CYBERCRIME EVIDENCE AND ROLE OF INVESTIGATING AGENCIES: DIGITAL EVIDENCE AN APT FRONT FOR INTRODUCTION AND DEVELOPMENT OF COMPUTER FORENSIC SCIENCE IN INDIA.

Sneha Singh*

St. Xavier's University, Kolkata

ABSTRACT

In India, understanding of the term of 'Cyber crime' is restricted to certain kinds of the crime such as tampering with computer source code, hacking and cyber pornography. Despite a specific legislation in the form of Information Technology Act, 2000 provisions of the Criminal Procedure Code are followed in the process of investigation of the cyber crimes as any cognizable case falling within the jurisdiction of the investigating officer. The Investigating officer has the powers to initiate and proceed with the investigation without any judicial order to the same effect. The Information Technology Act, however, does not contain any specific provisions to define or classify the offences and the punishment-either cognizable or non cognizable or bail able or non bail able except for the indicators and provisions under Section 65 to 74 of the Act. But the opinion of the expert for authentication of the evidence is given equal importance and has recently been in vogue. Thus paving way for the development of forensics more specifically computer forensic science, which is a streamlined branch of the general forensic science, in India. This paper is an attempt to analyse the ground for development of computer forensic science in India and it can aid the investigating agencies to deal with the menace of cyber crimes in a more detailed and efficient manner as a prevalence in the developed countries.

KEYWORDS: *Cybercrime, Digital Evidence, Role of Investigating Agencies, Information Technology Act, 2000.*

INTRODUCTION

In India, the legislation specially dealing with the advancements of the information age is the Information Technology Act in the year 2000 (hereinafter also referred to as "IT Act"). This Act was drafted in consonance with the existing procedural laws and deals with the offences by the use of technology and electronics, acceptability of the electronic records, procedure of adjudication etcetera. This legislation was duly amended in the year 2008. The provisions elaborate upon the procedure to deal with the unique features of electronic offences. However, categorically the term '*Cyber Crime*' is not defined under the legislation. The meaning of the term, is thus, deduced as used and understood in common parlance. It is '*any offence or crime wherein technology or computers are used*'. In Cyber crime, computer or the data itself is the ingredient of committing a crime. The offence is committed by the use of gadgets, tools and technology like Computer, mobile networks, etc. Nevertheless, Computer[1] in this context is a species whereas technology is a genre. The use of technology may differ in extent and the list of crimes may be elaborated and classified.

Law enforcers or Investigating agencies are the police officials and the act specifies that the Investigating Officers in such cases cannot be an official below the rank of Sub Inspector in the Police. But not

*Research Scholar, West Bengal National University of Juridical Sciences, Kolkata and Research Assistant, Centre of Regulatory Studies, Governance and Public Policy, WBNUJS.

[1] The Information Technology Act, 2002 defines Computer, computer network, data, information and the other ingredients to the concept of cyber crime. Computer resource is defined in clause k of sub section (1)

every police official involved in the process of investigation of cyber crimes is acquainted with the nuances and technical details of the evidences of cyber crime. This paper will analyse as to what are the essential features of the evidence in cyber crimes and the need of Forensic expertise to decode and explain the content. The role of the Investigating agencies in the context of cyber crimes will be studied to understand the limitation of the enforcer of law to ensure that the offences are tried efficiently without due indulgence of the computer forensic sciences expert and the need to resort to professional expertise to understand the logistics of the crime and given the uniqueness of the nature of digital evidence. Thus the paper concludes as to how with the increase in the number of cyber crimes, scope of forensic criminology, especially computer forensic sciences in India has increased and the investigating agencies have an added responsibility to prove beyond reasonable doubt through reports of the experts the authenticity of the evidences in electronic forms.

UNIQUE FEATURES OF DIGITAL EVIDENCE:

With the reliance on digital technology, critical infrastructure's dependence on the networked communications has increased. Digital evidence is progressive and cyber crimes, like any other crime, are best judged by the nature of the evidence produced before the courts of law. Additionally, it requires proof of authenticity and reports of the expert[2]. In India, courts have taken a pragmatic overview by recognizing digital evidence[3]. They have in instances appreciated the evidence and rendered admissibility despite the deviation from the grund norm- admission of oral or documentary evidence. This helps the country keep up with its counterparts globally and progress. Indian Evidence Act, 1872 governed the principles of evidence. The procedural law has evolved over the years acknowledging the developments and adapting the nuances as and when required. There have been changes in the Evidence Act as well to introduce the admissibility of electronic records over and above the paper based documents. Post amendment, Evidence as defined under the Act includes electronic records[4]. Oral admissions of the contents of the electronic records are not relevant unless the genuineness of the electronic records produced in question is proved[5]. When a piece of evidence in the form of statement is part of a longer piece of conversation or a document or series of letters or papers, the relevant portion should only be considered depending on the facts and circumstances of the case[6]. Similarly, when the electronic evidence in a particular instance is a series of computer codes, recordings or data, the relevant portion should be considered and deliberated upon[7]. The need of authentication and certification of that particular content is only needed. The IT act provides for the provisions of authentication and certification of the content of the electronic evidence in the offences specified from section 64 to 74 of the Act.

The collection of evidence in such crimes of computer networks and extensive webbed infrastructure is tedious process. The relevancy of the Indian Evidence Act, 1872 was proved beyond reasonable doubt by The Information Technology Act, 2000. The kind of evidence in cyber crimes are mostly '*electronic records*'. The Evidence Act was modified as per the provisions of the IT Act and introduction of the relevant provisions. Expressions in the electronic form can be on the screen of the monitor, hard disk, floppy or CD. Electronic numbers are used to process the data. Data evidence cannot be rejected if it is inconsistent with the oral evidence

[2] Expert as in professionals who can expressly decode the data contained in the electronic form to the simplest form of understanding the criminality content and certify the nature and genuineness of the data. In the developed countries, it is a common practice to send any evidence to the team of professionals and obtaining a report from the experts testifying the veracity and content of such evidence.

[3] In *State of Maharashtra versus Dr. Praful B Desai* (2003) 4 SCC 601 the apex court has on examination of witness by video conference advancement of science and technology should be recognised and appreciated. In this particular case the presence of the witness in person was waived off with the video conferencing opportunity. This decision of the Supreme Court was subsequently followed by the High Courts. Also see *Amitabh Bagchi* versus *Ena Bagchi* AIR 2005 Cal 11 and *Bodala Murali Krishna* versus *Bodala Prathima* 2007 (2) ALD 72.

[4] Section 3 (a) Indian Evidence Act, 1872. Electronic records means 'data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generate micro fische'.

[5] Section 17 of the Indian Evidence Act deals with admissibility of electronic records as evidence and Section 22 A of the Indian Evidence Act specifically deals with the admissibility of the electronic evidence.

[6] Section 39 of the Indian Evidence Act, 1872. In *National Textile Workers Union* versus *PR Ramakrishnan* AIR SC 1983 at 75 the conventional means were considered to be obsolete and the need to accept the records in the changing nature with the society was considered important and necessary.

[7] The Court observed in *State* versus *Mohd Afzal* (2003) DLT 385 at 278 that records and data processing have become outdated and admissibility of electronic evidence in Indian Laws is accepted.

but opinion evidence is only an inference drawn from the data and does not have precedence over direct eye witness testimony. However, expert opinion is accepted and once accepted it becomes the opinion of the court.

The Information Technology Act, 2000 amends the provisions related to digital evidence and its admissibility in the courts of law[8]. Section 65A and 65B were inserted in the existing act of procedural law as per the Second schedule of the IT Act. A new provision was introduced to the Indian Evidence Act (section 65A) providing for procedure that the contents of electronic records may be proved in accordance with the provisions of section 65B. As per section 64(B) (2) of the Evidence Act there are certain conditions which must be fulfilled prior to admission of a computer output as evidence. These conditions are – activities carried out from a computer over a period of time and the person having lawful control over the use of the computer; information contained is derived as regularly fed in the computer; combination of computers operating over that period of time and different computers operating in succession over that period of time and so described in the provisions.

With the increase in the retail and the technological advancement, cyber crime has seen phenomenal increase at a steady pace. The IT act also deals with the issues of legal recognition of electronic documents, digital signatures, offences and contraventions of the provisions of the act in the process of finding alternatives to the paper based methods of communication and storage of information. The need for special legislation was the advent of globalisation and the technological development of the nation. And since then there has been no looking back, instead the country has understood the need for integration of the principles of evidence used in developed countries like US to deal with the complicated and hybrid nature of cyber crimes.

INVESTIGATING AGENCIES AND DIGITAL EVIDENCE:

Electronic evidences decide conviction and prosecution in a case of cyber crime[9]. Transmission of data or any kind of computer source code is considered of relevance and admitted in the courts as evidence[10]. Data theft and misuse of information are some of the major forms of cyber crimes listed as per the act without defining as to what would constitute cyber crime.

According to the statute, tampering with the source documents either by concealing, destroying, altering any computer source code is an offence punishable[11]. Some of the crimes as per this section are fabrication of electronic record or commission of forgery[12] by changing or managing the contents of the compact disk produced as evidence in the court or doing any kind of mischief with the computer source code[13] to distract or mislead the investigating agencies. The material being refined and sophisticated cannot be interpreted or understood by an investigator with nominal or no knowledge of technology. Appointment as an investigating officer in a case of cyber crime, the Central government has no directive to ensure and consider for appointment only officials who have expertise of some kind in dealing with the complex nature of electronic evidences. Any officer not below the rank of a Sub Inspector is empowered to investigate and be the Investigating Officer of a particular case. For special provisions like under Section 80 of the Act[14] (power to arrest from any public place without warrant), a police officer has to be not below the rank of Deputy

[8] The IT Act is based on the UNCITRAL model of Law on Electronic Commerce and, apart from providing amendments to Indian Evidence Act, 1872 (Evidence Act), the Indian Penal Code, 1860 and the Banker's Book Evidence Act, 1891, mainly recognizes transactions that are carried out by means of electronic data interchange and other means of electronic communications.

[9] Stephen Mason, et.al., *Electronic Evidence: Disclosure, Discovery and Admissibility*, (First Edition, Lexis Nexis, 2007).

[10] Real evidence is any material evidence but it is not available relating to the digital transactions so the alternative for the Indian courts is admissibility of the digital evidence. The parameters for admissibility are as per Section 60, 64 and 91 of the Indian Evidence Act, 1872.

[11] Punishment is three years imprisonment or two lakhs or both.

[12] *Bhim Sen Garg* vs *State of Rajasthan and others*, 2006, Cri LJ, 3463, Raj 2411

[13] Computer source code under this Section refers to the listing of programmes, computer commands, design and layout etc in any form.

[14] Under Section 80 of the Act, the police officer was empowered to enter, search a public place and arrest without warrant a person for offences defined and punishable under the IT Act, 2000. Certain features of the cyber crimes does not, however, allow immediate arrest and the provision can be avoided in almost 99% of cases.

Superintendent of Police (DSP)[15]. The police as enforcers of Law and the investigating agency have to, in the process of investigation, monitor, intercept, encrypt and decode data. They have to find out the instruments used in the process of transmission or receipt of criminal content or any content which would constitute or have the ingredients of crime of a particular nature under the Law.

Being a very recently drafted and rarely applied legislation, the IT act picked pace only with the increase in the concern of the governments of the State. The increase in the use of technology for commission of crimes and lack of expertise to tackle the menace was the prime cause of action. Special Cyber crime police stations were established and technological training was departed to the officials. However, at present adjudication or investigation of offences with such applications are concentrated in the major metros or industrialised states.

Initially, the role of the investigators was primarily to rely on the tested and tried methods under the Indian Penal Code (which in itself is one and half century old) even in the technology based and oriented cases with unique facts and circumstances. Huge amount of money was proportionately spent and invested in the nation to sternly take on cyber criminals and creation of a protective technology to safeguard the interests of the vulnerable as the systems used by these criminals to commit such offences are critically designed and the information infrastructure is based on technological developments and expert finesse.

The investigating agencies handle the data. The information, collected in the process of investigation, is stored as evidence for the use of the courts of law in the process of adjudication. The evidences in cyber crime be like hardware of the machine used to commit the crime, software, data bases etc. In India, usually the evidence collected in cyber crimes is stored in the police *malkhana* room under the risk of exposure to moisture and too much light. It is only after the investigating officers' diligence, a part of the evidence is sent to the forensic science laboratory and expert advice is sought.

SCOPE OF DEVELOPMENT OF FORENSIC CRIMINOLOGY:

Crime in the information age has transformed. Any crime related to computers is not the only cyber crime. The scope of cyber crime has increased and local police works within prescribed and well outlined budgetary parameters which creates a restrain to deal with the globalised electronic networks. The knowledge of the local police is also limited to understand the hybrid offences and the nuances of the evidences without the use of expertise. This has increased their dependence on the forensic scientists to ascertain the nature and source of evidence to create the linking loops of the crime- cyber crime. Computer content crimes may not be directly illegal and can be very personal, incite violence, political unrest or prejudicial actions against others. Digital realism has the potentials to adversely affect the investigating procedure. The police can with other groups and in association with the networking agencies increase their public participation. This will extend their symbolic and normative level by reconstitution of fundamentals to understand the nature of the principles at a more practical level[16]. The herculean task is to prove the continuity of evidence in cyber crime cases. Investigating any cyber crime or e-crime, identifying the cyber criminal and locating the weapon of the offence which is not available in most of the cases poses a barrier in the entire process of collection of evidence and subsequent evaluation of the same[17]. With the increase of number of computer users in geometric progression, virtual activities have multiplied and so has the nature of crimes.

With developments in the management of information systems, electronic data interchange systems has extensively developed. It represents the exchange of documents and transactions by a computer in one company with the computer(s) of one or more companies in an open system environment[18]. The developed technology leads to quick generation, transmission and share of information. Such processing of data has raised concerns for the organisations that have to secure their survival as well as be innovative enough in the changing times. Crimes of data related to this information require expert knowledge of the systems and the features which can ease the coding and decoding of the information. General knowledge of the computer and its applications by the

[15] The power to arrest without warrant under section 80 of the Act raised brows for material period of time in the country.
[16] David S. Wall, *Cyber Crime*, 2007 Polity Press, pp 207 -214
[17] Vivek Sood, *Cyber Law Simplified*, Tata McGraw- Hill Publishing Company Limited, 2001
[18] Alex Wilson, *Internet Laws and Information Technology*, Koros Press Limited, First Edition 2015.

enforcement agencies just gives a smooth entry in the area but the need is for special expertise and then the need of forensic experts is considered important and crucial.

Forensic along with the Judiciary and the Police is an important aspect of justice delivery system to uphold the rights of the innocent people as per Article 21 of the Constitution of India. There are state laboratories established by the government of India. The main functions of the laboratory are: to visit the scene of crimes and aid the investigating officers in the detection and collection of evidence, reconstruction of crime scenes and provide examination reports of the evidence; scientific examination of the exhibits/samples received at the laboratory for generation of forensic reports; providing scientific evidence in the court of law; providing theoretical and practical training to various ranks of police personnel, excise & narcotics department, Judicial officers, medical and other law enforcing agencies with aspect of scientific method of investigation. In cyber crimes and the evidences collected therein, the role of the forensics is exemplified in handwriting examination and identification to establish the authenticity of the document or any part thereof to ascertain the genuineness of important documents such as stamps, documents and security papers. The major section is the photography division which deals with identification of the camera from the film negatives, identification of the source camera (important feature for the digital pictures). The forensic scientists are regularly trained and updated with the latest scientific techniques for improved expertise skills. These forensic scientists also conduct theoretical and practical training of the police officers who are involved in the process of investigation and assist them in preserving the evidences without affecting the quality or unknowingly tampering with the with the method of investigation. Thus, with the latest developments and inclusion in the field of technology, forensic sciences have gained its own niche in the administration of justice.

Nevertheless, it will not be incorrect to mention how Computer forensic science is applied in the cases of digital evidence and cyber crimes. This stream of science is different from most of the traditional forensic disciplines[19]. Computer forensics is description of those activities associated with the identification and preservation of computer and electronic evidence in support of some legal or official action. In the process of identification and preservation, analytical and investigative techniques are used. Evidence is examined while the data stored or encoded magnetically is retrieved and simplified by the use of the binary number system. Computer networks are either the target of some illegal activity, medium of commission of such activity or incidental to the commission of such illegal activity. This stream of investigation is more important in terms of preservation of the evidence in its original form so as to avoid modifications changing the nature of the evidence and at the same time the time stamps can be avoided[20].

There are four steps in the entire computer forensic investigation- acquisition (post identification of the evidences), evaluation and presentation. The first two steps are repeated until the investigation is complete. The challenges in preventing cybercrime are fundamental and have its own threats and issues of management. To investigate in such cases, the investigating agencies have to consider and apply the Intrusion Triangle of Crime. This theory can be used to understand the motive, means and opportunity of the criminals involved. The investigation has to be technically sound and detailed considering the organizational vulnerabilities. The investigator is expected to understand the complex issues relating to personal computer user safety and security. The security can be of the hardware or the software. Crimes can be in the form of free credit reports, scams, free prizes, pyramid schemes[21], chain to letters, charities, offer to work-at-home, job advertisements, check cashing, credit information requests, scam baiting[22] and scam resources.

This is the advanced methodology and scientific procedure of tracking the footprints of the criminals who are widely based and established all around the globe. The limited knowledge of the investigating agencies in the technical know-how of the subject allows the filed for successful mushrooming of the content of computer forensic sciences in the country. The technical knowledge is highly needed and recognised as an essential requirement for the apt investigation in the cases of crimes wherein the computer and the technological advancements are misused or tweaked to create a menace.

---

[19] Forensics is the study or practice relating to legal proceedings or augmentation whereas the Computer forensics has picked pace with the technological revolution which provided enormous opportunity for illegal activities.

[20] Robert C. Newman, *Computer Forensics Evidence Collection and Management*, (Anerbach Publications, 20070

[21] A pyramid scheme is fraudulent scheme in which people are recruited to make payments to the person who recruited them while expecting to receive payments from the persons they recruit.

[22] Scam baiting is a practice of eliciting attention from the perpetrator of a scam by feigning interest in whatever bogus deal is offered.

CONCLUSION:

Crime as a social phenomenon adversely affects the society and the economy as a whole. The origin of crime can be traced to the time of origin of humans. The most recently recognised category being cyber crimes. Cyber Crime multiplies and increases proportionately with the socio-economic development and growth of a country. Widespread use of Internet and digitisation of basic economic activities has made the dependence of human on technology inevitable. In fact, technological failure or unavailability leads to perturbed processes which would have been otherwise irrelevant or usual. For instance, even grocery shops have their customer avail services related to technology such as the card swipe machine and the availability of the technological gadgets decides the popularity and sales of the shop wherein otherwise cash was the primary mode of payment for goods. A day without the use of technology is unimaginable and practically not possible. Digitisation is popular mode of shaping the overall growth of the economy. Every system has its own weaknesses. Exploiting such weaknesses and then social engineering the contents for one's own good i.e. by taking advantage of computer and human limitations bypassing passwords and protections in the form of authentications are some of the common areas of attack and concern for the cyber systems. Cyber crimes are on rise and the main victims are the vulnerable classes such as women, children and the marginalised sections. The vulnerable classes due to lack of exposure and education become easy preys to vicious circle of the crimes. The criminals are uniquely talented to manipulate the contents on the computer networks for their illegal and ulterior motives damaging the equilibrium of the society and creating an imbalance, by misusing an otherwise useful invention and creation of human kind- computer technology and increased infrastructure for enhanced information amongst classes.

Evidence in Cyber crimes are different in nature to those available at the crime scene or created by recreating the incident of crimes. Computer codes, stored information, binary calculation and like requires professional expertise to understand the nature and the extent to which the offence of cyber crime was committed. For instance, in a cyber cafe, Mr. A while using a computer with the code 003 commits the offence of cyber pornography. After Mr. A exists at 2.50pm the same computer is used by Ms. Y for important work at 3.05pm. To consider whether or not any offence as per the Act has been committed, the relevant evidence is the Computer 003 and the server details can only reveal as to who has committed the crime and at what point of time of the day to ascertain the actual criminal activity. The Information Technology Act, 2000 has been the recent step forward by the country to recognise and deal with the nuisances created by the criminal minded by the use of technology. The country has a number of legislations and the procedurally outlined system through adjective laws and the judgements of the courts of law has created its own niche to deal with the range of cases and cyber crimes. But the investigating agencies are not specially trained to deal with the uniqueness of the digital evidence. The dependence of the investigating agencies on the computer forensic sciences expert has increased and so has the reliance on the expert opinion by the courts. The infrastructure in the country in the forensics being limited has also picked up pace with the increase in the awareness of the investigating agencies to track the criminals in cyber crimes. Thus, front for introduction of computer forensic sciences in the country have increased with the increased awareness of the laws followed across the globe and the influence being derived from the countries under the civil law (European Union) who have successfully followed the expertise knowledge to maintain a healthy equilibrium between the investigating agencies and the development of the information technology in the country.

REFERENCES:

BOOKS:

1. Alex Wilson, *Internet Laws and Information Technology*, Koros Press Limited, First Edition 2015.
2. David S. Wall, *Cyber Crime*, 2007 Polity Press, pp 207 -214
3. Robert C. Newman, *Computer Forensics Evidence Collection and Management*, (Anerbach Publications, 20070
4. Stephen Mason, et.al., *Electronic Evidence: Disclosure, Discovery and Admissibility*, (First Edition, Lexis Nexis, 2007).
5. Vivek Sood, *Cyber Law Simplified*, Tata McGraw- Hill Publishing Company Limited, 2001

LEGISLATIONS:

1. Banker's Book Evidence Act, 1891
2. Indian Evidence Act, 1872
3. Indian Penal Code, 1860

4. Information Technology Act, 2002

CASES REFERRED:

1. Amitabh Bagchi versus Ena Bagchi AIR 2005 Cal 11
2. Bhim Sen Garg versus State of Rajasthan and others, 2006, Cri LJ, 3463, Raj 2411
3. Bodala Murali Krishna versus Bodala Prathima 2007 (2) ALD 72.
4. National Textile Workers Union versus PR Ramakrishnan AIR SC 1983 at 75
5. State versus Mohd Afzal (2003) DLT 385 at 278
6. State of Maharashtra versus Dr. Praful B Desai (2003) 4 SCC 601