International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

"Cyber Policing: Evidentiary Value of Electronic Records"

Shafiq Mushtaq Lone*
Mufti Nahida**

1. Introduction

The use of internet has become the part and parcel of every educated person in this world. It has opened the gates to the information superhighway connecting the rest of the world to whole a lot of information and to all corners of the world at once. It connects the person sitting in the remote corner of the home or office to the entire world thorough the information highway called passionately web, cyber, etc. It connects everyone to his office, bank, electricity dept., water works, travel service, bazaar, bookshop, friend in other country and also dangerously and unknowingly to cyber criminals waiting to hit the gullible internet user. So comes to web of national and international laws with its enforcing agencies and intelligence to curb this menace of cyber-crimes and protect the society from high-end, sophisticated, high-tech criminals. The effectiveness of the implementation of the cyber laws in India is an utmost important to protect our society new generation of crimes and criminals and whether it has been successful in India or not.

Success in any field of human activity leads to crime that needs mechanisms to control it. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe[1].

Until recently, many information technology (IT) professionals lacked awareness of an interest in the cyber-crime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws

*Research Scholar at Faculty of Law , Jamia Millia Islamia, New Delhi
**Research Scholar at Faculty of Law , Jamia Millia Islamia, New Delhi
[1]GarimaTiwari, *Understanding Laws:Cyber Laws & Cyber Crimes*(LexisNexis, Haryana,1st edn.,2014).

hadn't quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust— between the two most important players in any effective fight against cybercrime: law enforcement agencies and computer professionals. Yet close cooperation between the two is crucial if we are to control the cyber-crime problem and make the Internet a safe "place" for its user.

Cyber-crime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, United Nations has defined cyber-crime[2]:

A. Cyber-crime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

B. Cyber-crime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another. There are more concrete examples, including

- Unauthorized access.
- Damage to computer data or programs.
- Computer sabotage.
- Unauthorized interception of communications.
- Computer espionage.

[2] Harish Chander, *Cyber Laws and IT Protection*,(PHI Learning Private Limited, Delhi, 4th edn., 2016).

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

These definitions, although not completely definitive, do give us a good starting point—one that has some international recognition and agreement—for determining just what we mean by the term cybercrime.

2. Cyber Crimes and Law Enforcement Agencies in India

There are some parameters to study and investigate the implementation of cyber laws in India, i.e., identification, investigation, prosecution, punishment and prevention of cyber-crimes by the enforcement authorities which include special police force properly trained to handle such sophisticated crimes passionately called as *cyber police* (supported by technical wing for the identification and detection of cyber-crimes) and the Indian law courts with specially trained judicial authorities trained in the technicalities of internet crimes. The Law enforcement agencies would include all these things the police and judicial authorities - the level of awareness of cyber-crimes, their abilities (level) to identify the crimes, their knowledge level to understand the technicalities of the subject and process of crime and damage it has and it might in future cause and technical ability level to take up proper steps to stop the further damages to general public. The enforcement personnel's social concern and ability to involve other stake holders from society like internet cafes, internet providers, education and other institutions (where in particular internet suave youths use the facility extensively for their official as well as past time) and national and international website launchers and maintaining super computer based web companies in the process of judicial administration and prevention of cyber-crimes in India[3].

In the present global situation where cyber control mechanisms are important we need to push cyber laws. Cyber-crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. In India, there are 30 million policemen to train apart from 12,000 strong Judiciary. Police in India are trying to become cybercrime savvy and hiring people who are trained in the area.

2.1.How to report a cyber- crime?

[3] P. K. Vineetha,"Managing cyber-crimes in India – issues and challenges" 1 *JEMS* (2012).

A victim of the cyber-crime can lodge a criminal complaint with the local police or he can give information to the various cyber-cells across the India. The FIR would be an official request to the police to investigate the cyber-crime. It should be noted that victim can directly file a complaint before the adjudicating officer[4] , Ministry of Information Technology, Government of India. On making such a complaint, the cyber police may take the following steps[5]:

1. Take a report of the crime; identify the offence(s) under state legislation.
2. Compile a relevant victim and witness statement.
3. Take copies of relevant documents.
4. Consider capturing electronic evidence.
5. Conduct any relevant checks relating to suspect information and include an investigating file.
6. Compile a cover sheet detailing the investigation conducted and requesting the further investigation.
7. Transfer the file to the appropriate agency with jurisdiction relating to the suspect.

3. Regulatory Authorities: under Information Technology Act2000.

There are various regulatory authorities to deal with the cyber-crime and cyber criminals, however the cyber police is the most important of all. The authorities are

A. Local police stations.

If any cyber-crime has taken place and any person(s) is aggrieved from it, he can file the complaint regarding such cyber-crime in the local police station having jurisdiction over the area and the local police are authorized to investigate the same as per the provisions of Code of Criminal Procedure read with Information Technology Act.

B. Cyber Crime Cell

[4] The Information Technology Act, 2000 (Act 21 of 2000), s. 46.
[5] *Supra* note 1 at 1.

Cyber Crime Cell is a wing of law enforcement agencies established to expedite the investigation of cyber-crimes. It is not a police station where one can go and register a complaint. In India Bangalore is the only Cyber Crime Police station where one can register a complaint and can get a copy of the FIR. Some of the duties of the Cyber Crime Cell are:

- To assist law enforcement agencies in investigating cyber-crimes.
- To spread awareness about cyber-crimes and preventive measures in its territory.
- To act as an expert in giving opinions on cyber-crime related issues.

As per Section 78[6] of the IT Act, notwithstanding anything contained in the code of Criminal Procedure, a police officer not below the rank of an Inspector shall investigate an offence under this Act. Such powers were conferred to officer not below the rank of a Deputy Superintendent of Police earlier in the IT Act which was later amended as Inspector in ITAA.

C. Adjudicating Officer

The AO is appointed under section 46[7] of the IT Act to adjudicate offences under chapter IX and it has been declared that the Secretary of Department of Information Technology of every state and the Union Territory shall serve as Adjudicating Officer.

Section 46 of the IT Act, provides that any person aggrieved of cyber-crime can file complaint directly to the AO and the AO shall conduct an inquiry, after giving a reasonable opportunity of representation and if satisfied that there is a contravention of the Act, the AO may impose such penalty or award such compensation as he thinks fit in accordance with the law.

D. Indian Computer Emergency Response Team (CERT-In)

It is the National Incident Response Centre for major computer security incidents in Indian cyber community. Critical Information Infrastructure and Protected system has been discussed in section 70 of IT Act. CERT-In coming under the Ministry of Information and Technology,

[6] The Information Technology Amendment Act , 2008.
[7] The Information Technology Act, 2000 (Act 21 of 2000) , s. 46.

Government of India, has been designated as the National Nodal Agency for incident response under section 70(B) of the ITAA.

Section-70 B[8]: Indian Computer Emergency Response Team to serve as national agency for incident response

1. The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.

2. The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.

3. The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

4. The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-

(a) Collection, analysis and dissemination of information on cyber incidents

(b) Forecast and alerts of cyber security incidents

(c) Emergency measures for handling cyber security incidents

(d) Coordination of cyber incidents response activities

(e) Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

(f) Such other functions relating to cyber security as may be prescribed

5. The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

[8]The Information Technology Amendment Act, 2008.

6. For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person

7. Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

8. No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1). It also monitors web-traffic and intercepts and blocks the sites, whenever so required with due process of law.

E. National Technical Research Organization (NTRO)

It is also designated as the national nodal agency in respect of Critical Information Infrastructure Protection under section 70A of the ITAA.

Section 70A National nodal agency[9]:

1. The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.
2. The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.
3. The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

4. Investigation and Forensics

[9]The Information Technology Amendment Act , 2008.

In cyber-crime cases, the investigator's challenge is to establish the crime beyond reasonable doubt using digital evidence that exist in cyber space. This requires Computer or Cyber Forensics special skills, equipment, laboratory and capabilities far different from conventional crime detection. Computer forensics is extremely important to track and establish proof in all computer related offences. The computer forensic field has developed techniques to improve the detection, connection, and classification of digital information. Thus, the field includes a multitude of systems to extract useful information from computer media and involves the application of varied tools. The stages in computer forensic investigation are usually as follows[10]:

- Identifying the doer of the crime i.e., the one who has committed the crime.
- Locating the means and equipment through which the crime was committed.
- Collection and extraction of the physical evidence.
- Correlating the evidence to the crime and facilitating the arrest of the wrong-doer.

5. Evidence in Cyber Crimes: Challenges and Implications

It is difficult for the police officer investigating a cyber-crime to discover and collect evidences of crimes committed against, or by means of them. It is just because the culprit can easily delete a file in a computer and thereby make the data not available to any investigator for evidence. Unlike other crimes of real world, there may not be any tangible evidence available such as weapon, paper, records, etc. The science of computer forensic, however, is developing fast to tackle with the situation, the challenges and implications involved in the collection and presentation of evidences.

5.1. Search, Seizure and Collection of Evidence

[10]MohitGoyal, "Ethics and Cyber Crime in India" 2 *IJEMR* 1-3 (2012).

The investigator must ensure that the evidences are collected through search and seizure of hardware or through information discovery of logical evidence in a lawful manner. It is important to know that the validity of any evidence in the court of law depends on the legality of the method through which it is collected. A criminal based on illegal search and seizure may be declared illegal in the eye of law. It is, therefore, necessary for the investigator that necessary procedures are followed before proceeding to actual collection. For example, the related provisions of India Evidence Act and Criminal Procedure Code should be followed while making search, seizure and collection of evidences in India.

It is also important to note that according to section 293 of Criminal Procedure Code, reports of certain government service experts can be seed in evidence without formal proof in any inquiry, trial or other proceeding under the code. But if such report has been signed by an officer not within the ambit and scope of section 239 Cr.P.C. then the report could not be read in evidence unless signatory of the report was examined to prove it[11]. Furthermore, one of the formalities required to be observed when making a search is that the searching officer should give his personal search to the witness before entering the premises to be searched and should similarly search witnesses also in the presence of one another[12].

Section 80 of Indian Information Technology Amendment Act, 2008 contains provisions concerning power of police officer and other officers to enter, search etc., which reads as follows:

Section 80, Power of Police Officer and other Officer to enter, search etc.:

1. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of it Inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is

[11] *State of H.P. v.Chareton*, 2001 (1) Crimes 50.
[12] *State of Bihar v. KapilDeo Singh*, AIR 1962 SC 53.

reasonably suspected of having committed or of committing or of being about to commit any offence under the Act.

Explanation: For the purpose of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

2. Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer in-charge of police station.
3. The provisions of the Code of Criminal Procedure, 1973shall, subject to the provisions of this section, apply so far as may be, in relation to any entry, search or arrest, made under this section.

5.2. Forensic Examination of Evidence

For any computer data to be accepted as admissible evidence there may be forensic examination of such data. All the forensic examinations of discovered files must be carried out or backed up copies. These backups should be implemented in a raw, uncompressed format, creating duplicates which should a copy like their originals. The lab evidence which contains details of discovered relevant information such as name of investigator, current date and time, description of each information must be mentioned on the log. Sometimes authentication by investigator is also necessary to confirm that no alteration of electronic data has been made by anyone. There are certain tools which are needed for computer application. These tools are network sniffer (hardware), portable disk duplicator or duplication software, chain-of-custody documentation hardware, cash management software, etc. Forensic examination of electronic evidence has a very important role to play in the field of cyber-crimes investigation.

5.3.Computer Generated Evidence and their Admissibility

The second and third schedules to the Indian Evidence Act, 1872 and the Banker's Book Evidence Act, 1891, respectively have been amended to make computer generated evidences

admissible in a court of law. The insertion of section 65A and 65B in the second schedule are the most important among the amendments which contain special provisions as to evidence relating to electronic records. These sections are as follows:

Section 65-A[13], Special Provisions as to Evidence Relating to Electronic Record: The contents of electronics record may be proved in accordance with the provisions of section 65 B.

Section 65-B[14], Admissibility of Electronic Records:(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded on copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question shall be admissible in any proceeding, without further proof or production of the original, as evidences of any contents of the original or of any fact stated therein or which direct evidences would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: (a) The computer output containing the information was produced by the computer during the period over which the computer was need regularly to store or process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly feed into the computer in the ordinary course of the said activities;

(c) Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of period, was not such as to affect the electronic record or the accuracy of its contents; and

[13]The Indian Evidence Act, 1872 (Act 1 of 1872),s. 65A.
[14]The Indian Evidence Act, 1872 (Act 1 of 1872),s. 65B.

(d) The information contained in the electronic record reproduces or is derived from such information feed into the computer in the ordinary course of the said activities.

(3) Where over any period, the functions of storing or processing information for the purpose of any activities of any regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computer, whether-

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period, or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purpose of this section as constituting a single computer, and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,

(a) identifying the electronic record containing the statement and describing the manner in which it is produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate; and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate and for the purpose of this

sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purpose of this section:

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official information supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of these activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation: For the purpose of this section, any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process;

The case laws are yet to develop in the field of Information Technology Act in India. The interpretation of various provisions of the IT Act, therefore, has to be made according to the natural meaning flowing from it. The pronouncement of Supreme Court stating that the recording of evidence through, video conferencing is valid in law and under section 273 of Criminal Procedure Code[15], has an appreciable development in the field of appreciation of evidences.

6. Judicial interpretation of Computer related Evidence

The proper and appropriate gathering of evidence through investigation is, of course, necessary for success of a criminal prosecution. However, the success of prosecution largely depends upon

[15]State of Maharashtra v. Praful B. Desai, Crimes JT 2003 (3) SC 382.

the appreciation of computer generated evidence by the judiciary. There is need to make judiciary capable of appreciating the tangible evidences as and when they are produced in the court. It is nowadays important that the judicial officer should have a maximum level of knowledge in the computer and network technology in the present days of fast developing cyber age.

Section 46 and section 48 of the Information Technology Act, 2000 provide provision according to which the Central Government is empowered to appoint adjudicating officers who must have the experience in both information technology and legal fields for proper adjudication of any contravention of various provisions of the Act. There is also the provision for the constitution of a Cyber Regulation Appellate Tribunal for hearing the appeals against the orders of adjudicating officers. But these provisions make it clear that the adjudications of contraventions of cyber regulations should be made by the people of specialized knowledge. The judge before whom the prosecutions and the defence lawyers are presenting and evaluating the evidences, must be technically competent to evaluate the merits of the evidences as well as the evidentiary value of the document of data produced.

Anvar v. P.K. Basheer and Others[16]

In this significant judgment, the Supreme Court has settled the controversies arising from the various conflicting judgments as well as the practices being followed in the various High Courts and the Trial Courts as to the admissibility of the Electronic Evidences. The Court has interpreted the Section 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate U/s 65 B(4) of Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and also the opinion of the expert U/s 45A Evidence Act cannot be resorted to make such electronic evidence admissible.

The judgment would have serious implications in all the cases where the prosecution relies on the electronic data and particularly in the cases of anticorruption where the reliance is being

[16]Civil Appeal No. 4226 of 2012, decided on 18.09.2014.

placed on the audio-video recordings which are being forwarded in the form of CD/DVD to the Court. In all such cases, where the CD/DVD are being forwarded without a certificate U/s 65B Evidence Act, such CD/DVD are not admissible in evidence and further expert opinion as to their genuineness cannot be looked into by the Court as evident from the Supreme Court Judgment. It was further observed that all these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic records sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.

In the anticorruption cases launched by the CBI and anticorruption/Vigilance agencies of the State, even the original recording which are recorded either in Digital Voice Recorders/mobile phones are not been preserved and thus, once the original recording is destroyed, there cannot be any question of issuing the certificate under Section 65B(4) of the Evidence Act. Therefore in such cases, neither CD/DVD containing such recordings are admissible and cannot be exhibited into evidence nor the oral testimony or expert opinion is admissible and as such, the recording/data in the CD/DVD's cannot become a sole basis for the conviction.

In the aforesaid Judgment, the Court has held that Section 65B of the Evidence Act being a 'not obstante clause' would override the general law on secondary evidence under Section 63 and 65 of the Evidence Act. The Section 63 and Section 65 of the Evidence Act have no application to the secondary evidence of the electronic evidence and same shall be wholly governed by the Section 65A and 65B of the Evidence Act. The Constitution Bench of the Supreme Court overruled the judgment laid down in the *State (NCT of Delhi) v. Navjot Sandhu*[17] alias Afsan Guru by the two judges Bench of the Supreme Court. The court specifically observed that the Judgment of *Navjot Sandhu* supra, to the extent, the statement of the law on admissibility of electronic evidence pertaining to electronic record of this Court, does not lay down correct position and required to be overruled.

[17](2005) 11 SCC 600.

The only options to prove the electronic record/evidence is by producing the original electronic media as primary Evidence court or it's copy by way secondary evidence U/s 65A/65B of Evidence Act. Thus, in the case of CD, DVD, Memory Card etc. containing secondary evidence, the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.

7. Conclusion

Though in India we have Information Technology Act, 2000 which provides various provisions relating to the police powers in cases of cyber-crimes and there are so many provisions under The Indian Evidence Act, 1872, The Indian Penal Code, 1860 regarding the electronic documents and there admissibility as an evidence still India is lagging far behind as there are not proper cyber cells to deal exclusively with the cases of cyber-crimes. Cyber-crimes are increasing by leaps and bounds. Newspapers are full of information on various scams. India has seen a 280 percent increase in bot infections that is continuing to spread to a larger number of emerging cities in India. India has the highest ratio in the world of outgoing spam or junk mail of around 280 million per day worldwide. India's home computer owners are the most targeted sector of cyber-attacks. Mumbai and Delhi are emerging as the top cities for cyber-crimes. In such a situation need is to have proper cyber cells with specially trained police officers, lawyers, judges to deal with the technicalities of the cyber-crimes