Issues and challenges in the investigation of the Cyber offences of Electronic Fund Transfer in India: An analytical study

MAMTA SANJAY KARKAR
Research Scholar
Raksha Shakti University (now Rashtriya Raksha University)
Lavad, Gandhinagar

1. Introduction

The growth and development of the Internet and electronic devices has shaped a new virtual world which run on the tip of the fingers. Those days are now forgotten when the bank customers have to make a long queue in the banks waiting for their token number to come and make transactions. Now a days one can exercise everything on the mobile with the help of mobile banking, internet banking. The world has shrunk because of cyber space or cyber world. The various new technologies have still banished the limits or borders of physical world. But at the same time the risk of cyber crime has been increased. With the advent of technology, the e-commerce and e-banking sector experienced the cyber treats of financial nature.

Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

In a general sense Cyber crimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading, e-governance, e-documentation has led to a phenomenal burst in incidents of cyber crime.

Information Technology (Amendment) Act, 2008 (ITAA) –

Information Technology Act 2000 was the first legislation in India on technology, computers and e-commerce, e-communications. There were numerous controversies and extensive criticism on the effectiveness of the Act.

National Policy of Information Technology, 2012

Union Cabinet had approved the National Policy on Information Technology 2012 on the date 12th of September 2012. The National Policy on IT focuses on application of technology enabled approaches to overcome monumental developmental challenges in education, health, skill, development, financial inclusion, employment, generation etc to enhance efficiency across the board in the economy.

The Banker's Book Evidence Act, 1891 ('BBE')

Prior to IT Act, it was a provision that a bank was supposed to produce the original ledger or other physical register or document during evidence before a Court. This is changed now and the BBE recognizes the printout from a computer system and other electronic document as a valid document during course of evidence subject certain compliance of procedure.

Reserve Bank of India Act, 1934

The Reserve Bank of India Act 1934 was amended in 1934. in Section 58 of the Reserve Bank of India Act, Sub-section (2), after clause (p), a clause relating to the regulation of funds transfer through

electronic means between banks i.e. transactions like Real Time Gross Settlement (RTGS) system which facilitates online transfer of high-value funds between bank customers of different banks on real-time basis, National Electronic Funds Transfer (NEFT), and other fund transfers was inserted to facilitate such electronic funds Transfer and ensure legal admissibility of documents and records therein.

The Indian Penal Code, 1860

The Indian Penal Code, 1860 (IPC) is the enactment which provides for the procedure to be followed in a criminal trial. IPC was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records or false documents. The Indian Evidence Act, 1872

After the enactment of Information Technology Act 2000, the electronic records and documents are recognized as evidences. The Indian Evidence Act 1872 provides for the law dealing with evidence to be provided in a legal proceeding.

Investigation in cyber offences of Electronic Fund Transfer in India

The meaning of Electronic Fund Transfer refers to use of computers and telecommunication technology for making the money transactions inter banking or intra banking. In Indian banking sector, the Electronic Banking was evolved with the help of Shere Committee recommendations, Rangrajan Committee reports for computerization of banks and other valuable suggestions from the experts.
The following are the cases registered under IT Act

- Tampering of electronic documents – sec. 65 of IT Act
- Loss or damage to computer utility or resource – sec 66(1)
- Hacking – sec. 66(2)
- Electronic obscenity – sec. 67
- Failures of order of certifying authority – sec. 68
- Unauthorized access to computer system – sec. 70
- Misrepresentation – sec. 71
- Fake digital signature publishing – sec. 73
- Fake digital signature – sec. 74

Major hurdles in the investigation of cyber offences of EFT

The Jurisdictional limits are becoming the hurdles in the implementation of cyber laws and conviction of the cyber criminals because concept of cyber space is like Universe and had no boundaries. The cyber crimes not mere physical offences but by and large they are the product of criminal psychology, criminal behavior and can not be strict subject of local law of the land. With rapid evolution of IT space, keeping pace with the emanating threats and consequent legislative response in India lacks may vital links.

Though Indian cyber law has provisions to counter cyber offences related to electronic fund transfer, the ratio of conviction is less and compensation to the victim is still uncertain. On the latest background of currency demonetization, and demand of online payment transaction, with rapid evolution in technology, the law should reflect the same to keep pace with the trend.

2. Techniques of cybercrime investigation commonly adopted

Searching the culprit
Tracking IP address
Analysis of webserver logs
Tracking of email account
Trying to recover deleted evidences

Trying to crack the password
Trying to find out hidden data

A computer forensic investigator should follow some of the investigation methodologies in order to find out the truth. One should gather the evidences without affecting the chain of custody of the evidences. Once the evidence is gathered, maintaining the original data safely and working on the duplicate data is included. It is important that Data integrity should be maintained by the forensic investigator. Forensic investigator has to follow the various steps in investigating the cyber forensic cases like - legal opinion the company should call for a legal advisor, preparing the First Response of Procedures (FRP), the evidence from the crime scene is gathered by forensic investigator and it is afterwards taken to the forensic lab. The collected evidences are prepared as bit stream images and it is converted to MD hashing algorithm. Before concluding the investigation, the forensic investigator should examine the evidences and finally he should prepare the investigation report etc.

3. Research Problem

The Title of the paper is 'Issues and challenges in the investigation of the Cyber offences of Electronic Fund Transfer in India: An analytical study'. The Researcher has focused on the various new challenges that has arisen in the investigation methods of cybercrime in India in the light of various techniques of cyber forensic used in the investigation procedure, the new modus operandi of the cyber offences of the Electronic Fund Transfer adopted by the cyber criminals, and rapidly changing Information Technology. The main aim is to find out the efficiency of Indian cyber legislations to implementation of the investigation of cyber crimes.

4. Research Objectives

- To discuss about the effective investigation of cybercrimes in India
- To focus on the importance of the modern-day technology in crime investigation
- To identify the issues and challenges in the procedure of investigation in cyber crimes
- To identify the difficulties in investigations of such complaints on the grounds of jurisdiction and judicial officers to deal with cases of cyber offences in e-commerce.

5. Research Methodology

Researcher had used the secondary data for illustrating the research paper to clarify certain cybercrimes and issues related to the Investigation and cyber forensic with various legal implications.

6. Issues and Challenges

Law enforcement investigators in India are not computer literate. It is needed to understand the basics of IP addressing in order to trace users of the Internet to a physical location. IP addresses provide a connection point through which communication can occur between two computers. Investigators must be familiar with how these various systems work and how one might be able to retrieve critical case information from stored communications or fragments of previous exchanges.

Our criminal laws are still based on old policies, investigators must be aware of the different types of digital media that exist and be able to identify the media in the field. The variety, and more importantly the size, of media must be taken into consideration when applying for search warrants where digital evidence is suspected; the hiding places for this type of storage are countless.

7. Major findings

The study pointed that the cybercrime handling requires an appropriate legal framework and technical infrastructure to analyse cyber forensics data. It also found that knowledge of cyber forensics tools for capturing evidence from the crime site and network which may vary in the cyberspace is a skillful task and demands special training for the investigators. It is also observed that for investigation of

cybercrime and securing digital evidence, special software and tools are required for the effective cyber forensic. There is need for officers in handling and application of forensic tools and techniques. Wide publicity is needed on a sustained level, regarding modus operandi of cyber fraudsters, especially to alert them against dangers involved in responding to tempting e-mails or SMSs and preserving the electronic evidence in secured condition till the investigation ends.

8. Utility of the Research

This research paper will cater the information of various cybercrimes and legislation in India. Also focusing on such burning issue of the evidence in cybercrime cases in terms of cyber forensic in the era of e-banking, e-commerce and digital India. The study of new challenges emerging in the cyber investigation and cyber forensic will encourage further study for the aspirants in this area of law and technology.

9. Conclusion

As per the present scenario in the implementation of cyber laws, it is found that law enforcement personnel use to understand the criminal mind-set and have knowledge of the evidence bases judicial system, investigation and producing offenders in courts. Whereas the technology persons have knowledge of technology only. Both of the agencies are finding difficulties to defeating the cyber criminals due to lack of other side in their professions. Another aspect of the research question is to locate the reasons for less conviction and low remedial justice to the cyber victimization as well as solutions for the effects of cyber crime on e-commerce and e-governance.

References

1. Sankalp Jain, “Electronic Fund Transfers: A critical study in Indian context with special reference to security and privacy issues”
2. NITI AYOG July 2018
3. R.K. Uppal and N. K. Jha, “Online Banking in India, Anmol Publications, New Delhi, 2008
4. Barkha, Mohan UR. Cyber law and crimes. IT Act 2000 and Computer Crime Analysis. 3rd ed. 2011.
5. Information Technology Act 2000
6. Gupta, AK, Gupta MK. E-governance initiative in cyber law making. International Archive of Applied Sciences and Technology. 2012
7. Cyber Crime Investigation Manual, by Data Security Council of India, 2011