International Journal of Management and Humanities (IJMH)
ISSN: 2394-0913 (Online), Volume-4 Issue-7, March 2020

Admissibility of Electronic Evidence under the Indian Evidence Act, 1872

Soni Lavin Valecha, Sonika Bhardwaj

Abstract: ***Information Technology or computerization is playing a vital role in various fields like business, communication, services, government sector etc. Also it has left its impression on judicial system & existing laws in India. The IT Act made several reforms in regulations such as the Indian Penal Code of 1860, the Indian Proof Act of 1872, the Reserve Bank of India Act of 1934 etc. The word proof can be described as evidence that helps to explain or refute a truth. The information technology Act 2000 is intended to understand the moral sanctity and structure of electronic records, which may include witness testimonies, notes, etc. Some changes are required to accept the electronic records as facts in the Evidence Act. In the light of section 65-A of the Indian Evidence Act, 1872, Indian courts provide electronic records. Section 65 B of the Indian Evidence Act 1872 specifies the framework for the filing of electronic records as evidence. According to Section 65-B of the Indian Evidence Act, 1871, the report shall be considered any data found in the electronic records of the written, discharged or replicated machine system, and may be permitted to provide evidence in any process which continues without the confirmation of the initial. It is era of speedy and faster communication, the use of internet and information technology is common among people. Nevertheless, the admissibility of the Act is subject to different provisions laid down in section 65-B of that act. So, with this paper I will be determining the extent of implementation of amended laws of Information Technology Act, 2000 with reference to Evidence Act, 1872.***

Keywords: Computer System, Electronic Evidence, I.T. Act, Information Technology

I. INTRODUCTION

The 21st century have seen a technological revolution that fascinated the whole world as well as India. The creation of IT created a cyber world in which Internet offers every person equal opportunities to access, store data, analyze etc. with high-tech applications, all of which can be accessed by means of the Web. This increased dependence on electronic correspondence, online enterprise and data capacity in advanced structures has certainly led to a change to legislation that identifies both common as well as criminal issues in India with data innovation, and rules on the tolerance of electronic data.

The changes to the 1872 Indian Evidence Act, the 1860 Indian Penal Code and the 1891 Banker Buch Evidences Act provide a legislative framework for e-world operations.

Indian courts have developed case law with respect to relying on online data with the transition to the rule.

Revised Manuscript Received on March 05, 2020.
***** Correspondence Author
Soni Lavin Valecha*, Master of Law (Corporate and Commercial Laws), Christ (Deemed to be **University**), Bengaluru, India. Email: Lavinvalecha01@gmail.com
Sonika Bhardwaj, School of Law, Christ (Deemed to be University), Bengaluru, India. Email: sonika.bhardwaj@christuniversity.in

In addition, judges showed perceptiveness of the typical "such" existence of testimony, which requires an appreciation of the acceptability of such proof and incorporation into law regarding the means of bringing and recording electronic information under a court's watchful eye[1]. All probative documents which are installed or distributed in a computerized system and may be used in advance by the judicial process is tangible information or electronic proof. It is important that the Court will figure out its value, truthfulness and truthfulness before tolerating computerized facts and if the fact is noise or repeat. Electronic proof is "fact meaning data that is omitted or passed on in a paired system."

Evidence isn't just restricted to that found on computers however may likewise stretch out to remember evidence for advanced gadgets, for example, media transmission or electronic interactive media gadgets. The e-EVIDENCE can be found in messages, computerized photos, ATM exchange logs, word preparing, reports, text documentaries, records spared from bookkeeping programs, spreadsheets, web program accounts databases, Computer memory material, server upgrading, database printouts, Global monitor positioning system, Inn's electronic entrance keys, digital video or sound recordings, database information. In general, computerized proof is growing, progressively difficult to spray, efficiently adjusted, copied, perhaps more expressive and all the quicker accessible.[2].

II. MEANING OF ELECTRONIC EVIDENCE

The kind of proof we handle is presented differently as "electronic evidence," "advanced evidence" or "digital evidence." The word computerized is regularly utilized in figuring and hardware, particularly where physical-world data is changed over to twofold numeric structure as in advanced sound and advanced photography[3]. Meanings of digital evidence incorporate 'Data of probative worth put away or transmitted in paired structure; and 'Data put away or sent to the courtroom in double form. While the word ' computerized,' as you can see, is unnecessarily prohibitive to use' parallel,' considering that it only represents one sort of information. E-evidence: data that is monitored extracted or distributed, by any man-made machine, program or network system, through a communications process (including the performance of analog devices or data in digital format

[1]Tejas Karia, Akhil Anand and Bahaar Dhawan, The Supreme Court of India re-defines admissibility of electronic evidence in India.
[2] https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali-, (last accessed 28 Nov 2019)
[3] Dr. Swaroopa Dholam, Electronic Evidence and its Challenges

That can possibly make the truthful record of either party more plausible or less likely than it would be without the evidence[4].

This definition has three components. To begin with, it is planned to incorporate all types of evidence that is made, controlled or put away in an item that can, in its most extensive importance, be viewed as a computer, barring for the time being the human mind.

Second, it means to incorporate the different types of gadgets by which information can be put away or transmitted, including simple gadgets that produce a output. Preferably, this definition will incorporate any type of gadget, regardless of whether it is a computer as we directly comprehend the significance of a computer; phone frameworks, remote broadcast communications frameworks and systems, for example, the Internet; and computer frameworks that are implanted into a gadget, for example, cell phones, savvy cards and route frameworks.

The third component confines the information to data that is essential to the process by which a dispute is chosen by a hearing officer regardless of the form and degree of consultation regardless of the concept of distinction. That definition includes one element-just validity-but does not use the "suitability" as a standard condition as a consequence of certain proof being allowed but still denied in the dissemination of its role by the adjudicator or forbidden for purposes that have nothing to do with the principle of evidence, e.g. because of the manner in which I was provided. The final requirement is that the importance of written documentation be restricted to what the meetings offer as a major aspect of the process of discovery of fact.[5]

Despite the enormous growth of electronic administration throughout the federal, private and Web-based business activities, the main elements of communications, planning and reporting have been electronic evidence. The administration organizations are opening up to present different administration provisions digital and regular reports are rendered using automated tools for the administration and regulation of businesses. Such different forms of online evidence / digital proof are being used progressively in legal proceedings. At the preliminary stage, judges are often required to assess the acceptability of electrical proof and the outcome of the common claim or conviction / exemption of the accused are significantly affected. The new electronic frontier tends to be regarded by the Court as the one kind of testimony, just as the ease of processing or misrepresentation of it does not impede acceptability of various confirmations. For eg, different types of electronic evidence such as cd, DVD, memory / plate records, site details, communications with informal organizations, e-mails, speaking time notes, SMS / MMS and PC documentation are subject to a specific problem and challenge to be checked properly and subject to alternatives.

III. ELECTRONIC EVIDENCE AND THE INDIAN EVIDENCE ACT

A) the evidences of witnesses, i.e. oral proof, and b) documentary evidence, including electronic records created for the court's examination, as contained in the Indian Evidence Act, 1872.[6] Section 3 of the Act was amended and the phrase “All documents produced for the inspection of the Court” was substituted by “All documents including electronic records produced for the inspection of the Court[7]”. With respect to documentary evidence, the words ' information for documentation' with Section 59 have been substituted by the terms ' material of documents or digital records,' with the intention of adding electronic evidence in Section 65A & 65B. The basic rule of proof is generally that all truth, except documents, may be proven explicitly orally. The law of the hearsay means, unless one of the provisions listed in Sections 59 and 60 of the Evidence Act related to the testimony procedure is preserved, any oral evidence that is not clear can be relief. Nevertheless, in the case of records the law of hearsay is not as stringent or clear as in the case of oral testimony. Since oral testimony can not show the substance of a text and the document speaks for itself. In the case of absence of a record, however, oral proof of the document's authenticity cannot be produced and the contents of the document cannot be measured. It would disrupt this law of the hearsay (because there is no text, it cannot be contrasted with the facts or the quality of the oral proofs). Whether primary or secondary evidence must be given in order to prove the substance of a text?

While it is actually the database that is vital proof, it was known that conditions were not practicable to obtain critical evidence. For compliance with the Evidence Act (Area 63) for purposes to show the content of a document, discretionary proof as assured duplicates of the data, duplicates produced through automated processes and oral accounts of somebody seeing the documentation have been approved. The agreement to require the optional proof in a way weakens the prattle rule requirements and seeks to address the problems associated with ensuring that the documentary evidence is necessary where the first is inaccessible. Area 65 of the Proof Law provides conditions under which necessary proof of the database must not be provided and optional evidence can be marketed, as stated in Section 63 of the Evidence Law. It requires criteria in the first paper-

i. “Should be in hostile possession.
ii. Or has been proved by the prejudiced party itself or any of its representatives.
iii. Is lost or destroyed.
iv. Cannot be easily moved, i.e. physically brought to the court.
v. Is a public document of the state.
vi. Can be proved by certified copies when the law narrowly permits; and
vii. Is a collection of several documents.”[8]

IV. ELECTRONIC DOCUMENT

The noise law faced a few new challenges, when records became digitized. Although the legislation foresaw most of

[4] Ibid.
[5] Burkhard Schafer and Stephen Mason, The characteristics of electronic evidence in digital format, in Electronic Evidence, LexisNexis, 2013.
[6] Section 3 of the Indian Evidence Act, 1872.
[7] Ibid.
[8] Manisha T. Karia and Tejas D. Karia, ‘India’ (Chapter 13) in Stephen Mason, ed, Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012).

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

the basics (the first study itself, for instance) and offered exceptional requirements for the secondary facts, that digitisation meant the electronic disappearance of an ever-increasing number of documents. Therefore, indirect confirmation exposure to media has grown. In the Anvar case, the Supreme Court noticed that "there is an upset in how evidence is delivered under the steady gaze of the court. In India before 2000, electronically put away data was treated as an document and secondary evidence of these electronic 'documents' was cited through printed proliferations or transcripts, the credibility of which was guaranteed by an able signatory. The signatory would distinguish her mark in court and be available to interrogation. This straightforward technique met the states of the two sections 63 and 65 of the Evidence Act. Thusly, Indian courts basically adjusted a law drafted more than one century sooner in Victorian England. Be that as it may, as the pace and expansion of innovation extended, and as the creation and capacity of electronic data developed increasingly perplexing, the law needed to change all the more generously. The "record or content of records" is not supplemented by "Electronic documentation or substance of electronic documents" in compliance with Section 61 to 65 of the Indian Evidence Act of 1872. In accordance with this purpose, for example, it is explicitly clear that the legislative body does not apply the suitability of section 61 to 65 to the electronic record.

If the law has prohibited the use of a single word, it is the cardinal rule for translation that the omission is intentional. It is very clear that no word is being used in vain by the Law[9]. In such manner, the Apex Court in Utkal Contractors and Joinery Pvt. Ltd. v. Territory of Orissa[10] held that "...Likewise, Parliament is not to express in vain what it wants. Even though Parliament chooses something useless in no terms, Parliament does not follow where no law is needed. With reality, Parliament does not. Parliament cannot be permitted to legislate; nor can it simply declare what is meaningless to say, or do what is legally done at present. Parliament cannot be allowed to administer improperly."

The IT Act modified Section 59 of the Evidence Act 1872 in order to preclude electronic records from being evidence-based in the same manner as documentation had been prohibited. This is the reuse of the electronic records hearsay statute. Nevertheless, the Law introduced two additional evidentiary guiding principles on electronic records into Evidence Act, Section 65A and Section 65B, rather than the use of electronic records for checking supplementary evidence, found in Sections 63 and 65 for reportages. In fact, as the information in the electronic structure cannot be produced in the court room due to the computer / server scale, houses in machine language, and along certain lines, which allow the reader to analyze it. The legislative authority aims at providing a specific law that has its origin in advanced understanding of proof. Section 65A of the Evidence Act offers extraordinary electronic evidence legislation-Electronic proof material may be defined in compliance with section 65b provisions[11]. Each field has a similar capacity for electronic records as documentary evidence is given in section 61: a different strategy to insure that electronic record adduction complies with the law of the gossip, in particular the transparent method for oral testimony. It also tests the validity of creativity and the sacredness of the process of data recovery, for instance. In all cases, section 65A is further recognized because in articles 63 and 65 it is a unique law separate from the procedure on documentary evidence..

The particular method for the proofing of electronic documents is outlined in Section 65B of the Evidence Act. Sub-section (2) lists the technical requirements under which a copy (including a print-out)of an original electronic record may be used :

i. The computer generated must be in operation daily when producing the electronic record,

ii. The details in the electronic record must have been fed to the computer frequently and regularly,

iii. The computer worked correctly; and,

iv. A backup of the actual electronic record must be replicated.

The secondary copy, like printing or reproduced material on electronic / attractive platforms, is allowed as part of Section 65B of the Evidence Act. It provides[12]: “Notwithstanding anything contained in this Act, any data contained in an electronic record which is imprinted on a paper, put away, recorded or duplicated in optical or attractive media, created by a computer will be considered to be additionally a document, if the conditions referenced in this section are fulfilled in connection to the data and computer being referred to and will be permissible in any procedures, moving forward without any more verification or generation of the first, as evidence of any substance of the first or of any reality expressed in that of which direct evidence would be acceptable.”

A. Sec. 65B(2)

The computer through which the documents are produced has frequently been used to gather or process information regarding actions conducted daily by an individual with legal control over the time which refers to the duration of routine use of the device. The data has been transmitted to the database in the regular course of operation of the person with legal control over the computer.[13]

B. Sec.65 B(3)

The following computers are arranged as a single computer

a. By a combination of computers that run during that time ; or

b. By different computers running successively over that time ; or

c. By different combinations of consecutive computers over that span ; or

d. In any other way that involves the continual activity, in whatever sequence, of one or more e over that span. In any

[9] Prashanti, E-Evidence in India, www.legalservicesindia.com, (last accessed on 28/11/2019)

[10] Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa reported as AIR 1987 SC 1454

[11] Section 65-A of the Indian evidence Act, 1872: Special provisions as to evidence relating to electronic record.

[12] Section 65B provides for ‘Admissibility of Electronic Records

[13] Section 65 B (2) of the Indian Evidence Act, 1872 lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

other form involving the continual activity of one or more computers and one or more combinations of computers over that time, in whatever order.

C. Sec. 65B(4)

This includes the certificate for the individual who can grant the certificate and the contents of the certificate doing one of the following things: defining the electronic record comprising the declaration and explaining the manner in which it was created; Providing the particulars of the equipment related to any of the matters relating to the requirements referred to in subsection (2) and purporting to be certified by a person holding a qualified official position in relation to the activity of the particular system or the management of the specific activities (whatever the case may be) shall be proof of any subject referred to in the certificate and for the purposes of the certificate.[14] The point is further strengthened by the incorporation terms "Notwithstanding everything found in this Act" in Section 65A & 65B, which is a non-discriminatory provision, further reinforces the fact that only Section 65A & 65B is intended by the legislation to create or show electronic records. To order to give the enacting portion of the Act, in the event of a conflict, an overarching influence over the section in the same or any other act referred to in the nonmpre clause, a non embargo clause is usually appended to a Section. It is equivalent to saying that, given the clauses or actions alluded to in the non-discrimination clause, the law that occurs must function in full or the provisions included in the non-discrimination clause will not hinder the implementation of the statute or the system in which the non-discrimination clause takes place. The aforesaid principles of interpretation with respect to the non obstante clause in form of “Notwithstanding anything contained in this Act” is further supported by the Hon’ble Apex Court in Union of India and Anr., v. G.M. Kokil and Ors[15]. Observed "It is well recognized that a non-discriminatory clause is a legislative device generally used for overriding the presence and the implications of all the competing clauses in order to give effect to certain adverse laws which can either be found in that Act or some other law.”[16] Further, the Hon’ble Apex Court in the case cited as Chandavarkar Sita Ratna Rao v. Ashalata S. Guram[17], Explained as 'it is equal to stating it would work in full in the light of the provisions of the Act or any other Legislation specified in the Non-Discrimination Clause, or any other agreements or documentation referred to thereafter.”[18]

V. NEW FORMS OF EVIDENCE

Although the structures in which evidence exists can not be restricted, they have been widely ordered in oral and narrative form to date. For example, documentary evidence could, in general, be put on paper-statements and executed documents, pictures, maps, characters, etc. When documents on articles, such as tapes and gramophone circles, began to be made, they also began to become archives.

In February 2010, a terrorist attack in a popular bakery has recently threatened the city of Pune. Eventually, on the basis of the CCTV footage, the German Bakery bombings suspected were confirmed by the authorities. There is therefore a question of whether such a recording, which is not available in any tangible way either on the paper or on the negative camera or on the magnetic tape, can actually be presented as proof. The only proof that is possible is that that the CCTV device is regulated in the computer system.

This description illustrates the extraordinarily late excitement of the growing usage of machines in everyday life. With the web bureau now generally accessible to compose letters, there are an increasing number of agreements on the web. Consequently, individuals would now be able to arrange items on the web, and the merchants will deliver the dispatch over, the installment being made through e-banking. A chief and entertainer may go into an agreement with respect to a film through messages. A person interviewed by messages may assert the chief executive officer of an organization's form of employment. Any kind of correspondence and agreement that previously occurred in person or via letters could now be done via the web. In this way, the principal supporting proof would be the content of the messages if any of the agreements were to sue each other for breaking agreement.

Innovation is also used to construct offenses on the other side of the range. The horrific event of the terrifying assaults in Mumbai in 2008 showed how psychological activists today are versed and how they profit from creativity. Voice over Internet Protocol (VOIP), which makes transfers through the Western Union Money Transfer, had been obtained by the psychological oppressor controllers to keep contact with the aggressors and send them orders from Pakistan. The subtleties of the network transactions are proved by the court of law.

VI. CLASSIFICATION OF ELECTRONIC EVIDENCE

The Indian Evidence Act requires any material on which subject matter has been mentioned or portrayed to be called a text, implying that this is why it has been recorded or defined. Any records, document or data produced, picture or sound recorded, obtained or sent in electronic form, or the microfilm or the machine-generated microfiles, were specified in the information technology law in the year 2000. The electronic database can be accessed in a safe manner, as the question can be linked to statistics or tests on the computers as bits and bytes.

Computer records were commonly seen as gossip articulations since any evidence obtained from a software consists of information provided by a human person. Therefore, irrespective of whether it was a word archive of declaration comprising of one set or a picture of a person missing from a database depending from inputs, all those records will be gossiped.

[14] Section 65B (4) of the Evidence Act lists additional non-technical qualifying conditions to establish the authenticity of electronic evidence. This provision requires the production of a certificate by a senior person who was responsible for the computer on which the electronic record was created, or is stored. The certificate must uniquely identify the original electronic record, describe the manner of its creation, describe the device that created it, and certify compliance with the technological conditions of sub-section (2) of section 65B.

[15] [(1984)SCR196].

[16] Vivek Dubey, Admissibility of Electronic Evidence: An Indian Perspective,Volume 4 Issue 2 - 2017

[17] [(1986)3SCR866].

[18] Supra n.16

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Whether a record in a computerized system is an imprint from the original would include an electronic record. What is deliberately registered is a serious meaning database, yet no one who doesn't use the machine frame to which the documents were first. Therefore, if music creator A mixed up some of its songs, and another arranger, B, had to prosecute him for a breach of copyright, B wouldn't touch computerized records on A's digit. Despite the fact that an enticing repository such as the conservative circle (CD) can be graved, it would assume to be open to A's machine in any event. Everyone can see an index that includes a written version with computer records. Such archival copying will lead to additional evidence that the requirements of the Indian Evidence Act are treated carefully.

The extreme meaning of electronic information has been given as true proof, i.e. substantive data; nevertheless, such evidence needs clarification of the machine's dependability for validation.

VII. EFFECTS OF CONSIDERING ELECTRONIC EVIDENCE AS PRIMARY AND DIRECT

A. Blurring The Difference Between Primary and Secondary Evidence

The resolution strongly masks the distinction between primary and secondary forms of evidence by integrating any kind of electronic data into the overlay of primary evidence. Although the topic surrounding different types of documentation is still required to continue, a special case involving computers has been created. This, be that as it may, is fundamental, given the entangled idea of computer evidence as far as not being effectively producible in unmistakable structure. Along these lines, while it might make for a decent contention to state that on the off chance that the word document is the first, at that point a print out of the equivalent ought to be treated as secondary evidence, it ought to be viewed as that creating a word document in court without the guide of print outs or CDs isn't simply troublesome, however very unimaginable.

B. Making Criminal Prosecution Easier

Considering the ongoing spate of fear based oppression on the planet, including psychological oppressors utilizing profoundly complex innovation to do assaults, it is of incredible assistance to the arraignment to have the option to create electronic data as basic and key proof at trial, because it showed that the responsibility for its argument far surpassed that of reaching for traditional forms of proof that could in any situation not override electronic records. As we have seen in the case of Ajmal Kasab, psychological oppressors today schedule any exercise in relation to it or through programming. Having the option to create transcripts of web exchanges helped the arraignment case a lot in demonstrating the blame of the charged.

C. Risk Of Manipulation

The decision also underestimated the possibility of restricting when requiring certain forms of device performance to be included as critical proof. The brass with electronic evidence is not particularly troubling and the villagers may believe that the documents to be submitted in courts are easy to change. In all cases, creativity itself has answers to these questions. The rule of computers has evolved enough to find methods to test when, where and in what respects an online record is being messed up.

D. Opening Potential Floodgates

Computers are the most generally utilized contraption today. A great deal of different contraptions include computers contributes their working. Along these lines, the extent of Section 65A and 65B is to be sure extremely enormous. Every gadget, including a computer chip, should be adducible in court as evidence, if the rule is articulated carefully. In any case, relevant observations of the same moral nature should be given high priority before giving an ability to flow to the reach of these parts. The Supreme Court has declared, for example, that the study results of narco-research are excluded as facts because of dama.

VIII. NON-APPLICATION THE SPECIAL LEGAL PROVISIONS.

No use was made of the rare statute and procedure provided for electronic proof under section 65A and 65B of the Proof Act. The explanation for this non-use disappointingly does not include the regulation at all[19]. India's lower legal executive, the third level of courts where preliminary proceedings are being tried, is inconceivably uncouth and innovatively unhealthy. Despite loopholes, preliminary judges don't really have the foggiest idea of the creativity that the IT Act grasps. Continuing with electronically dismissing data as narrative evidence is simpler. In India, the reasons behind that are basic and, I suppose, common to poor nations that produce them. India's equity system is weak and financially inefficient. Whatever the length of time the legal framework is not updated, India's preliminary judges may remain unaware of online proof and procedures to ensure validity. Through bypassing the special legislation on electronic records, Indian courts have proceeded to enforce the provisions set out in sections 63 and 65 of the Evidence Act to electronically transmit evidence, which refer to papers. Areas 65A and 65B of the Evidence Act were largely ignored by the courts. Inquisitively, this situation was honored by the Supreme Court in Navjot Sandhu (the Parliament Attacks case)[20], that was a particularly prominent early mystery from moral psychological deprivation. On the topic of the guard's check of the genuineness and authenticity of certain call information records (CDRs) that relied on the arraignment, which were identified as generations of the first records that were electronically deleted, a Division Bench of Justice P. Venkatarama Reddi and Justice P. P. Naolekar held.

As mentioned in Section 63, secondary evidence methods and integrates, as well as other elements, "duplicates created using the first by technological procedures which in

[19] Prior to 2000 in India, electronically stored information was dealt with as a document, and secondary evidence of electronic records were adduced as ‘documents’ in accordance with section 63 of the Evidence Act.

[20] (2005) 11 SCC 600

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

themselves guarantee the accuracy of the copy, and contrasted copies and such copies." Section 65 empowers secondary evidence of a report's content to be shown if the first is of such a nature as not to be easily portable. It is not in doubt that the data contained in the call records are put away in giant databases that can't be moved and generated successfully in litigation. That is the aspect the High Court also saw at paragraph 276. Subsequently, printouts taken from the computers / servers through mechanical method and checked by a cautious authority of the administration supplying agency may be observed by an analyst who can identify the markings of the guarantor or, in general, tackle the realities depending on his information[21].

IX. RESULTS

Many individuals who want posts, forums or online records in a civil or criminal preliminary are currently required to comply with section 65B under steady eyes of the Indian courts. The Indian Supreme Court has this task to ensure that electronic data reliability and accurate verification are regarded as electronic records are more prone to alteration and adjustment.

The electronic record generated by the computer cannot be relied entirely on, provided that there is a possibility that it will be hindered. In addition, the Indian Evidence Act could be modified to prohibit some interference-in any case for the purposes behind believing at first sight the validity of the electronic record evidence-by including a provision that the record was created in the standard way by a person who was not involved in the procedures and that the record protector did not control the record production Through ensuring that the record was documented by a meeting that was antagonistic to the record supporter and that the record was used against the adverse faction, the likelihood of record ownership would be substantially reduced.

The statute should also contend inventively with the need for the weight of the defender to indicate with the author of a report whether the records were checked or updated or whether the computer program that created them had reliable data, and whether they were finished or not. The courts must also ensure the evidence is properly generated or modified, which is not covered by Section 65B of the Evidence Act. For examples, the sender will modify the message while transmitting an e-mail. These adjustments are often not noticed by the receiver, and in this way an outside witness to the matter may not necessarily be a good condition for the record to match the facts.

X. CONCLUSION

India still has a long way to go to keep pace with the developments all inclusive of its issues with suitability and appraisal for electronic proof. Although the reforms were considered to reduce the weight of the consumer, they cannot be said to be without limitations. Actually, India cannot seem to formulate a mechanism to guarantee the veracity of electronic records which can be monitored by a database through obtaining access to the server or room where it is located.

At the same time it can also be perplexing to validate online proof together with focal points. The courts must insure that the testimony satisfies the three basic, legal standards of integrity, unchanging quality and reliability. After the Supreme Court's decision on the Anvars case laying down the standards of electronic evidence tolerability, it is not uncommon for the Indian courts to provide a reliable solution and conduct any possible appeal for electronic evidence toleration and recognition.

REFERENCES

1. Tejas Karia, Akhil Anand and Bahaar Dhawan, The Supreme Court of India re-defines admissibility of electronic evidence in India.
2. https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali-, (last accessed 28 Nov 2019)
3. Dr. Swaroopa Dholam, Electronic Evidence and its Challenges
4. Burkhard Schafer and Stephen Mason, The characteristics of electronic evidence in digital format, in Electronic Evidence, LexisNexis, 2013
5. Section 3 of the Indian Evidence Act, 1872
6. Manisha T. Karia and Tejas D. Karia, 'India' (Chapter 13) in Stephen Mason, ed, Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012).
7. Prashanti, E-Evidence in India, www.legalservicesindia.com, (last accessed on 28/11/2019)
8. Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa reported as AIR 1987 SC 1454
9. Section 65-A of the Indian evidence Act, 1872: Special provisions as to evidence relating to electronic record.
10. Section 65B provides for 'Admissibility of Electronic Records
11. Section 65 B (2) of the Indian Evidence Act, 1872 lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used.
12. Section 65B (4) of the Evidence Act lists additional non-technical qualifying conditions to establish the authenticity of electronic evidence. This provision requires the production of a certificate by a senior person who was responsible for the computer on which the electronic record was created, or is stored. The certificate must uniquely identify the original electronic record, describe the manner of its creation, describe the device that created it, and certify compliance with the technological conditions of sub-section (2) of section 65B.
13. [(1984) SCR196].
14. Vivek Dubey, Admissibility of Electronic Evidence: An Indian Perspective, Volume 4 Issue 2 – 2017
15. [(1986)3SCR866].
16. (2005) 11 SCC 600
17. www.cidap.gov.in/.../State_(N.C.T._Of_Delhi)_vs_Navjot_ Sandhu@_Afsan_Guru, (Last accessed on 28/11/2019) Som Prakash vs. State Of Delhi AIR 1974 SC 989, 1974 Cri. LJ 784, MANU/ SC/0213/1974

AUTHORS PROFILE

Soni Lavin Valecha, pursuing Masters of Law on Corporate and Commercial Laws, from Christ School of Law. Has presented papers and attended various Seminars on contemporary issues, also successfully completed various proposals and research work in the field of law, I.T. Act, Companies Act etc. I am an active member in various academic and cultural activities which takes place in or outside my college. I was President of moot court committee in my College where I pursued my Under Graduate studies. I have good public speaking and leadership skills, and I always look forward and always want to learn and polish my skills.

Dr. Sonika Bhardwaj, Assistant Professor, School of Law, Christ (Deemed to be University), Bengaluru, Karnataka. I have teaching experience of 15 years. I have published 14 papers and attended around 15 conferences by now.

[21]www.cidap.gov.in/.../State_(N.C.T._Of_Delhi)_vs_Navjot_ Sandhu@_Afsan_Guru, (Last accessed on 28/11/2019) Som Prakash vs. State Of Delhi AIR 1974 SC 989, 1974 Cri. LJ 784, MANU/ SC/0213/1974.