Himachal Pradesh National Law University, Shimla (India)

HPNLU Law Journal

Journal Articles *ISSN:2582-8533* *HPNLU Law Journal*

Volume II (2021)

ELECTRONIC EVIDENCE AND CYBER FORENSICS IN INDIA

Shubham Singh Bagla

Contents

Volume II | *ISSN: 2582-8533* | April 2021-March 2022

ELECTRONIC EVIDENCE AND CYBER FORENSICS IN INDIA

Shubham Singh Bagla*

[***Abstract****: Cyber forensics refers to the methodical recovery, storage, analysis, and presentation of digital information. Electronic evidence is the product of that process. This process is to be carried out after the commencement of cybercrime to extract, recover, analyze and store the electronic data that can be used as evidence to determine the culpability of the perpetrator by the judicial authorities. The critically essential factors are the identification of the evidence, its collection, and determining the method of attacks because of the level of complexity of cyber-attacks. The investigator must pay special attention to details like maintaining the proper chain of custody of the evidence gathered and ensuring that proper documentation of the same is maintained at all times. The success of a case depends on the evidence collected in such cases; hence the role of the investigator is very important. Due to this constant rise in digital or cybercrimes, there is a need for a robust legal framework that can prevent, prohibit, and redress the issue of cyber forensics. The researcher has found certain facts that exist and left a wide research gap in digital evidence, its relevancy and admissibility. There is a pressing need to upgrade the preservation of electronic evidence in Indian Courtrooms. This paper compares the legal dimensions of cyber forensics in different jurisdictions. This study assays to analyze the ambiguities in the system and what are the potential solutions for these challenges to ensure speedy justice.]*

Science & technology have freed humanity from many burdens & given us this new perspective & great power. This power can be used for the good of all. If wisdom governs our actions, but if the world is mad or foolish, it can destroy itself just when great advances & triumphs are almost without its grasp.

— Jawaharlal Nehru

* Research Scholar, Ph.D., Himachal Pradesh National Law University, Shimla. *Email:* shubhamsinghbagla@gmail.com. The Author is indebted to the guidance and discussions with Prof. (Dr.) Nishtha Jaswal, Dr. Chanchal Kumar Singh, Dr. Santosh Kumar Sharma, Dr. Mritunjay Kumar, Mr. Aayush Raj, and Mr. Tijender Kumar Singh. Views expressed are personal.

I

Introduction

According to Steve Hailey, President of the Digital Forensics Certification Board (DFCB), Computer forensics is "*the preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, the integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceedings as to what was found.*"[1]

Cyber forensics[2] has evolved with the inception of the internet and technology. Since the late 19th century, experts have considered various forensic tools to determine the evidence's flawlessness. This caters for the need for Forensics Sciences, which booms the discovery and intervention of Forensics Methodologies in the 20th century. In 1984, The Computer Analysis and Response Team (CART) was introduced as a limb of the Federal Bureau of Investigation (FBI), supporting field offices with evidence derived from computer forensics. FBI organized the first international conference on computer evidence, viz., International Law Enforcement Conference on Computer Evidence, in 1993 within the United States at the Federal Bureau of Investigation Academy in Quantico, Virginia and attended by representatives from as many as twenty-six countries to discuss the fallacies of electronic evidence. In 1995, The International Organization on Computer Evidence (IOCE) was envisaged to become a platform for exchanging knowledge between international law implementing agencies with reference to cybercrime investigations and cyber forensics. Further development in this field was done in 1998; another International Forensic Science Conference came up as a platform for forensic managers to exchange knowledge among different countries and establish a platform to exchange their technical information to curb globally emerging cyber-crimes. In 2000, The First Federal Bureau of Investigation Regional computer forensic Laboratory (RCFL) was formed for the examination of digital evidence in support of criminal investigations like identity theft, hacking, computer viruses, terrorism, investment fraud, cyberstalking, drug trafficking, phishing/spoofing, wrongful programming, credit card fraud, online auction fraud, e-mail bombing and spam, and property crime.

In India, the trace of advancement in the field of cyber forensics can be seen after The Information Technology Act, 2000 (No. 21 of 2000) (IT Act) was introduced to provide legal recognition of electronic records as evidence. The IT Act instituted provisions in the Indian Evidence Act 1872, which provide the legal framework for the cyber forensic

---

1 Nilima Prakash, Dr. Roshni Duhan, *Computer Forensic Investigation Process And Judicial Responseto The Digital Evidence In India In Light Of Rule Of Best Evidence*, 8(5) IJMSS (2020).

2 North Carolina Wesleyan College, *Digital Evidence Collecting & Handling*, *available at*: http://faculty.ncwc.edu/toconnor/495/495lect06.htm (last visited 17 Mar., 2020).

investigation of cybercrime in India regarding the relevancy and admissibility of electronic evidence.

Cyber forensics has been gaining importance with every passing day and with the increasing forms and manners of cybercrimes and litigations involving parties of a more significant institutional character.[3] It is a sine qua non for each organization in modern times to use the services of a cyber forensics agency or rent a specialized professional from the same field to protect the organizations with regard to cybercrimes and data protection.

Objectives of computer crimes became more pervasive with a rise in computer crime incidents starting from theft of intellectual property to cyber-terrorism.[4] The result of all cyber forensics is to discover a computer incident, identify the intruder, and prosecute the offender in a court of law. Cyber forensics and its auxiliary areas, still aloof from a full-scale development, presently exist in an aborning stage[5]. This paper focuses on cyber forensics processes, methodology and outcomes in the form of electronic evidence. This is followed by a characterization of the necessity of developing cyber forensics and additional discussion on the various doable processes and ways of practising the same, and also elucidates on cyber-crime investigations.

II

Cyber Forensic Methodologies

There should be a typical set of pointers adhering to specific methodologies to be used throughout the investigation. It should be understood that the evidence obtained in cyber-crimes will be tampered with and is volatile in nature, and thus, the procedure given should not be deviated from in any manner. The methodologies concerned in cyber forensics could disagree depending upon the measures, assets, and target company. The investigator will utilize tools to get back the information that has been hidden or deleted or may have been temporary. Forensic readiness helps with cyber-crimes and beat cyber-attacks on their systems or networks.[6]

---

[3] Bruce J. Nikkel, *The Role of Digital Forensics within a Corporate Organization*, IBSA CONFERENCE, Vienna, 2006 *available at*: http://www.digitalforensics.ch/nikkel06a.pdf.

[4] Byron S. Collie *et. al*., COMPUTER AND INSTRUSION FORENSICS 257- 320 (2003).

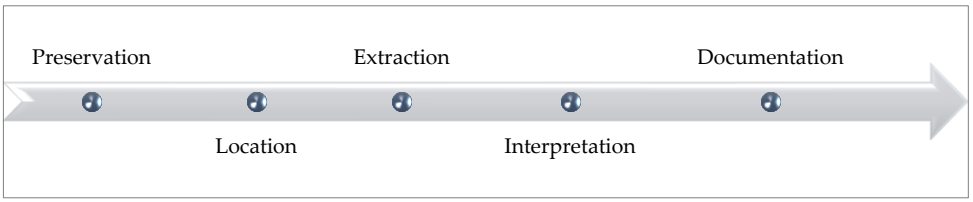
[5] Warren G. Kruse II & Jay G. Heiser, COMPUTER FORENSICS: INCIDENT RESPONSE ESSENTIALS 22 (2001).

[6] Eric N. Newburger, *Current Population Reports: Home Computers and Internet Use in the United States: August 2000*, U.S. CENSUS BUREAU (Sep. 2001) *available at* - https://www.census.gov/prod/2001pubs/p23-207.pdf.

Cyber-forensic professionals emphasized essential areas like standalone computers, workstations, servers, and online channels. Whereas investigating computers and workstations is comparatively simple, the ransacking through the servers and online channels is very complicated.

During investigations, logs are usually not examined or audited. The investigator should appreciate that logs play an essential part throughout investigations. In many cases, they have been identified to produce necessary results in the offender's apprehension.[7]

Cyber forensic methodologies encompass the following basic activities:



Preservation: The forensic expert should ensure that the initial evidence is not tampered with or broken. The experimentations should be carried out on a copy/image of the original. The copy should be compared with the original for any error/oddity.

Location: There is a difference between evidence containers and real evidence. Before the investigation, the examiner should determine the evidence and its actual locations, i.e., where it is contained. Locating and identifying data and information could be challenging for each cyber forensic investigator. Processes like keyword searches, log file analyses and routine system checks facilitate the investigation at different stages.

Extraction: Post identification, the foremost vital method is extracting the information from the same. The information being volatile, the digital investigator should extract the information from a copy/image of the original evidence. Also, a backup should be taken at different stages of the investigation to ensure that no evidentiary information is lost.

Interpretation: The primary part of the investigator throughout the investigation is also to investigate what his/her find is. The same should have lots of clarity and stand high on technical ground.

Documentation: From the initial investigation of the crime scene to the bagging and tagging and ultimate analysis of evidence, the investigator has to maintain a transparent

---

[7] COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION; UNITED STATES DEPARTMENT OF JUSTICE, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations; Office of Legal Education*, Executive Office for United States Attorneys 2002 *available at*: https://law.ku.edu/sites/law.ku.edu/files/docs/media_law/Searching_Seizing_Computers_and_Obtaining_Electronic_Evidence_in_Criminal_Investigations.pdf.

documentation form. This may relate to the queries concerning the chain of custody as well.

Broad tests for evidence for electronic record

After the evidence is collected, investigators perform general tests on the evidence (utilizing both cyber forensics as well as generic forensics) to see the *authenticity* and r*eliability* of evidence which the investigator should verify the supply of the evidence and also verify if the evidence is reliable and perfect, respectively to be admissible in the court of law.[8]

III

Legal framework of different countries

In this part, the researcher discussed the legal framework of the relevancy and admissibility of the electronic record in the court of law. Australia, South Africa, United Kingdom (UK), United States of America (USA) has been dealt in this part while Indian legal framework was covered in next part of the paper.

Australia

The law regarding documentary evidence originated centuries before, and they have been formulated to apply to document in hard copy.[9] Hard copy and electronic records are different from each other; hence, the law needs to be different for them respectively so that the law of evidence related to them must be considered again since there is a difference between a filing cabinet, where the files will be stored, and any other storage device like a hard disk drive, as the data stored on it, is embedded in the storage medium.[10]

Law of Evidence

The common law and the statutes dealing with the admissibility of evidence in Australia. It is a federal system. This implies that there are eight distinct state Evidence Acts and a federal Act. Therefore, in Australia, the practice of documentary evidence in

---

[8] David L. Sobel, *Will Carnivore Devour Online Privacy?*, 34(5), IEEE COMPUTER 87 (2001).

[9] Allison Rebecca, THE AUTHENTICATION OF ELECTRONIC EVIDENCE, Queensland University of Technology (2016) [Thesis] *available at*: https://eprints.qut.edu.au/93021/1/Allison_Stanfield_Thesis.pdf.

[10] *Innovative Health Group Inc.* v. *Calgary Health Region*, 2008 ABCA 219 (CanLII).

legal proceedings is sophisticated and subject to different jurisdictions.[11] The researcher will mainly deal with the Uniform Evidence Acts applicable in federal courts.

Relevancy and Admissibility

The evidence must be sufficiently relevant to be admissible. Under section 55[12]of the Uniform Evidence Acts, the evidence is sufficiently relevant if it can affect the rational assessment of a probability of a fact in issue.[13]

According to the abovementioned Act, anything from which writing can be produced with or without any other aid is a document. Therefore, the same rules of evidence apply to electronic evidence. However, the above Act contains various related provisions relevant to electronic evidence.[14]

Section 146[15], Uniform Evidence Acts, holds a rebuttable presumption that admits a photocopy or electronic copy of a document to be assumed to be a true copy of the source document. It would be onerous to rebut the assumption that a photocopy is a true copy of the original if the anti-tampering processes were done.

The Uniform Evidence Acts caters for the assumption that copies of the source are admissible as evidence. However, there is no rule regarding the reliability of such evidence. The operation of such law can be so that the copies of the original document or electronically stored version of the original may be given less weightage if introduced in evidence. Accordingly, when the electronically stored information is dealt with, the emphasis is on the integrity of the procedure by which the data is extracted, stored, and produced electronically.

United Kingdom

In the United Kingdom, under Sec 20[16] of the *U.K. Police and Criminal Evidence Act*, 1984, the Digital evidence is relevant and admissible in the United Kingdom court of law and

---

[11] EVIDENCE LAW IN AUSTRALIA, *available at* - http://www.naa.gov.au/information-management/information-governance/evidence/evidence-law-australia/index.aspx, (last visited 20 Apr., 2020).

[12] S. 55, Uniform Evidence Act, 1995. *Relevant evidence.*

(1) The evidence that is relevant in a proceeding is evidence that, if it were accepted, could rationally affect (directly or indirectly) the assessment of the probability of the existence of a fact in issue in the proceeding.

(2) In particular, evidence is not taken to be irrelevant only because it relates only to: (a) the credibility of a witness, or (b) the admissibility of other evidence, or (c) a failure to adduce evidence.

[13] EVIDENCE: OVERVIEW OF THE PRINCIPLES OF RELEVANCE AND ADMISSIBILITY, *available at*: http://www.findlaw.com.au/articles/113/evidence-overview-of-the-principles-of-relevance-a.aspx (last visited 25 Apr., 2020).

[14] *Id*.

[15] S. 146, Uniform Evidence Acts, 1995.

[16] S. 20, U.K. Police and Criminal Evidence Act, 1984.

accordingly, the Police have carried out the investigation while the tools and techniques related to the procedure of the collection of the evidence are more or less same as the United States and India.

The Certification for the admissibility of digital evidence, similar to the Indian Evidence Act, 1872, laid down in section 69[17] of the *U.K. Police and Criminal Evidence Act, 1984* (now repealed[18]), provided two conditions for the admissibility of the computer record, i.e.,

i. There are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;
ii. That at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.

In *R* v. *Shephard*,[19] the question arose, "Whether a party seeking to rely on computer evidence can discharge the burden under section 69(1)(b) of the Police and Criminal Evidence Act 1984 without calling a computer expert, and if so, how?"

Lord Griffiths observed that:

> *"The object of section 69 of the Act is clear enough. It requires anyone who wishes to introduce computer evidence to produce evidence that will establish that it is safe to rely on the documents produced by the computer. This is an affirmative duty emphatically stated:-*
> *"A statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown.*
> *Such a duty cannot be discharged without evidence by the application of the presumption that the computer is working correctly expressed in the maxim omnia praesumuntur rite esse acta as appears to be suggested in some of the cases. Nor does it make any difference whether the computer document has been produced with or without the input of information provided by the human mind and thus may or may not be hearsay.*
> *If the prosecution wishes to rely upon a document produced by a computer, they must comply with section 69 in all cases…"*

From the above observation, we see the juxtaposition of the U.K. and Indian legal frameworks as to the admissibility of electronic evidence are quite similar before the further amendment in the Police and Criminal Evidence Act, 1984. The same requirement now ceased to have effect by Section 60 of the Youth Justice and Criminal Evidence Act, 1999. In U.K. law, no distinction is made between computer-generated evidence and other evidence either qua the admissibility of or the attachment of weight to such evidence.

---

[17] S. 69, U.K. Police and Criminal Evidence Act, 1984.

[18] S. 60, The Youth Justice and Criminal Evidence Act, 1999.

[19] *R* v. *Shephard,* 1993 AC 380; (1993) 2 WLR 102 (HL).

United States of America

Cyber forensics is a burning subject in the court of law, and many existing laws are used to prosecute computer-related crimes. Precedents and practices with reference to cyber forensics are still uncertain. The best source of information in this area is the United States Department of Justice's Cyber Crime website[20]. The important point for forensics Experts is that evidence must be collected in a way that is legally admissible in a court of law. Increasingly, laws are being passed that require organizations to safeguard data privacy.[21] Due to the constant technological changes, law enforcement agencies must draft up-to-date policies to address electronic evidence issues. To do so, these authorities need to work with other partners to determine the legal requirements regarding electronic evidence's relevancy, custody, and admissibility.[22]

There are three areas of law related to important cyber security. The First is found in the United States Constitution. In Fourth Amendment,[23] the protection against unreasonable search and seizure is allowed, and the Fifth Amendment[24] protects against self-incrimination. Although the amendments were written before, there were problems caused by people misusing computers, and their principles apply to how cyber forensics is practised. The Fourth Amendment protects against unreasonable search and seizure by government authorities. To carry out the search, law enforcement officers are required to obtain the warrants from the appropriate court.[25]

Second, anyone concerned with cyber forensics must know how three U.S. Statutory laws[26] affect them and :

i. Wiretap Act (18 U.S.C. 2510-22)
ii. Pen Registers and Trap and Trace Devices Statute (18 U.S.C. 3121-27)
iii. Stored Wired and Electronic Communication Act (18 U.S.C. 2701-120)

Violations of any of these statutes during cyber forensics practice could constitute a federal felony punishable by a fine, imprisonment, or both.[27]

Third, the U.S. Federal rules of evidence about hearsay, authentication, reliability, and best evidence must be understood. In the U.S., two primary areas of legal governance

---

[20] Cybersecurity & Infrastructure Security Agency, US CERT, *available at*: https://www.cisa.gov/uscert/sites/default/files/publications/forensics.pdf.

[21] Id.

[22] *Riley* v. *California* 573 US 2014.

[23] See also, *A detailed analysis of issues surrounding the Fourth Amendment on this web site*, THE FOURTH AMENDMENT - UNREASONABLE SEARCH AND SEIZURE http://caselaw.lp.findlaw.com/data/constitution/amendment04 (last visited 02 Mar., 2020).

[24] U.S. DEPARTMENT OF JUSTICE, *available at*: http://www.usdoj.gov/criminal/cybercrime/cclaws.html (last visited 02 Mar., 2020).

[25] *Horton* v. *California,* 496 US 128 (1990).

[26] *Supra note* 20, CISA.

[27] *Id.*

affect cybersecurity actions related to the collection of network data, viz., authority to monitor and collect the data and admissibility of the collection methods.

Admissibility

It is required by the Federal Rules of Evidence that the scientific and expert evidence must be reliable in terms of the use of principles and methods used as well as the application of these principles to the specific set of facts.[28] The original test for scientific evidence was the Frye Test.[29]

This test made the scientific evidence admissible if the scientific community generally accepted the science upon which the evidence rested. The Daubert guidelines have replaced this test.[30] These guidelines provided certain criteria that must be met while determining the admissibility of scientific evidence.

South Africa

The validity for excluding or admission of evidence has been proposed to be the relevancy of such evidence. However, South Africa adopts an exclusionary approach as far as the admissibility of evidence is regarded. How to treat electronic evidence has been exercised by the South African Law Commission since 1976 when in a civil matter, the Appellate Division would not admit bank records generated by a computer as evidence.[31]

Recently, the Electronic Communications and Transactions Act (The E.C.T. Act) of 2002 was passed. The E.C.T. was the responsibility of the Department of Communications. Neither the Department of Justice nor the Law Commission appears to have bestowed much to what the Act talks about evidence. The Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA)[32] governs the interception of electronic communications. Chapter 6 of RICA allows the Minister responsible for the intelligence services to institute interception centres that will be permanently linked to the telecommunication systems and will enforce any interception centres that are run by a Director aided by representatives of the departments responsible for the following areas of government: defence, intelligence, communications, Police, and justice.[33]

---

[28] R. 801[d][2], The Federal Rules of Evidence, 1975.

[29] *Frye* v. *United States* 293 F 1013 (D. C. Cir. 1923).

[30] *Daubert* v. *Merrell Dow Pharmaceuticals, Inc.* 509 U.S. 579 (1993).

[31] *Narlis* v. *South African Bank of Athens* 1976 (2) SA 573 (A) at 578.

[32] Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (South Africa).

[33] S. 209, The Intelligence Services Oversight Act, 1940.

IV

India

Introduction

In legal terminology, "the application of science to the identification, collection, examination, and analysis of data, while preserving the integrity of the information and maintaining a strict chain of custody for the data while adhering to the legal rules of evidence is defined as cyber forensics."[34] Activities and studies covered under it often overlapped and conducted simultaneously, such as wireless forensics, media forensics, network forensics, database forensics, mobile forensics, disk forensics, I.P. Address tracking, e-mail tracking, cloud computing and other modes of digital forensics.[35] The primary object of a collection of electronic evidence is to link the accused with the crime through tracing footprints via systematic and careful preservation, extraction, evaluation, interpretation, and documentation under the broad canvass of 'fair and reasonable' procedure. The complexity of the task cannot be undermined, for it not only includes the discovery of data, recovery of deleted data, the revelation of hidden or confidential data or content in encrypted files while protecting the computer system and after an in-depth analysis, testimonial evidence based on the evidence collected.

Legal Provisions

The challenges and problems with the cyber world have caught the attention of the legislators, who, through the confluence of two legal paradigms, i.e., the law of evidence and that of information technology, have provided a structure to tackle them. They are the Indian Evidence Act of 1872 (herein IEA) & Information Technology Act of 2000[36](herein IT Act). Different cybercrimes have been provided under the I.T. Act, 2000; Indian Penal Code, 1860; Narcotic Drugs and Psychotropic Substances Act, 1985; Arms Act, 1959 & other special laws. In 2000 Parliament enacted the Information Technology (I.T.) Act 2000 amended the existing Indian statutes to allow for the admissibility of digital evidence. The I.T. Act is based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce and, together with providing amendments to the IEA, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891; it recognizes transactions as electronic records that

---

[34] Albert J. Marcella, Jr. & Doug Menendez, CYBER FORENSICS: A FIELD MANUAL FOR COLLECTING, EXAMINING, AND PRESERVING EVIDENCE OF COMPUTER CRIMES 297 (2007).

[35] Munkhondya, Howard *et. al., Digital Forensic Readiness Approach for Potential Evidence Preservation in Software-Defined Networks,* INTERNATIONAL CONFERENCE ON CYBER WARFARE AND SECURITY, ACADEMIC CONFERENCES INTERNATIONAL LIMITED 268 (2019).

[36] S. 4, Information Technology Act, 2000 & Ss. 65A and 65B, Indian Evidence Act, 1872.

are carried out through electronic data interchange and other means of electronic communication.[37]

Electronic evidence's legal recognition and admission have been provided in Section 3 of IEA. The conventional definition of documentary evidence now includes electronic records as well. The other parallel provision exists in Section 4 of I.T. (Amendment Act), 2008, which allows matter in the electronic form to be accepted and regarded as 'written' for legal purposes if the need arises. Thus, digital evidence is prima facie acceptable in the Indian courts of law.

In a step further towards defining the scope of electronic evidence, it has been defined as information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital audio, digital fax machines, digital video under Section 79A of the I.T. (Amendment) Act, 2008.[38]

The admissibility of electronic records is covered primarily under Section 65-B[39] of IEA, which lays down several conditions for the same.

There are two significant questions in cybercrime investigation, one regarding storage devices and the other being the reliability of digital evidence. Regarding the first question, the admissibility of storage devices, primarily computers, is important since all digital evidence needs to be secured, extracted, stored and preserved in a particular form. A cumulative reading of both provisions of the Indian Evidence Act 1872 indicates that the computer outputs original electronic record has been made admissible as evidence "without proof or production of the original record. Thus, the matter on computer printouts, floppy disks, and CDs becomes admissible as evidence."[40]

With regards to the second question, the clarification can also be found clarified by Section 79A of the I.T. (Amendment) Act, 2008, which empowers the Central government to appoint any department or agency of the Central or State government as Examiner of Electronic Evidence. This agency will play a crucial role in providing expert opinions on the electronic form of evidence. The question of recognition of digital evidence is officially settled under Indian law.[41] The scope of electronic evidence has been further widened by Section 79A of the I.T. Act. It provides that electronic evidence refers to the information-carrying probative value, including digital audio/video, cell phones, computer-based evidence & digital fax machines.

---

[37] A. Venkateshwara Rao, *Admissibility Of Electronic Evidence, available at*: https://districts.ecourts.gov.in/sites/default/files/Webinar%20on%20Admissibility%20of%20Electronic%20Evidence%20By%20Sri%20A%20Venkateshwara%20Rao.pdf.

[38] Editor, *Electronic Evidence Understanding through Case Laws,* VI(I) RLR 1 (2021).

[39] S. 65B, Indian Evidence Act, 1872.

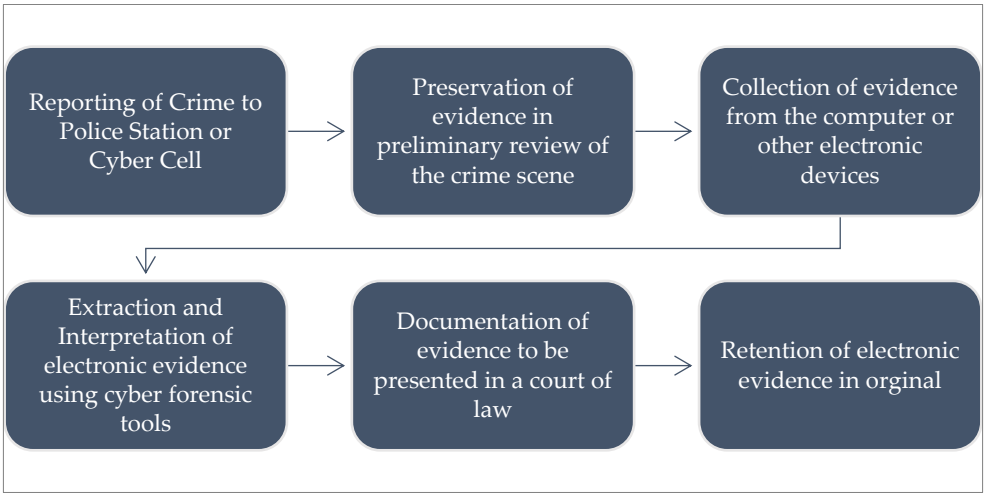
[40] T. Vikram, *Cyber Crimes - A Study with a Case*, INDIAN POLICE JOURNAL 78 (2002).

[41] S. 3, The Indian Evidence Act, 1872.

Cyber Forensic Investigation – An Overview

Crimes, where a computer serves as a means to serve an illegal purpose include data modification and deletion, cyber staling, data theft, identity theft, child pornography, theft of intellectual property or trade secrets, financial frauds, cyber warfare and corporate espionage. Crimes where a computer is a target are hacking, spoofing, spamming, virus dissemination, service denial, botnet attacks, website defacement, and other cyber-crimes. Each category of cyber offence has its essentials that need to be fulfilled. Under Section 66 of the I.T. Act, 2000, for an act to be investigated, it has fallen under Section 43 of the I.T. Act, 2000 and done with dishonest and fraudulent intention as defined under Sections 24 and 25 of the Indian Penal Code. The requirement needs to be fulfilled. Otherwise, the offence will not be investigated as a cybercrime.[42]

From here, cyber forensics plays an important role in the image, recovery, extracting or salvaging and examining the information stored in the storage medium or digital device to establish the link between the accused and the crime. Due care must be taken that the line of custody is not to be broken, if it broken at any point of time, questions arose as to the integrity of the original message and its probable alteration by the interested party, and such evidence loses its integrity and credibility in the court of law.



The procedure of reporting the cases and investigating is quite a tedious process. Firstly, reporting of crime, the aggrieved person approaches the police station or specialized cyber cell if available in the department. The officer in charge looks upon the matter and collects the requisite information per the case. If it reveals that any act violates the I.T. Act 2000 and is the case of cognizable offence, then particulars like modus operandi,

[42] See also, Pavan Duggal, *Cyberlaw In India: The Information Technology Act 2000 available at-* https://www.mondaq.com/india/it-and-internet/13430/cyberlaw-in-india-the-information-technology-act-2000--some-perspectives (last visited 05 Jul., 2020).

time, place of commission, details of the targeted individuals or system, etc., are recorded.

Secondly, a preliminary review of the crime scene is done for potential evidence that may be secured, and pre-investigation is conducted, followed by serving notices for the preservation of evidence to all affected persons.[43]

Thirdly, access to the criminating devices or machines is limited to forbid further contamination or unnecessary loss. The procedure of collecting evidence from the system, whether on or off, have to do as per Section 165 of the Code of Criminal Procedure (CrPC) read with Section 80 of the I.T. Act.

Fourthly, the chain of custody should not be broken or tampered with, and due care has to be done to ensure the integrity of the evidence by the expert, e.g. hashing method[44], i.e. the generating a value or values from a string of text using a mathematical function.[45] The officer in charge of the investigation should track it down in the Digital Evidence Collection Form, which contains the description of the whole process, the tools used, the hash value acquired from the forensic images of evidence, and the hash algorithm used in such processes.

Fifthly, the documentation and collection of evidence by forensic imaging or storage in another device like a compact disk, hard drive, or USB is followed by the packaging, labelling, tagging, and updating of the evidence database.

Sixthly, a court order can be sought to retain seized evidence, and it is sent for forensic analysis. If the property owners advance the court for the release of property, an officer in charge should preferably restore the copy of the forensic image of the seized evidence, not the original.

Cyber Crime Investigation by C.B.I. & other Institutions

The C.B.I. has three primary divisions to deal with different categories of offences. Firstly, the Anti-Corruption Division, as the name suggests, is for the offences enumerated under the Prevention of Corruption Act, 1988, against government employees and public officials. This is the most active and largest of its division. Secondly, the Special Crimes Division deals with widely publicized organized offences under I.P.C. and other laws at the states' request or under the orders of the High Courts or the Supreme Court. Lastly, the Economic Offences Division investigates serious economic frauds, financial scams, fake currency, bank frauds and cyber crimes.[46] The

---

[43] DATA SECURITY COUNCIL OF INDIA, *Cyber Crime Investigation Manual, available at:* https://uppolice.gov.in/writereaddata/uploadedcontent/Web_Page/28_5_2014_17_4_36_Cyber_Crime_Investigation_Manual.pdf.

[44] *See,* S. 3(2) Explanation, Information and Technology Act, 2000.

[45] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, 2001.

[46] CENTRAL BUREAU OF INVESTIGATION, *available at:* http://cbi.nic.in/faq.php (last visited 11 Apr., 2020).

C.B.I. can be approached for any grave economic offence not of a routine or general nature.

The Central Bureau of Investigation has three primary divisions: Anti-Corruption Division (the largest & the most active division), the Special Crimes Division & Economic Offences Division.

Furthermore, it has a total of 4 bodies that handle computer-related offences: -

Firstly, the Cyber Crime Investigation Cell, formed in 1999 (Operating since 2000), is headed by police superintendent & is the nodal contact point for Interpol.[47]

Secondly, the Cyber Forensics Laboratory, dating back to 2003, functions under the Director of the Central Forensic Science Laboratory. It provided expert testimony for law enforcement agencies.

Thirdly, Cyber Crimes Research & Development Unit collects information for further investigation & prepares a monthly Cyber Crimes Digest for the benefit of government agencies. Work for research & development of cyber forensics is also carried out by it.

Fourthly, the Network Monitoring Centre is responsible for internet policing.[48] Other than C.B.I., numerous other institutions help to maintain internet security in India, to name a few responsible for this herculean task which comes under different ministries of the Government of India, i.e. Under the *Ministry of Home Affairs*,[49] there are different departments which deal with cyber forensics, viz., National Intelligence Grid, Intelligence Bureau, National Investigation Agency[50], National Crime Records Bureau, National Cyber Coordination Centre[51], National Informatics Centre, Cyber and Information Security (C&IS) Division[52]; under the *Ministry of Information and Broadcasting*, there are two department dealing with cyber forensic, viz., Electronic Media Monitoring Centre[53], and New Media Wing;[54] under the *Ministry of Electronics &*

---

47 CYBER CRIME, CYBER CRIME INVESTIGATION CELL, *available at*: http://cybercrime.planetindia.net/cybercrime_cell.htm (last visited 28 Apr., 2020).

48 EDUCATION AND RESEARCH NETWORK, EARLIER PROJECTS, *available at*: http://www.ernet.in/Rnd/earlierRnd.html (last visited 01 May, 2020).

49 MINISTRY OF HOME AFFAIRS, *available at* - https://www.mha.gov.in/en/about-us/organizational-structure (last visited 15 May, 2020).

50 NATIONAL INVESTIGATION AGENCY, *available at:* https://www.nia.gov.in/organisational-chart.htm (last visited 15 May, 2020).

51 MINISTRY OF HOME AFFAIRS, *Division available at:* https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme (last visited 15 May, 2020).

52 *Id*.

53 ELECTRONIC MEDIA MONITORING CENTRE, *available at* - http://emmc.gov.in/ (last visited 15 May, 2020).

54 NEW MEDIA WING, *available at* - http://nmw.gov.in/ (last visited 15 May, 2020).

Information Technology,[55] there are different divisions which deals with cyber forensics, viz., Cyber Security Division, Cyber Laws Division, Research and Development Division, Emerging Technologies Division, National Informatics Centre,[56]India Computer Emergency Response Team (CERT-In),[57]etc.; Under the *Ministry of Finance,* Central Economic Intelligence Bureau[58]also use cyber forensics tools and methodology to secure their financial transactions; Under the *Ministry of External Affairs,* EG & IT [E-Governance & Information Technology] Division[59]deals with cyber-related issues using cyber forensics; Under the *Ministry of Defence*[60], Defence Research and Development Organisation, Department of Defence, use cyber forensic to safeguard India from cyber-attacks and cybercrimes.

Challenges to Cyber Security in India

In India, several cyber forensic tools are employed to tackle the issues in cyberspace. A notable example is the Cyber & Hi-Tech Crime Investigation & Training (CHCIT) Centre in Ghaziabad, Uttar Pradesh which assists in ongoing investigations with forensic analysis through certified investigators and the latest gadgets and technologies, some of which are; triage tools, relationship analysis/call data analysis software, write blockers, field forensic devices, social networking analysis tool, password recovery tools and software, cellular and P.D.A. analysis forensic tools; phone memory & sim card analysis, forensics softwares for image analysis viz. Cybercheck, F.T.K., Winhex, Encase, Paraben; forensic workstations & FREDS (Forensic Recovery Of Evidence Destroyed) with hi-end processors equipped with internal media wiping devices, internet investigation tools, steganography detection & analysis tool, system imaging and analysis tools, hardware-based imaging tools, in-situ examination forensic tools and others.[61] This is indicative and not an exhaustive list.

Law enforcement agencies require better, legally, and technically sound training for all the agents in the criminal justice system. However, the training will be inadequate without the upgradation of internationally acceptable tools and the establishment of institutions catering to cyber forensics services. Often, where techniques have been

---

55 MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, *available at:* https://www.meity.gov.in/about-meity/organization-chart (last visited 15 May, 2020).

56 NATIONAL INFORMATICS CENTRE, *available at*: https://www.nic.in/emerging-technology/ (last visited 15 May, 2020).

57 INDIAN COMPUTER EMERGENCY RESPONSE TEAM, *available at:* https://www.cert-in.org.in/ (last visited 15 May, 2020).

58 MINISTRY OF FINANCE, DEPARTMENT OF REVENUE, *available at*: https://dor.gov.in/link/ceib (last visited 15 May, 2020).

59 MINISTRY OF EXTERNAL AFFAIRS, *available at*: https://mea.gov.in/divisions.htm (last visited 15 May, 2020).

60 MINISTRY OF DEFENCE, *available at*: https://mod.gov.in/ (last visited 15 May, 2020).

61 CBI ACADEMY, *Cyber & Hi-Tech Crime Investigation & Training (CHCIT) Centre, available at*: http://www.cbiacademy.gov.in/chcit.php (last visited 15 May, 2020).

provided, they are either underused or avoided, such as video conferencing in trials. Even the Police have been found to incline towards traditional forms of oral and documentary evidence despite the accuracy and authenticity of electronic evidence.

While the country is geared up to become one of the most effective E-services countries of the world, the initiatives on the part of the government to deal with the ever-rising number of cyber criminals have been half-hearted and marginally successful. It would not be false to comment that several citizens are blissfully unaware of the potential lying in cyber forensics. The strength of internet users is increasing, and the easy accessibility of data with the user's anonymity makes the virtual world a breeding ground for cybercriminals. To meet the danger before it becomes a thorn in the flesh, emphasis must be placed on preventive methods, for prevention is always better than cure. Awareness campaigns, especially for young users, development of anti-virus software, greater control over website owners and administration, the framing of guidelines, international cooperation and exchange for information are some of the measures that may be undertaken.

International Cooperation and private forensic investigators

Private investigation is also widely popular in India. When faced with money laundering charges, HDFC Bank appointed Deloitte Touche Tohmatsu India, an independent cyber forensic agency, to investigate the matter, which the R.B.I. later questioned. The reliability of such investigations is yet to be decided.[62]

Multiple private bodies also offer forensic services in India, such as Labsystems, Foundation Futuristic Technologies, ANA Cyber Forensic Pvt. Ltd., A & R Info Security, Forensics Guru and Secugenius, Synclature.[63] These companies have worked independently or in collaboration with government bodies to cater to cyber forensic facilities. In India, the participation of private investigators is looked upon with suspicion & the admissibility of evidence tendered by such organizations is doubted due to the high probability of alteration & manipulation by powerful companies or persons. Supporters, however, argue that corruption is not restricted to private bodies & hampers public investigation agencies.

The investigation of cybercrimes is still at its nascent stage in India & to ensure that a fair trial is provided to each & every cybercriminal, tools & techniques must be improved. The Apex Court has also called for systematic regulation & control of

---

[62] Anand Adhikari, *Too many loopholes*, BUSINESS TODAY (14 Apr., 2013) *available at* - http://www.businesstoday.in/magazine/features/cobrapost-expose-on-money-laundering-by-banks/story/193462.html.

[63] *Top 5 Cyber Forensic Companies Indian 2016*, SILICON INDIA, *available at* - http://www.siliconindia.com/ranking/cyber-forensic-companies-2016.html (last visited 28 Feb., 2020).

cybercrimes in India and made observations regarding the lack of procedural checks.[64] Better cyber security will ensure the fraternity of the individual and the security & integrity of the nation, a constitutional objective. [65]

In the virtual world, remote access to the location has required cooperation between international agencies and the INTERPOL to follow the track of cybercrimes. Various international instruments like Mutual Legal Agreement Treaties (MLATs) also assist in transferring information and collaborative investigation. In India, Sections 166A and 166 B of the Code of Criminal Procedure, 1973 allow a criminal court to send a letter of request to a competent authority for investigation in a foreign country and a letter of request issued by the foreign country to an Indian authority for investigation of crime in India. [66]

In India, private investigators are not popular or widely accepted in the current system. To seek the expert's opinion, it is advisable for numerous law enforcement agencies that the collection, procedure, and analysis of electronic records by the private forensic investigators were improper, and adverse inferences was raised on the reliability of the evidence. Recently, facing serious Benami transactions and money laundering charges, HDFC bank galvanized into action and appointed Deloitte Touche Tohmatsu India, an independent forensic agency, to probe the allegations. The same was questioned by R.B.I., which raises several questions about the reliability of the private investigator's evidence.[67]

Role of Indian Judiciary

The Indian Judiciary has emerged as a pioneer in preserving online privacy & cyber security, expanding the scope of digital evidence & individual rights.[68] The evolution of computers, the influence of technology and the ability to store records in digital form have all required Indian law to include provisions on the appreciation of electronic

---

[64] *Dilipkumar Tulsidas* v. *Union of India* [W.P.(C).No. 97 of 2013].

[65] Preamble, *Constitution of India* (1950).

[66] Bureau, *Money laundering charges: HDFC Bank appoints Deloitte to conduct enquiry*, THE HINDU BUSINESS LINE (12 Mar., 2018) *available at*: http://www.thehindubusinessline.com/money-and-banking/money-laundering-charges-hdfc-bank-appoints-deloitte-to-conduct-enquiry/article4515472.ece.

[67] *Id.*

[68] *See, K.Ramajayam @ Appu* v. *The Inspector of Police* 2016 (2) CTC 135; *Syed Asifuddin* v. *State of Andhra Pradesh* 2005 CriLJ 4314; *Shreya Singhal* v. *Union of India* (2013) 12 SCC 73; *Avnish Bajaj* v. *State (NCT of Delhi)* (2005) 116 DLT 427; *Kent RO Systems Ltd & Anr* v. *Amit Kotak & Ors* (2017) 240 DLT 3; *Vyakti Vikas Kendra* v. *Jitender Bagga & Google* AIR 2012 Del 180; *NCT of Delhi* v. *Navjot Sandhu,* (2005) 11 SCC 600; *Tukaram S. Dighole* v. *Manikrao Shivaji Kokate*, (2010) 4 SCC 329; *Anvar P.V.* v. *P.K. Basheer & Ors*, (2014) 10 SCC 473; *Tomaso Bruno* v. *State of U.P.* (2015) 7 SCC 178; *Harpal Singh @ Chhota* v. *State of Punjab,* (2017) 1 SCC 734; *Shafhi Mohammad* v. *State of Himachal Pradesh* (2018) 5 SCC 311; *Arjun Pandit Rao Khotkar* v. *Kailash Kushanrao Gorantyal and others,* (2020) 7 SCC 1.

evidence. The Indian Judiciary very much articulates the interpretation of the law in a number of cases. A few critical cases on the relevancy and admissibility of electronic evidence were handpicked by the researcher, viz.,

NCT of Delhi v. *Navjot Sandhu*[69]

In this case, five heavily armed persons stormed the Parliament House complex and inflicted grievous casualties on the security person on duty. In the Act of waging the war that lasted for more than half an hour, these five terrorists were killed when they tried to enter the Parliament in session. The investigating agency filed the report under Section 173 of CrPC against the four accused. Charges were framed under various sections of Indian Penal Code, the Prevention of Terrorism Act, 2002, and the Explosive Substances Act by the Designated Court.

This case dealt with the proof and admissibility of mobile telephone call records. While considering the appeal against the accused of attacking Parliament, a submission was made on behalf of the accused that no reliance could be placed on the mobile telephone call records because the prosecution had failed to produce the relevant certificate under Section 65B (4) of the Evidence Act.[70] The arguendo raised was that in the absence of a certificate issued under sub-Section (2) of Section 65B of the Evidence Act with the particulars enumerated in clauses (a) to (e), the information contained in the electronic record could not be cited in evidence. In any case, in the absence of examination of a competent witness acquainted with the functioning of the computers during the relevant time and the manner in which the printouts were taken, even secondary evidence under Section 63 is not admissible.[71]

The Supreme Court concluded that cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the way in which the printouts of the call records were taken was sufficient to prove the call records and admissible under section 65A of Indian Evidence Act, 1872.

Anwar P.V. v. *P.K. Basheer And Others*[72]

The facts of this case were related to the assembly election in 2011 in Kerala. In this case, some alleged voices and slogans about election propaganda were recorded by some device which was later copied into a compact disk whose admissibility is in question in the court of law whether it amounts to secondary or primary evidence.

The Supreme Court has settled the controversies arising from the numerous contradictory judgments and the practices being followed in the various High Courts and trial courts regarding the admissibility of electronic evidence. The court has

---

[69] *NCT of Delhi* v. *Navjot Sandhu*, (2005) 11 SCC 600.

[70] See condition provided in S. 65B(4), Indian Evidence Act, 1872.

[71] *NCT of Delhi* v. *Navjot Sandhu*, (2005) 11 SCC 600.

[72] *Anvar P.V.* v. *P.K. Basheer & Ors*, (2014) 10 SCC 473.

interpreted Sections 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 under section 65 B (4) of the Evidence Act. It has been elucidated that electronic evidence without a certificate under section 65B cannot be proved on the basis of oral evidence, and the expert's opinion under section 45A of the Evidence Act cannot be resorted to making such electronic evidence admissible.

The judgment would have severe implications in all cases where the prosecution relies on electronic data, particularly in anti-corruption cases where the reliance is on the audio-video recordings 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 under section 65B of IEA, such CD/DVD has not been admissible in evidence, and the court cannot further investigate expert opinion on its genuineness 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 were more susceptible to tampering, alteration, transposition, excision, etc.; without safeguards, the whole trial based on proof of electronic records could lead to a travesty of justice.

In the anti-corruption cases launched by the C.B.I. and anti-corruption/Vigilance agencies of the State, even the original recording, which was recorded either in Digital Voice Recorders/mobile phones, has not been preserved. Thus, once the original recording was destroyed, there could not 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 was admissible and could not be exhibited into evidence, nor the oral testimony or expert opinion is admissible, and as such, the recording/data in the CD/DVDs could not become a sole basis for the conviction.

In the Judgment, the court held that Section 65B of the Evidence Act is a non-obstante clause[73] and would override the general law on secondary evidence under Sections 63 and 65 of the Evidence Act. Sections 63 and 65 of the Evidence Act have no application to the secondary evidence, which shall be entirely governed by Sections 65A and 65B IEA.

The Constitution Bench of the Supreme Court overruled the judgment laid down in the *State (N.C.T. of Delhi)* v. *Navjot Sandhu alias Afsan Guru*[74]by the two-judge Bench of the Supreme Court. The court specifically observed that the judgment of Navjot Sandhu, to the extent the statement of the law on the admissibility of electronic evidence pertaining to the electronic record of this court, does not lay down the correct position and required to be overruled. The only options to prove the electronic record/evidence is by

[73] *Supra note* 39.

[74] *NCT of Delhi* v. *Navjot Sandhu* (2005) 11 SCC 600.

producing the original electronic media as Primary Evidence court or its copy by way of secondary evidence under sections 65A and 65B of IEA. Thus, in the case of CD, DVD, Memory Card, and other digital devices 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.

Harpal Singh @ Chhota v. *State of Punjab*[75]

In the present case, the principle of S. 65 B was reiterated, i.e., the certificate requirement is mandatory under section 65B of the Indian Evidence Act, 1872[76]. In this case, evidence related to incriminating call (relating to conspiracy to abduct for ransom) details was in question and sought to be proved on the basis of a printed copy of computer-generated call details. However, the prosecution failed to comply with the certificate relatable thereto as required under S 65 B of the Act. The court, in this case, held that such evidence is not admissible in the court of law as the position is clear after the *Anvar P.V.* v. *P.K. Basheer*[77] case, while the conviction is held valid on other evidence purporting to the crime.

Shafhi Mohammad v. *State of Himachal Pradesh*[78]

In the present case, the admissibility of the videography of the crime scene during the investigation by the Police was in question whether it was admissible under section 65B of IEA and its subsequent requirement of the certificate under clause (4),[79] as the party had not fulfilled the certificate requirement. The court passed an order dated 30.01.2018[80] and held that the applicability of the procedural requirement under the Act of furnishing certificate is to be applied only when such electronic evidence is produced by a person who can produce such certificate being in control of the said device and not of the opposite party.

Accordingly, the court elucidated the legal position on the admissibility of electronic evidence, especially when a party has not possessed the device from which the document was produced. The such party could not be required to produce a certificate under section 65 B (4) of IEA. The court further held that the requirement of the

---

[75] *Harpal Singh @ Chhota* v. *State of Punjab,* (2017) 1 SCC 734.

[76] *See supra note* 39.

[77] *Anvar P.V* v. *P.K. Basheer & Ors*, (2014) 10 SCC 473.

[78] *Shafhi Mohammad* v. *State of Himachal Pradesh* (2018) 5 SCC 311.

[79] *See supra note* 39.

[80] *Shafhi Mohammad* v. *State of Himachal Pradesh* (2018) 2 SCC 801

certificate, being procedural in nature, could be relaxed by the court wherever the interest of justice so justifies.[81] The division bench also observed that:

> *"New techniques and devices are the order of the day. Though such devices are susceptible to tempering, no exhaustive rule could be laid down by which the admission of such evidence may be judged. Standard of proof of its authenticity and accuracy has to be more stringent than other documentary evidence."*[82]

Arjun Pandit Rao Khotkar v. *Kailash Kushanrao Gorantyal and Others*[83]

In this landmark judgment on the admissibility of the electronic evidence, the full bench decided *per curiam* that the requirement to furnish the certificate under Section 65B of the IEA, 1872 has mandatory and could not be waived away with as decided by the division bench in *Shafhi Mohammad* case. The facts of the case were that the appellant won the State Legislative Assembly elections and the respondent, aggrieved from the election result, challenged the appellant's nomination on the ground that the Returning Officer had improperly accepted the nomination paper after the cut-off time, i.e., after 3.00 p.m. on 27-9-2014. The respondents had requested the video of arrangements made within and outside Returning Officer's Office. The Election Commission had produced Video Compact Disks (VCDs) before the Court. The R.O.'s office had yet to furnish a certificate under Section 65-B (4) of the Act along with the VCDs, but the RO refused to do so even after the respondents had made a request. During the trial, the returning officer had given his statement on oath regarding the validity of the records before the court. The High Court declared the elections null and void, relying on the evidence produced by the respondents. The appellant challenged it before the Supreme Court of India on the admissibility of electronic evidence in India under IEA.

In the present case, the Supreme Court had confirmed the decision of the *Anvar P.V.* case[84] and per incuriam the decision of the Shafhi Mohammad case[85]and held that said certificate is mandatory for all the cases where the primary (original) electronic record cannot be produced before the court. The oath of the person handling and operating the device has been considered invalid regarding the certificate mandates. The Supreme Court also entered a caveat on the impossibility of furnishing the said certificate by applying two Latin maxims, i.e. *lex non cogit ad immpossiblia* and *impotentia excusat legem*,

---

[81] See also, Yuvraj P. Narvankar, *Recent Judgement Of The Supreme Court In Arjun Khotkar: A Missed Opportunity To Revisit 65B*, *available at*: https://www.livelaw.in/columns/recent-judgement-of-the-supreme-court-in-arjun-khotkar-a-missed-opportunity-to-revisit-65b-160201 (last visited 20 Jul., 2020).

[82] See also, *Tukaram S. Dighole* v. *Manikrao Shivaji Kokate*, (2010) 4 SCC 329; *Tomaso Bruno* v. *State of U.P.* (2015) 7 SCC 178; *R.* v. *Robson*, (1972) 2 All ER 699.

[83] *Arjun Pandit Rao Khotkar* v. *Kailash Kushanrao Gorantyal and others,* (2020) 7 SCC 1.

[84] *Anvar P.V.* v. *P.K. Basheer & Ors*, (2014) 10 SCC 473.

[85] *Shafhi Mohammad* v. *State of Himachal Pradesh* (2018) 5 SCC 311.

which means law, does not demand the impossible and inability excuses the law, respectively.[86]

V

Conclusion

While the Information Technology Act 2000 has addressed cyber security breaches & crimes, thus providing a basic structure of Indian Cyber Law, the rapidly progressing technological advancements coupled with the underdeveloped forensic tools, evidentiary procedures & suitably trained personnel bring into light the need for a comprehensive & holistic legal framework & machinery to meet the challenges of the E-world.

Cyber forensics, still at a nascent stage in India and as a subset of the enforcement machinery of cyber law, requires the systematic development and encapsulation of the most effective practices for a fair and better trial in criminal cases. Technological development is happening at light speed. The crimes have changed their pattern, and technology is also helping to find out the real accused. Digital evidence is become vital to decide the truth. The digital evidence and the admissibility of digital evidence are crucial for the prosecution to prove their case, and if it is difficult to do so, then it is almost impossible to prove the case beyond a reasonable doubt in the absence of solid evidence against it the accused. The legislative framework has done much, but that is not the end but rather a beginning to transform ours as technological advances and the nature of crimes evolved. The Supreme Court interpret the existing law on electronic evidence in the best possible way, but there will be a need to reform our existing laws along with latest trends in the law and technology. The Indian approach to cyber forensics portrays a dismal picture of indifference coupled with overturned institutions and staff, which need to be remedied to achieve the broader goals of criminal prosecution.

---

[86] *Supra note* at 83, paragraph 47.