INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

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

ISSN: 2582-6433

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

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

REGULATION OF CYBER FRAUDS IN THE ARENA OF E COMMERCE LAW

AUTHORED BY - ADV. RASHMI. A
Pursuing LLM in Corporate and Commercial laws.

ABSTRACT

The barter system, the time when the act of exchange of goods and services between people to satisfy their needs and wants, gave birth to the term "trading". Since then, trading has become an integral part of our society. In the year 1989, when the concept of the internet took birth, the virtual world became accessible at the fingertips of people; it would not be wrong to say that the internet has absolutely become an integral part of every person as it governs almost all the important aspect of human lives like Education, shopping, gaming, and virtual socialization. In today's era, the buying and selling of goods and services are vastly done over the internet. Any kind of such online transactions made over the internet will be termed as Ecommerce.

From one angle, we can see how the E-commerce sector is becoming an important part of our lives, but on the flip side, we are also witnessing the dark side of this platform where people are becoming the victims of cybercrime and cyber fraud. E-commerce is a platform that involves monetary and informational transactions online, which is also highly susceptible to data breaches and money theft. We should know that the theft of information of someone causes more harm and damage than the latter and puts millions of innocent internet users into mental trauma.

In order to tackle these problems, the Indian government enacted the Information technology act in the year 2000. However, this has just been an enabling statute to deal with cyber-related issues and crimes. Other than this act, we can clearly observe that there are no further dedicated acts to deal with in the matters of E-commerce law. The nation is witnessing the growth of Digital India; the trajectory of the e-commerce industry has been exponentially growing and is expected to beat the US by 2034; by this analysis, we can determine how the sector has tripled its growth from 2015. however, this is just the beginning of our technology sector getting ready for an e-commerce warfare and competition of its own. At least now, it's high time that we can get fresh

ISSN: 2582-6433

regulation to give provisions and regulations to anticipate the problems that might occur due to fraud and data breach that happens in E- the commerce industry.

Therefore, this research paper follows the doctrinal method of research examining various primary resources like acts, statutes, commentaries etc., tries to make an in-depth analysis on-

1. why we need stronger regulations in order to enable a friendly environment in the arena of E-commerce
2. and we shall also try to analyse various kinds of cyber fraud-related cases
3. explore the grey areas as to where the Indian cyber regulation can do better and their effectiveness in dealing with the legal issues involved in E-commerce.

And thereby conclude why the nation is in dire need of new regulation and a proper framework for a hassle-free online transaction where people can be safe, and their information can be protected, and monetary transaction can take place in a secure manner.

INTRODUCTION

The legal domain of e-commerce in India is multifaceted and dynamic, addressing several aspects such as contract law, cybersecurity, data protection, and consumer protection. The Information Technology Act, 2000 (IT Act) is the primary legislation of law that governs e-commerce in India. A comprehensive framework for regulating cyberspace, including e-commerce, is provided under the IT Act. The IT Act, however, has come under criticism for being outdated and unable to keep up with the quick speed of advancement in technology and the ever-evolving landscape of e-commerce. Notwithstanding these recent advancements, the Indian e-commerce legislation still has a lot of unclear provisions. For instance, India lacks a comprehensive data privacy regulation, which is problematic given the growing volume of private data that e-commerce companies gather and handle.

In the field of e-commerce law, cyber fraud regulation is a complicated matter, but it is one that must be addressed to safeguard customers and companies. To provide a more reliable and safer environment for online transactions, a new legislative framework addressing the critical areas of consumer protection, data protection, cybersecurity, and payment security is required.[1]

[1] Rao &Metts, Electronic Commerce Development in Small and Medium Sized Enterprises: A Stage Model and its Implications 9 (1) Business Process Management Journal 11-32 (2003).

ISSN: 2582-6433

Furthermore, e-commerce companies are not yet subject to any particular cybersecurity regulations from the Indian government. Companies that operate in the Indian e-commerce sector must to be aware of the applicable rules and legislation and take the necessary precautions to abide by them. This entails putting in place suitable cybersecurity and data protection safeguards as well as making sure that their online contracts adhere to Indian law.

All things considered; Indian e-commerce legislation is still developing. However, the government is dedicated to developing a strong legislative framework for online commerce that safeguards the interests of both businesses and consumers.[2]

Some of the key features of E-commerce is as follows:

i. Data protection: The IT Act stipulates a number of fundamental data protection measures, including the need to get consent before collecting or using personal information. But the IT Act doesn't offer a thorough foundation for data security.
ii. Protection of customers: In the context of e-commerce, consumers are given further protection under the Consumer Protection Act, 2019. For instance, the Act grants customers the right to a fast and equitable resolution of their complaints as well as the right to a refund or exchange within seven days of receiving a goods.
iii. Cybersecurity: E-commerce companies are not subject to any special cybersecurity regulations under the IT Act. On the other hand, the Indian government has released cybersecurity rules for online retailers.
iv. Contract law: Online and offline contracts are formed and enforced in accordance with the Indian Contract Act, 1872. Certain laws pertaining to electronic contracts are also included in the IT Act.

RESEARCH QUESTIONS

1. What are the gaps and challenges in the current regulatory framework? Which are the grey areas as to where the Indian cyber regulation can do better and their effectiveness in dealing with the legal issues involved in E-commerce.
2. Which are kinds of E commerce fraud and analyse with case study.
3. How can consumers be educated about the risks of cyber fraud in e-commerce and how

[2] See Dearmon Valorie, Risk Management and Legal Issues (Jones and Bartlett Publisher, LLC) Available on http://www.jblearning.com/samples/0763757144/57144_CH15_470_493. pdf

ISSN: 2582-6433

to protect themselves?

RESEARCH OBJECTIVES

The aim of the research is to help create a stronger and more efficient legal and regulatory framework to fight cybercrimes in e-commerce, safeguarding both companies and customers.

i. to determine the legal obstacles to controlling cybercrimes in e-commerce, especially when dealing with international transactions.
ii. to create a legislative framework to control payments made through online stores in an effort to lower the danger of cybercrime.
iii. to evaluate the contribution of data protection laws to the control of cybercrimes in online shopping.
iv. to create suggestions for strengthening consumer protection legislation in order to shield customers against online scams.
v. to determine the best methods that companies may use to stop and fight online fraud.
vi. to provide consumer education on the dangers of cybercrime in e-commerce and self-defence strategies.

RESEARCH METHODOLOGY

For this current research work, the doctrinal method of research has been followed. In order to conduct this research, the reference of all the Primary sources like Acts, statutes and bare acts have been made and the reference of the secondary sources like websites, Legal databases like Manupatra has been utilised for the purpose of this research.

ANALYSIS

why we need stronger regulations in order to enable a friendly environment in the arena of E-commerce

The way we purchase has been completely transformed by e-commerce, but it has also given fraudsters new avenues to operate. Cybercrime in electronic commerce can manifest in several ways, including credit card fraud, identity theft, and phishing schemes.[3]

[3] Eisingerich, Andreas B.; Kretschmer, Tobias, In E-Commerce, More is More, 86 Harvard Business Review 20–21 (March, 2008):.Available on http://hbr.org/2008/03/in-ecommerce-more-is-more/ar/1

ISSN: 2582-6433

Some nations have additionally enacted particular rules and regulations to handle particular forms of cyber fraud in e-commerce in addition to these basic guidelines. The Information Technology Act, 2000, for instance, was put into effect in India and provides prohibitions against cybercrime. The Act also created the Indian Computer Emergency Response Team (CERT-In), whose duties include coordinating cyber security measures in India and reacting to intrusions.

Regulators' best efforts notwithstanding, cyber fraud in e-commerce persists. However, hackers are finding it harder to operate as a result of the increased regulation of e-commerce.

Here are a few particular instances of how regulations are being applied to stop cybercrime in online shopping:

i. European Union: The General Data Protection Regulation (GDPR) in the European Union mandates that e-commerce businesses get consumers' consent before collecting or using their personal data. Customers now have the ability to view, update, or remove their personal data thanks to the GDPR.
ii. The United States: The Federal Trade Commission (FTC) in the US has released rules for online retailers on how to safeguard customer information. In addition, the FTC has taken legal action against online retailers that have neglected to secure customer information.
iii. China: According to China's E-Commerce Law, online retailers must confirm the legitimacy of their vendors and take action to stop the selling of fake goods. Additionally, customers have the legal right to return items they bought online for a complete refund within seven days.[4]

Cybercrime legislation in e-commerce is a complicated and developing legal field. Regulators' dedication to shielding customers from this kind of deception is evident, though.

Which are the grey areas as to where the Indian cyber regulation can do better and their effectiveness in dealing with the legal issues involved in E-commerce.

There are a few murky areas under the Information Technology Act, 2000 (IT Act), which codifies Indian cyber legislation, and they might be filled in. These consist of:

[4] Ramakrishnan Et Al., E-commerce in India-Growth and Prospects, 2(3) Asia Pacific Journal of Research in Business Management 101-114 (2011).

ISSN: 2582-6433

i. Privacy: In the context of e-commerce, the IT Act lacks a thorough structure for safeguarding user privacy. This has raised questions about how e-commerce platforms gather and handle personal data and the possibility of data exploitation.
ii. Content regulation: The IT Act gives rise to some restricted authorities concerning content regulation, although these are not clearly outlined or put into practice. This has made it harder to handle new issues like hate speech and disinformation, and it has also created confusion about what material is allowed on e-commerce platforms.
iii. Protection of intellectual property: The protection of intellectual property rights in the internet space is not sufficiently covered by the IT Act. This has made it more difficult for companies to defend their intellectual property rights online and opened up gaps that can be taken advantage of by infringers.
iv. Domain name issues: There is no set procedure for handling these disputes under the IT Act. Due to this, many instances are now being tried in court, which may be expensive and time-consuming.[5]
v. Antitrust: Anti-competitive actions in the e-commerce industry are not specifically addressed by any provisions in the IT Act. This has sparked worries about the possibility of big e-commerce platforms abusing their position of market dominance.

Which are kinds of E commerce fraud and analyse with case study

E commerce fraud is a kind of criminal activity that includes using a computer or the internet to trick or take advantage of someone in order to get money. Cybercriminals employ a range of techniques, including identity theft, ransomware, malware, and phishing campaigns, to perpetrate cyber fraud. Victims of E commerce fraud may suffer greatly on an emotional and financial level. E commerce fraud victims could experience financial loss, credit damage, or even extortion or blackmail.[6]

Following are some of the infamous kinds of E- commerce frauds that people should be aware of:

1. **Classic Online Credit Card Fraud**: This kind of e-commerce fraud is the most prevalent and is usually committed by inexperienced thieves.

[5] Ali.Z. Marossi, Globalization of Law and Electronic Commerce, 'Toward a Consistent International Regulatory Framework' (Delta Fredericton New Brunswick, Canada The Eighth International Conference on Electronic Commerce, August 14-16, 2006).
[6] The Electronic Commerce and Consumer Protection Group ("E-Commerce Group"), See http://www.ecommercegroup.org/guidelines.htm

ISSN: 2582-6433

This kind of attack involves the fraudster obtaining credit card information that has been stolen in one way or another (for example, by buying credit card credentials that have been stolen from the dark web or by breaking into someone's credit card account and taking note of the credentials). The fraudster then uses the credit card credentials that they have obtained to make an online purchase.

The con artist may employ a number of ruses to make sure they can get their hands on the products (such as sending them to re shippers) and may also employ a number of strategies (such as using home proxies) to conceal their identity.[7]

1. **Phishing**: Phishing is a kind of social engineering assault in which a hacker sends a phony text message or email purporting to be from a reputable organization, bank, or government agency. Frequently, an attachment or link in the email or text message can download malware or take the recipient to a phony website when clicked. The victim can be asked to submit sensitive information, such their credit card number or bank account number, after they are on the fraudulent website.

2. **Malware**: it is harmful software that can take data from a computer, harm it, or both. Numerous channels, such as USB devices, compromised websites, and email attachments, can propagate malware.

3. **Ransomware**: Malware that encrypts a victim's data and requests a ransom to unlock it in return for the decryption key is known as ransomware. Attacks using ransomware may be incredibly expensive for both people and companies.[8]

4. **Identity theft**: When a thief takes a person's name, Social Security number, or credit card number and utilizes it to perpetrate fraud or other crimes, it is known as identity theft. For victims of identity theft, there may be severe financial and legal repercussions.

[7] Delamaire, Linda & Abdou, Hussein & Pointon, John. (2009). Credit card fraud and detection techniques: A review. Banks and Bank Systems. 4.
[8] Ramesh, Sai & Ck, Yogesh. (2022). Google Play Malware Detection based on Search Rank Fraud Approach. KSII Transactions on Internet and Information Systems. 16. 3723-3737. 10.3837/tiis.2022.11.014.

ISSN: 2582-6433

KEY FINDINGS AND SUGGESTIONS

HOW TO FIGHT BACK AGAINST E COMMERCE FRAUD?[9]

1. **Maintain PCI Compliance**: The Payment Card Industry Data Security Standard (PCI DDS) is a generally accepted collection of guidelines that make sure businesses, such as e-commerce enterprises, that store and handle credit card and cardholder data do so in a safe manner. Basic security measures, such as putting a firewall between your internet connection and any system that stores credit card details, are the outcome of PCI compliance. In the end, PCI compliance is required, therefore in order to avoid any sanctions or penalties, you must make sure that you are adhering to the applicable PCI requirements.

2. **Be Extra Watchful During the Holidays**: With more people shopping online on Black Friday, Cyber Monday, and other December holidays, the holiday season might be one of the most important times for your company. Additionally, customers are distracted and busy during these hours, and they frequently take less safety precautions.

   The truth is that during these months, a lot of con artists take advantage of merchants who are too busy or distracted to notice possible fraudulent activity. Be especially cautious over the Christmas season if you get a large volume of rush orders, small-dollar sales, or foreign orders. These actions may indicate that con artists are trying out ruses such as card testing fraud.

LEGAL PROVISION

PROVISIONS UNDER IT ACT W.R.T. INFORMATION TECHNOLOGY ACT

India's main statute against e-commerce fraud is the Information Technology Act, 2000 (IT Act). Any conduct that exploits information technology to perpetrate fraud or deceive others is considered e-commerce fraud according to the IT conduct.[10]

[9] Dharmavaram, Vijaya Geeta. (2011). Online identity theft - An Indian perspective. Journal of Financial Crime. 18. 235-246. 10.1108/13590791111147451.
[10] Shaikh, Nihal & Chudasama, Dhaval. (2021). Research on Cyber Offenses under Information Technology Act, 2000. 8. 2021. 10.37591/RTPC.

ISSN: 2582-6433

Some of the specific provisions of the IT Act that deal with e-commerce fraud include:

1. ***Section 43***: This section prohibits the use of information technology to cheat or defraud any person.
2. ***Section 44***: This section prohibits the use of information technology to make false or misleading representations.
3. ***Section 46***: This section prohibits the use of information technology to commit forgery.
4. ***Section 66C***: This section prohibits the use of information technology to commit identity theft.
5. ***Section 66D***: This section prohibits the use of information technology to commit cheating by impersonation.

Additionally, the IT Act stipulates penalties for e-commerce fraudsters. E-commerce fraud carries a maximum sentence of three years in jail and a maximum fine of Rs. five lakhs.

There are other Indian statutes that can be utilized to punish e-commerce fraud in addition to the IT Act. The Trademark Act, the Consumer Protection Act, and the Indian Penal Code are some of these laws.

CONCLUSION

In the field of e-commerce law, cyber fraud regulation is a complicated matter, but it is one that must be addressed to safeguard customers and companies. To provide a more reliable and safer environment for online transactions, a new legislative framework addressing the critical areas of consumer protection, data protection, cybersecurity, and payment security is required.

Adopting stricter legal safeguards for protecting sensitive data, information, and intellectual property online becomes essential as technology develops and leads to breakthroughs. The advent of innovative cybercrimes directed at intellectual property necessitates the creation of new rules that go beyond conventional prohibitions. This is due to the fact that the current legal system is unable to handle the particular difficulties involved in identifying and apprehending those who violate intellectual property in the online realm. The Information Technology Act now governs the e-commerce industry in India, with specific legislation pertaining to the protection of intellectual property. Legal professionals are essential in ensuring that e-commerce businesses

ISSN: 2582-6433

operate in accordance with current laws by striking a balance between the potential of technology and realistic regulatory constraints.[11]

To prevent e-commerce fraud, the Indian government has also implemented a variety of measures. Among these stages are:
Creating a National Cyber Crime Reporting Portal: Victims of cybercrime can report offenses online using the National Cyber Crime Reporting Portal.

Giving law enforcement agencies cybercrime training: The Indian government has given law enforcement agencies cybercrime investigation and prosecution training.

Developing self-regulatory mechanisms in collaboration with industry stakeholders: To stop and identify e-commerce fraud, the Indian government is collaborating with industry stakeholders to establish self-regulatory systems.

In order to combat the problem of cyber fraud in the e-commerce industry, the Indian government has established the National Cyber Crime Reporting Portal and trained law enforcement organizations on how to investigate and prosecute cybercrimes. To create a thorough and efficient regulatory framework for e-commerce legislation, further effort must be done.

However, there are issues with taxation, data privacy, consumer rights, and cross-border trade when there is no explicit legislation in place. The Indian government, business leaders, attorneys, and other interested parties must work together to resolve these problems. Adequate legal framework creation necessitates a thorough e-commerce policy that promotes sustainability and inclusion. A strong regulatory framework that protects consumer rights, promotes domestic and global trade, and creates an open and predictable business climate for investors and entrepreneurs should be in place to support this approach. India can fully realize the promise of e-commerce as a major accelerator for economic growth and development by fostering an enabling environment.

[11] Krishna Prasad, Smitha, (Draft) Paper on Information Technology Act, 2000 and the Data Protection Rules (December 30, 2017). Available at SSRN: https://ssrn.com/abstract=3094792 or http://dx.doi.org/10.2139/ssrn.3094792

ISSN: 2582-6433

REFERENCES

i. India: e-commerce market size 2030 Published by A. Minhas & 16 https://www.statista.com/statistics/792047/india-e-commerce-market-size/

ii. Indian e commerce law under Cyberlaw (IT act). King Stubb & Kasiva. (2022, July 13). https://ksandk.com/regulatory/indian-e-commerce law-under-cyber-law/