded in reality. E-commerce is seeing an increase in the number of customers. Consequently, the transactions are documented as being available to customers and criminals.

A favourable association has been shown between the rise in internet business and the subsequent rise in cybercrimes. Cybercrime has been affecting millions of people's lives and e-commerce worldwide, spreading its broad tentacles. Even while not every person with an internet connection is a victim of cybercrime, practically everyone is in danger. Every single person with an internet connection is susceptible in some manner. More specifically, there are many avenues available to cybercriminals to perpetrate crimes when discussing e-commerce. Consequently, developing technical and non-technical solutions to this issue is imperative. Although there can never be a complete solution to the cyber security issue, we must combat it with rigour and commitment.

Regulated Legal framework and Enforcement Capabilities

The legal framework for cybercrimes legally existing in India is not efficient enough to handle the cases. The advancement of cyber technology has outpaced the development of cyber regulation. In light of the worldwide issues, the Information and Technology Act is a single piece of insufficient legislation. Though they have been drafted, nations such as Europe and Singapore do not enforce them. Even though different standards for determining cyberspace jurisdiction have been established, determining the jurisdiction in cybercrime cases involving many nations remains a contentious issue in legal forums.

Different governments use different criteria to define jurisdiction. However, as the world's population will use the Internet more and more every second, rules about their jurisdiction should also be innovative enough to tackle cybercrime. The capability to apply the legal provisions and theories on the issues and the whole process of finding the culprit has to be efficient enough and quick to avoid delays.

Public Awareness

The most effective solution to cybercrimes is public awareness. Citizens should be aware of the intentions of fraudsters and the methods of cyber hacking involved in the technological environment. They should be taught what information is to be shared and what is not to be. The Passwords must be strong. The OTP’s are not to be shared. No bank will contact you directly and ask for any personal information. All these are to be shared. Citizens who are vulnerable, uneducated about the internet are targeted more. Therefore, they should be initially provided with awareness.

Public-Private Collaboration (Deterrence and detection)

The public and private sector businesses should collaborate to prevent cybercrimes. They must ensure cybercrimes do not occur through the leak of data from their end and take action against others who are indulged in it. Thereby, preventing these crimes can be enforced rather than regretting the losses. Digital forensics is used to investigate digital documents. Digital forensics must be made strong by the government to detect cybercrimes and prevent them as soon as possible.

Other Recommendations

Furthermore, the research suggests reforms in banking, financial services and e-commerce platforms to improve and develop new cybersecurity and anti-fraud systems. Wider adoption of multifactor authentication, Artificial intelligence (AI) based anomaly detection, stringent data protection standards, cyber hygiene and cybersecurity awareness programs, and compliance mechanisms are recommended. Ultimately, a combination of proactive technological safeguards, vigilant policing, contextualised legislation and public-private cooperation is requisite to nurture the immense benefits of e-commerce while curtailing its criminal downsides.

REFERENCES

1. Sujoy Kapoor, Cybercrimes in E-commerce, International Journal of Scientific & Engineering Research Volume 11, Issue 7, July 2020
2. N. Leena, Cyber Crime Effecting E-commerce Technology, Oriental Journal of Computer Science & Technology, Vol. 4(1), 209-212 (2011)
3. Grant Thornton India LLP, Law & Technology: Evolving challenges as a result of fraud in the E-commerce Sector (2015)
4. Shweta, Vikas Deep and Naveen Garg, Cyber Threats and Its Impact on E-Commerce Sites, International Journal of Control Theory and Applications, Vol 10, Issue 15, 2017.