`The Admissibility of Electronic Evidence and its Impending Challenges in Bangladesh: A Comprehensive Study

Rafea Khatun*

Abstract: It is well experienced that human civilization is now in an era where everything is digitalizing and shifting towards electronic means and internet-based like e-mail, e-judiciary, e-communication, online shopping, online classes, and many more. Consequently, most of the disputes are now connected with these e-forums. Besides, in the fast technological advancement, most of the facts are being recorded through internet-based technologies such as audio-video recording and photo taking through cell phones, CCTV footage, etc. To solve these disagreements, investigation authorities often need to consider various types of e-evidences that include both analog electronic and digital electronic evidence. The Evidence Act 1872, which is ancient colonial legislation, does not comply with the current needs. Against this backdrop, this study aims to examine the justification of the present eminence of admissibility of e-evidences in our investigations and inquiries under the general and special laws on evidence. Also, this research will examine the lacunae in the existing legislation and practices and will provide some prospective recommendations. This will also be within the periphery of this research to chalk out the impendent challenges faced by our judiciary in adopting e-evidences.

Keywords: E-evidence, digital evidence, relevancy, admissibility, and digital forensics.

1. Introduction

Electronic evidence has ably reformed voluminous aspects of contemporary issues in the litigation process. In our daily lives, electronic communications are being persistently used by texting, emailing, and using social media – and there's an online record of everything in the cloud, on a company's servers and hard drives. Nowadays, the manifestation of outcomes of crimes or civil disputes is directly or indirectly allied with various electronic mediums. To establish criminal responsibility or to solve civil rows, it is needed to take assistance from numerous types of evidence associated with electronic technologies. Nonetheless, the dream of 'VISION 2021' to achieve a digital Bangladesh is almost popularized, there is no comprehensive special law on the admissibility of electronic evidence. However, as one of the constitutional organs, digital Bangladesh will not be accomplished without a functional digital judiciary. Additionally, one proverb goes like this,

* Assistant professor at the Department of Land Management and Law, Jagannath University. The author is available at: rafeakhatunratna@yahoo.com

justice delayed justice denied. The restricted number of judges in proportion to a huge number of cases and the age-old procedural laws for proving the cases also make justice in vain when getting it. Besides the incorporation of provisions of digital evidence, preparation should be taken to tackle the future challenges of using electronic evidence by the investigation and the judicial authority for getting the ultimate utility of electronic evidence. It is projected that this paper will be backfiring for the concerned authority to espouse new legislation and to amend the existing legislation for admitting electronic evidence exhaustively. Moreover, ascribed challenges and ways forward will ease the implantation of electronic evidence legislation in our courts for safeguarding better access to justice in Bangladesh.

In this paper, mainly the doctrinal qualitative research methodology has been followed to analyze the existing legislation and judicial decisions for finding out the actual legal status of the admissibility of e-evidences in our country. Additionally, this paper applied a comparative qualitative research design to examine the mechanisms followed by some developing and developed countries to support the research's hypothecation. In the case of following both of the above methodologies, some judicial decisions from home and abroad have been illustrated. Furthermore, data's been collected both from primary and secondary sources. The researcher accumulated some data from the experiences of some law professionals such as judges, lawyers, other investigating authorities and experts in technological sciences.

2. Concept of E-evidence

Generally, evidence means anything by which any assertion or denial can be proved or disproved in a trial. Evidence has defined as "information drawn from personal testimony, a document, or a material object used to establish facts in a legal investigation or admissible as a testimony in a law court."[1]On a very broad view, it is permissible to include in this list such other means of proving a fact as admission and confession, judicial notice, presumption, and estoppel.[2]

As per the *Black's Law Dictionary* evidence is something (including testimony, documents, and tangible objects) that tends to prove or disprove the existence of an alleged fact. It is also the body of law regulating the admissibility of what is offered as proof in the record of a legal proceeding (specifically termed the rules of evidence).[3]

Evidence is any matter of fact that is furnished to a legal tribunal, otherwise than by reasoning or reference to what is noticed without proof, as the basis for

[1] Md Jahedul Islam, 'Digital Evidence: Some Must Needed Amendments', (2018) Volume 1, No 1, SCLS Law Review 47-50.

[2] T.A. Auguda, The Law of Evidence in Nigeria (2 edn., Ibadan, Spectrum Books Ltd 1974) 11.

[3] B.A. Garner, *Blacks Law Dictionary* (8th edn, USA, Thompson West 2004) 595.

ascertaining some other fact.[4] Evidence has also been defined to mean any species of proof legally presented at the trial of an issue, by the act of the parties, and through the medium of witnesses, records, documents, or concrete objects and the like.[5]

According to the Evidence Act 1872 with new amendment of 2022, evidence means and includes:

i. All the statements that the court permits or requires to be made before it by witnesses, in relation to the matter of fact under inquiry: such statements are called oral evidence;

ii. All documents produced for the inspection of the court; such documents are called documentary evidence.[6]

iii. All materials or objects relating to blood, semen, hair, all body material, organ, Deoxyribo Nucleic Acid (DNA), finger impression, palm impression, iris impression, and footprint or any other similar material or object which may-

   a. Establish that an offense has been committed or establish a link or relation between an offense and its victim or an offense and its offender, and

   b. Prove or disprove a fact

   Such materials or objects are called physical or forensic evidence. Besides these, the new amending Act also induced the digital signature, electronic signature, digital signature certificate, and certifying authority etc. expression within the definition of evidence under section 3 of the Evidence Act, 1872.[7]

   More on, the pervious definition of document was updated and 'digital record' or 'electronic record' were included. These two terms will mean any record, data or information generated, prepared, sent, received, or stored in magnetic or electro-magnetic, optical, computer memory, micro film, computer generated micro fiche including audio, video, Digital Versatile Disc or Digital Video Disc (DVD), records of Closed Circuit Television, drone data, records from cell phone, hardware, software or any other digital device as defined in Digital Security Act, 2018 (Act No 46 of 2018)[8]

In large, electronic evidence is meant, evidence generated by some mechanical or electronic processes. The use of computers and other forms of electronic storage

---

4 J.B. Thayer, *Presumption of Law and Evidence* (3rd Harvard Law Rev. 1889) 141-142.

5 Ibid.

6 Evidence Act 1872, section 3.

7 Evidence (Amendment) Act, 2022 (Amendment on 31 August 2022), section 2.

8 Ibid, section 2 (A) and (B).

and communication system are fast replacing the old-fashioned scheme of keeping chronicles and communication in written documents. Examples of electronic evidence may include computer print-outs, information storage devices such as disks, tapes, and microfilms, telegraphic transfers, taxes, electronic fund transfers, etc.[9] These would include banker's books of various types, e-mails, telephone records, text messages, digital cameras, mobile phones, letters, or other documents processed in a computer or electronic device or stored in a computer-based storage device.[10]

Electronic evidence is also defined by some scholars as-

> Data (comprising the output of analogue devices or data in digital format) that is created, manipulated, stored, or communicated by any manufactured device, computer, or computer system or transmitted over a communication system that is that has the potential to make the factual account of either party more probable or less probable that it would be without the evidence.[11]

Features of Electronic Evidence

One of the main features of electronic evidence includes any kind of data that is fashioned, wrought, or stockpiled in a computer. It will also embrace the numerous methods of devices by which data can be stored, or transmitted, including analogue devices that produce an output. However, as material, it has the potential to make the factual account of either party more probable or less probable than it would be without evidence.[12] Sometimes it may be paperless also. Commonly, though they are contained in tangible objects are visible by intangible.[13] On top of this, Burkhard Schafer and Stephen Mason considered the term electronic evidence as a generic one of which the species are both analogue and digital ones.[14]

---

[9] J. Chinwe, Admissibility of Documentary /Electronic Evidence Issues, Challenges and Options, (Ibadan University Press 2009) 15.

[10] J.O.K. Oyewole, 'Cyber Crime: Challenges before Judicial Officer'. (Presented at the All Nigerian Judges Conference 16-20, November 2009).

[11] Burkhard Schafer and Stephen Mason, 'The characteristics of electronic evidence', in Stephen Mason and Daniel Seng (eds) Electronic Evidence, (4th edition Institute of Advance Legal Studies for SAS Humanities Digital Library, School of Advance Study, University of London 2017) 19 <https:// humanities-digitallibrary.org/index.php/hdl/catalog/book/electronicevidence> accessed 31 May 2022.

[12] Ibid

[13] Muhammad Al Amin Deribe and Dr. Tijjani Musa Buba., 'Appraisal of the admissibility of electronic Evidence in Nigeria and the possibility of its Application under Sharia' <https://www.academia.edu ...NigeriaandthePossibilityofitsApplicationunderSharia> accessed 20 October 2021.

[14] Supra Note 8.

Sources of Electronic Evidence[15]

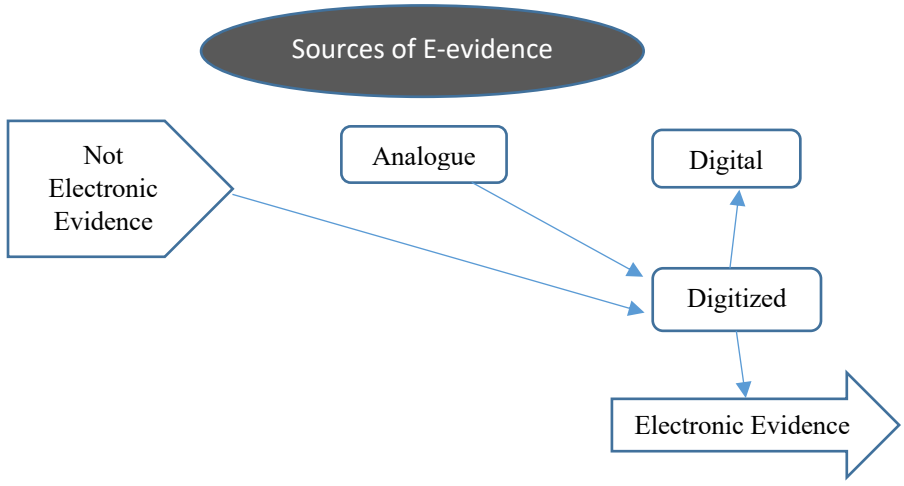

Figure.1: Sources of Electronic Evidence.

This chart is used to clarify the misnomer regarding electronic evidence and digital evidence which are often used interchangeably. However, both analogue and digital evidence are within the ambit of electronic evidence which is a generic term. Even, evidence that is not produced by any electronic medium can be later digitized (scanning form of any handwritten instruments) and can get the status of electronic evidence.

3. Why E-evidence

In the very recent past, the world is witnessing the unbelievable use of digital technology in various forms for various purposes. Remarkably, during the last covid-19 period we used to maintain our various daily life utensils through e-forums such as e-commerce, e-healthcare, online classes etc. The convergence of information technology and communication is rapidly changing the way transaction and relationships are carried out the world over.[16] With the advent of digitalization, the world has witnessed not only technological rebellion but also sophisticated, critical, digital and more organized means of committing a crime. Unfortunately, our orthodox prosecution laws have had a paralyzing impact on the justice disposal system in these changed circumstances.[17]

---

[15] Definition of Electronic evidence, <Electronic evidence - Wikipedia>accessed on 31st May 2022.

[16] Muhammad Al Amin Deribe and Dr. Tijjani Musa Buba., 'Appraisal of the admissibility of electronic Evidence in Nigeria and the possibility of its Application under Sharia' <https://www.academia.edu/37209893...and_the_Possibility_of_its_Application_under_Sharia> accessed 20 October 2021.

[17] Rajib Kumar Deb, 'Admissibility of digital Evidence in Court' *The Daily Sun*, (Dhaka 10 October 2019) <Admissibility of Digital Evidence in Court-430223 (daily-sun.com) > accessed on 2 June 2021.

Where digital technology adds slight to the original evidence, it is rarely worth the time and effort in preparing and present such evidence in a digital environment. However, where digital assistance allows the court to see or hear evidence that it would not otherwise have seen or heard or where it allows the court to see or hear such evidence in a more thorough, analytical format, it is well worthwhile. There have been numerous cases over the past decade where forensic video analysis has made the difference between a justified conviction and an unjust acquittal. Equally, it has also allowed for the exoneration of defendants who might otherwise have been wrongfully convicted a travesty we as a civilized society can ill afford.[18]

4. Relevancy and Admissibility of Electronic Evidence in Bangladesh

Electronic evidence can be relevant in many ways explained in sections (5-55) of our Evidence Act, 1872. Besides the above provisions, the new Evidence Amendment Act, 2022 also provides 16[19] full sections and 6[20] partially added sections for the relevancy and admissibility of electronic evidence and digital evidence in our civil and criminal courts. However, it may be directly or indirectly relevant. For example, expert opinion regarding electronic evidence may also be relevant under the previous law as well as under the new amending Act 2022 by adding two new sections respectively 45A and 47A[21]. Nevertheless, the most burning question is whether that relevant electronic evidence is admissible or not. From the various general, special laws on admissibility and judicial decisions, it can easily be seen that after the amendment in 2022, the admissibility of electronic evidence was directly incorporated by adding section 65B where the admissibility is dependent upon some conditions, and sub-conditions in our previous Evidence Act 1872. However, many special laws provided provisions admitting several types of electronic evidence. In contrast, having scattered provisions in special laws are also creating more complexity both for the advocate and judges. From the judicial precedence, it can be noticed that very few cases generally accepted all types of electronic evidence rather they accepted a special kind of electronic form of evidence in each decision such as videotape[22] recording or only audio recording. Consequently, the dilemma regarding the admissibility of all kinds of electronic evidence remained in the grey area. On top of that, the recent Evidence (amendment) Act 2022 created a wider door for various kinds of electronic

[18] W. Jonathan Hawk, 'The Admissibility of Digital Evidence in Criminal Prosecutions', <The Admissibility of Digital Evidence in Criminal Prosecutions (crime-scene-investigator.net) >accessed on 02.06.2021.

[19] Evidence (Amendment) Act, 2022 (Amendment on 31 August 2022), sections 10 and 11.

[20] Ibid.

[21] Ibid.

[22] *Mrs. Khaleda Akhter vs. State* [1985)] 37 DLR 275.

evidence. On points, regarding electronic evidence the following things are important –

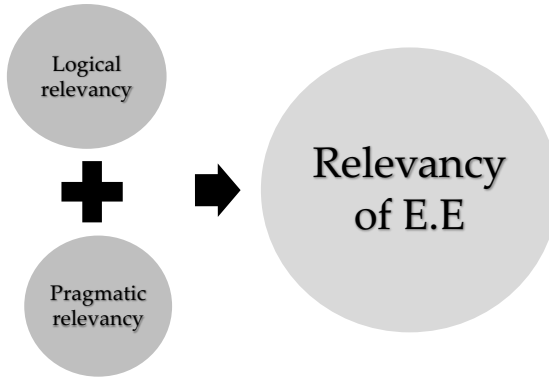

Figure 2: Types of Relevancy [23]

In this chart, two tiers of relevancy need to be justified before considering any electronic evidence as relevant. However, the logical relevance can be established through the lens of domestic law. In contrast, the pragmatic relevance can be ascertained by being assured that its probative value is not substantially outweighed by the other dangers of unfair prejudice or confusion of the issues etc.

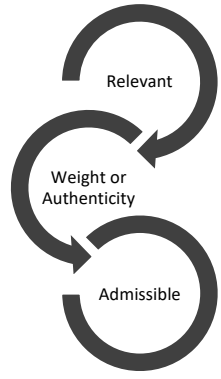

Figure 3: Essentials of admissibility.[24]

In this flow chart, it is stated that after being relevant the electronic evidence must be authentic to be admissible. However, this authenticity can be justified through the digital forensic process. Then, another question may arise, who will decide the admissibility of electronic evidence, is it the court or the digital forensic report that will get the finality? Section 148 of the Evidence Act 1872 will serve the answer that the court will ultimately decide which evidence is proper and which is not.

[23] This figure is created by the researcher for a better understanding of the information.
[24] This figure is created by the author for better understanding.

5. Governing Legislations for Admissibility of Electronic Evidence in Bangladesh

This part of the paper highlights various legal provisions having a direct or indirect connection with the relevancy and admissibility of electronic evidence in our country. As there are so many special criminal laws that provide direct provisions on the admissibility of some specific kind of electronic evidence, those are focused on in the table below.

5.1 Domestic Laws

Now for a better understanding of the relevancy and admissibility of electronic evidence or digital records, various domestic legislations are being explored below:

Constitutional Law: There is no dedicated article that can stimulate or signifies the concept of electronic evidence. However, article 35(3) can have some relevance in this regard where it is said that 'Every person accused of a criminal offence shall have the right to a speedy and public trial by an independent and impartial court or tribunal established by law'. The conception of the right to a speedy trial can be ensured through the proper and scientific use of electronic evidence. More on this, the above provision is qualified by Article 35(5) which created an objection to avoid the conflict with the provisions of prevailing general law.

General laws: Despite having several special legislations, the Evidence Act 1872 is the principal general enactment regarding the relevancy and admissibility of electronic evidence before the court. As a fundamental law, the Act was backdated in coordination with the fast growth of science and technology till 2022. With the pace of expansion in technologies, proof of various modern crimes needs to be explored and established through various electronic means of evidence such as audio recording, video recording, still photos, etc. Last year, drastic changes regarding the admissibility of electronic evidence or digital evidence were brought in our old Evidence Act, 1872 by the Amending Act of 2022. Under that amendment, sixteen full new sections and six partially amending sections were incorporated into our previous Act and which reverse the ancient scenario of electronic evidence and digital evidence. The newly added changes are as follows-

Though under the previous Act of 1872, the definition of the document included the physical or material things only, now the new Amending Act of 2022 incorporated the words any digital record or electronic record under the previous definition which includes a large list of electronic moods of evidence.[25] Besides this, the definition of Evidence was also broadened by adding clause 3 in the existing one which includes forensic evidence or physical evidence, and some relevant terms were clarified such as digital signature, digital signature certificate,

[25] Evidence (Amendment) Act 2022 (Amendment on 31 August 2022), sections 2 (A).

and certifying authority etc.[26] The provision regarding admission was also modified and under section 17 of the Evidence Act, 1872 the extension digital record has been added and a new section 22A was incorporated on the relevancy of admission as to the content of digital record only in case of genuineness of digital record produced is in question.[27] More on, sections 34, 35, 36, and 39 were slightly modified and the term digital was added which created a new window for digital maps, plans, books etc. being relevant.[28] The provisions regarding expert opinion were also modified by extending the subject matter of existing section 45 of the Evidence Act, 1872 inserting the various physical or forensic record or digital records within its ambit and also incorporating two new sections 45A and 47A in this regard.[29] Other miscellaneous provisions concerning the relevancy and admissibility of electronic evidence brought by the new amending Act of 2022 are proof as to digital signature (section 67A), proof as to verification of the digital signature (section 73A), comparison of physical or forensic evidence with others admitted or proved one (section 73B), the presumption as to Gazettes in digital forms (section 81A), the presumption as to agreements in digital forms (section 85A), the presumption as to digital record and digital signature (section 85B), the presumption as to digital signature certificates (section 85C). Under the amending provision, the court may presume regarding the digital communication but shall not presume regarding the sender which was as like as before under section 85 of the previous Act. In line with this, the court may presume as to physical or forensic evidence and as to five years old digital records with fulfilling the pre-conditions under the newly added section 89A and 90A respectively by the Evidence (amending) Act, 2022.

However, the foremost provisions on the admissibility of digital records were inserted as sections 65A and 65B by the Evidence (amending) Act 2022. Section 65A[30] explained nothing elaborately but refers to the fulfilment of some conditions under section 65B for proving the contents of digital records. Under section 65B it is clearly stated that any information contained in any digital form shall be considered a document if they are backed by condition fulfilled under sub-section (2), (3), and (4) of 65B. The four cardinal conditions are, the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes or any activities carried on over that period by the person having lawful control over the use of the computer; during the said period the concerned derived information was regularly fed into the computer in the ordinary course of the said activities; throughout the material part of the said period, the computer was

[26] Ibid, sections 2(C).

[27] Ibid, sections 4.

[28] Ibid, sections 5, 6, 7, and 8.

[29] Ibid, sections 9, 10, and 11.

[30] Evidence (amendment) Act, 2022 (Amendment on 31 August 2022), section 12.

operating properly and any non-operation did not affect the accuracy of the digital record and the information contained in digital record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities which need to be fulfilled for admitting any digital record before the court. However, regular use of the computer over the period was clarified under sub-section (3), the contents of a certificate regarding digital records were provided under sub-section (4), and sub-section (5) dealt with various means and methods of supplying information to the computer. Though more than 150 years have already passed, we can now dream of a digital Bangladesh standing with the recent amendment of the Evidence Act in hand.

Table 1: Other Special Criminal Legislations Incorporating the Concept of E-evidence[31]

Statutes	Evidence	Sections
Speedy Trial Tribunal Act 2002	Audio, Video, Image	16
Law and Order Disruption Crimes 2002	Audio, Video, Image	14
Anti-Corruption Commission Act 2004	Expert opinion	23(1)
Information and Communication Technology Act 2006	Electronic records-forms-gazettes-signatures-certificates, documents, data involved in EDI, data message (Email, SMS, etc.)	2, 6, 9, 10, 87
Anti-Terrorism Act 2009	Conversation, Facebook, Skype, Twitter Offence related image or video	21(3)
Pornography Control Act 2012	Electronic information, data, Traffic data stored by BTRC, ISPs, MOs, VOIPSPs	6(2), 6(3)
Mutual Legal Assistance in Criminal Matters Act 2012	Computer data, traffic data stored by SPs	28, 30
Digital Security Act 2018	Expert opinion, forensic evidence	51, 58

5.2 Judicial Decisions

There are some landmark judicial decisions that created the scope of admitting electronic evidence even before the recent amendment[32] in the Evidence Act, of 1872.

Mrs. Khaleda Akhter vs. State[33] was the first case that allowed a kind of electronic evidence in the judiciary of Bangladesh. It was held that "a video cassette is a document within the meaning of the Evidence Act and is accordingly admissible

[31] This table was taken from the public lecture given by Quazi Mahfujul Haque Shupan, Professor, Department of Law, Dhaka University, (Public lecture series, May 2020).

[32] Evidence (Amendment) Act 2022 (Amendment on 31 August 2022).

[33] (1985) 37 DLR 275.

in the document. The Supreme Courts both in India and Pakistan Approved of a tape recorder being used in evidence and the use of the evidence by tape recording in a proceeding before a court of law."

Major Bazlul Huda vs. State [34]case touched upon the admissibility of video evidence. In this case, the prosecution submitted a video cassette of a television program in which Major Rashid and Farooque Rahman admitted their participation in the killing of Bangabandhu Sheikh Mujibur Rahman. Both Justice Tafazzul Islam and Justice S.K Sinha determined that the question of admissibility of digital or electronic evidence as documentary evidence arises only when the accused denies his statement or admission.[3] Otherwise, digital or electronic evidence can be readily taken as documentary evidence. In case of denial, it can only be admissible under the prevailing law of evidence. After a strictly literal interpretation of section 3 of the Act, the court ultimately denied admitting electronic evidence. Unfortunately, neither the prosecution nor the court referred to the case of *Khaleda Akhtar* case. In such a situation, the prosecution could have convinced the court about the authenticity of the videocassette by bringing a qualified expert under section 45 of the Act. The prosecution brought a local video recorder who failed to convince the court.

In the *State vs. Kamrul Islam (Rajon Murder)* [35] case it was held that video footage is a document within the Act and is, therefore, admissible. The court drew a parallel interpretation from the *Khaleda Akhtar* case. However, the principle given in the *Khaleda Akhtar* case is applicable only for video recorded by an analogue camcorder. Analogue camcorders are recorded on tape or cassettes, but digital camera uses storage media such as Secure Digital (SD) cards. The court failed to elaborate on how their interpretation would apply to the digital camcorder.

Moreover, it is noticeable that the courts have used the term 'electronic evidence' and 'digital evidence' interchangeably. This is somewhat ambiguous because the two terms are not synonymous. Electronic evidence includes both analogue evidence (vinyl records, audiotape, and photographic film) and digital evidence (anything created or stored in a computer). [36] The matter of hope is that the video evidence even in digital form will be fallen within the definition of document.

In the *Biswajit murder* case,[37] the court observed the well admissibility of video footage, still photographs, and paper clippings without substantiation by the authors.[38] It was also noticed that video footage was authoritatively handed over

[34] [2017] 62 DLR (AD) 1[173] [726].

[35] [2017] LEX/BDHC/0019/2017.

[36] Burkhard Schafer and Stephen Mason, 'The characteristics of electronic evidence', in Stephen Mason and Daniel Seng (eds), Electronic Evidence (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London 2017) 19.

[37] [2018] 70 DLR (HCD) 26.

[38] Ibid.

to the investigation officer under a seizure list by a TV channel; so, its recording and publication/telecast were authenticated *ipso facto*.

In all these past and recent cases, the use of electronic means of evidence was permitted by the court. Though some of these cases were under special criminal law which was backed by specific provisions regarding the admissibility of electronic evidence, the first two cases opened the windows for electronic evidence under general law long before the recent gigantic amendment.

6. International and Regional Instrument on the Admissibility of E-evidences

The Budapest Convention[39] is a criminal Justice accord with a specific concentration on cybercrime and electronic evidence. It requires party a. to criminalize a range of offences against and using computers[40], b. to provide criminal justice authorities with procedural powers to secure electronic evidence about any crime[41] and c. to engage in efficient international cooperation[42]. In relation, to the above requirements, the second and third are very important and gave procedural power to investigate the crime effectively and to expand the hand of international cooperation which are very indispensable to combat various approaches to crime related to technology. Additionally, the Budapest Convention has backed up the Cybercrime Convention Committee, which among other things, gages the implementation of this treaty by the parties, and by capacity building program.

The Budapest Convention on Cybercrime of the Council of the Council of Europe was opened for signature in November 2001. By August 2016, 49 states were parties, and a further 18 had signed it or been invited to accede. However, Bangladesh is one of the observatory states of this convention.

Several regional instruments talk about electronic evidence unswervingly and circuitously. Among them, the Malabo Convention on Cyber Security and

[39] Convention on Cybercrime, Budapest, 23. XI. 2001.

[40] Budapest Convention, 2001; articles, 2-Illegal access, 3-Illegal interception, 4-Data interference, 5-System interference, 6- Misuse of device, 7-Computer related forgery, 8-Computer related fraud, 9-Offences related to child pornography, 10- Offences related to infringement of copyright and related rights, 11- Attempt and aiding or abetting, 12-Corporate liability & 13-sanctions and measure etc.

[41] Budapest Convention, 2001 Articles, 14- Scope of procedural provisions, 15- Conditions and safeguards, 16- Expedited preservation of stored computer data, 17-Expidited preservation and partial disclosure of traffic data, 18-Production order, 19-Search and seizure of stored computer data, 20- Real-time collection of traffic data & 21- Interception of content data etc.

[42] Budapest Convention, 2001 Articles, 23-General Principles relating to international cooperation, 24-Extradition, 25-General Principles relating to mutual assistance, 26-Spontaneous information, 27-Procedure pertaining to mutual assistance requests in the absence of applicable international agreements, 28-Confidentiality and limitation on use, 29-Expedited preservation of stored computer data, 30-Expedited disclosure of preserved traffic data, 31-Mutual assistance regarding accessing of stored computer data, 32-Trans-border access to stored computer data with consent or where publicly available, 33-Mutual assistance regarding the real-time collection of traffic data, 34-Mutual assistance regarding the interception of content data, 35-24/7 Network.

Personal Data Protection of the African Union, 2004, the Civil Evidence Act, 1995 and the Police and Criminal Evidence Act, 1984 which provide for electronic evidence in civil and criminal matters respectively in the United Kingdom, the Federal rules of evidence, which was first adopted in 1975, the Federal Rules of Evidence[43] codify the evidence law that applies in United States Federal Courts[44]. In addition, many states in the United States have either adopted the Federal Rules of Evidence, with or without local variations or have revised their own evidence rules or codes to at least partially follow the federal rules. Federal Rules of Evidence 902(13) and 902(14), which became effective on December 1, 2017, provide for the self-authentication of electronic evidence. Under these rules, electronic evidence can be authenticated by certification instead of by testimony. Rule 902(13) applies to electronic evidence such as computer files, social media posts, and smart device data. Rule 902(14) applies to electronic copies.[45]

7. Substantial Laws on the Admissibility of E-evidences in Other Jurisdictions

In India, the Evidence Act of 1872 has been amended by section 92 of the Information Technology Act, of 2000. Section 3 of the Act was modified and the phrase All documents included the term electronic records within it. Further, new 4 sections were added in the original 1872's Act regarding electronic evidence and procedures of its admissibility as 65B (1), 65B (2), 65B (3) & 65B (4).

In Malaysia, the admissibility of electronic evidence was predominantly dealt with by the Malaysian Evidence Act 1950. However, in the Malaysian court of law, the acceptability of electronic evidence is controlled by sections 90A, 90B, and 90C. Section 90A is an exception to the hearsay rule. It provides that a document created by a computer or a statement contained in such document shall be admissible as evidence of any fact stated therein whether or not the person tendering the same is the producer of such document or statement. This section applies to both criminal and civil proceedings. As well, the court has acknowledged three different terms that would imply the meaning of computer evidence. These can be seen in cases *PP vs. Lee Kim Seng*[46], *PP vs. Ong Cheng Heong*[47] *and Ahmad Najib b aris vs. PP*[48] etc.

---

[43] Federal Rules of Evidence < Federal Rules of Evidence | Federal Rules of Evidence | US Law | LII / Legal Information Institute (cornell.edu) > accessed on 15th September 2021.

[44] Federal Judiciary, < Federal judiciary of the United States - Wikipedia> accessed on 15th Sep 2021.

[45] Amendment to the Federal Rules<Amendments to the Federal Rules of Practice and Procedure: Evidence 2017 Self-Authenticating Electronic Evidence | Federal Judicial Center (fjc.gov) >accessed 15 Sep 2021.

[46] *PP. vs. Lee Kim Seng,* [2013] 7 MLJ 844 (Computer printout).

[47] *PP vs. Ong Cheng Heong,*[1998] 6 MLJ 678 (Computer Output)

[48] *Ahmad Najib b Aris vs. PP*, [2007] 2 MLJ 505 (Computer Evidence-Chemist report)

In Nigeria, there are limitations on the admissibility of computer or electronic evidence. As far as its authentication is reliable and acceptable to both parties in litigation, then such evidence becomes admissible while the weight to be attached is another issue entirely. Section 84 of the Evidence Act, 2011 provides for the circumstance of acceptability of computer evidence. It is stated that a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible. However, it must be shown that the conditions[49] in subsection (2) of the section are satisfied with the statement and computer in question.[50]

In the UK, both civil and criminal trials allowed electronic evidence. In civil litigations, the admissibility of electronic evidence is guided by the Civil Evidence Act 1995. Admissibility of computer records[51] and proof of statement of document[52] which also includes plans, photographs models,[53] etc., are also within the periphery of law in the UK. On the other side, the Police and Criminal Evidence Act 1984 defined electronic evidence as 'all information contained computer term and therefore allowable as evidence in courts for criminal cases. On this note, Video recording may be admitted as chief especially if the evidence was taken from the vulnerable witness[54] and it must go through some procedures[55].

In the USA, the Federal Rules of Evidence which codify the evidence law that applies in United States Federal Courts was first adopted in 1975. Additionally, self-authentication on certain types of machine-generated data and forensic electronic evidence is introduced by the Federal Rules of Evidence's amendment of Rule 902. Under this amended rule litigating parties are no longer bound to produce a witness for authenticating the produced evidence under rule 901. On this point Rule, 902 allows certain types of evidence to be self-authenticating, as they have "evidence of authenticity," including newspapers, commercial papers, business records, and several other materials.

In 2010, as a first attempt, Chinese statute mentioned clearly about electronic evidences, Additionally, provisions of the Supreme People's Court, The Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of State Security and the Ministry of Justice on Several Issues Concerning the Examination and Judgment of Evidence I Handling Death Penalty Cases elucidated that email,

---

[49] Evidence Act 2011, section 84 (2) (a)-regularity of the use of computer, (b) regularity of supply f information to the computer in the ordinary course of those activities information, (c) the computer was operating properly and (d) the information contained in the statement in the reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

[50] Evidence Act 2011, section 84 (1).

[51] Civil Evidence Act 1995, section 3.

[52] Civil Evidence Act 1995, section 8.

[53] Civil Evidence Act 1995, Miscellaneous rule 33.6 of part 33.

[54] Youth Justice and Criminal Evidence Act, 1999.

[55] Practice Criminal Directions, 2013.

electronic data interexchange, online chat records, blogs, short message were electronic evidence. Then the newest procedure laws including the Criminal Procedure Law (2013), the Civil Procedure Law (2013), and the Administrative Procedure Law (2015) all admit the Legal status of electronic evidence by adding 'electronic data' to the definition of 'Evidence'. However, sometimes misapprehension is created between the admissibility and probative value of collected electronic data in a legal environment. From the procedural practice, it can be observed that in the Chinese context the various regulations demand a strong authentication process of an original physical item of storage along with some other particulars.[56] Consequently, 50 % of the civil cases are involved various electronic evidence among which 60 % can be proved.[57]

In South Africa,[58] section 34 of the Civil Proceeding Evidence Act 25 of 1965 did not provide for admissibility issues relating to computer printers. The section provides for the admissibility under specific circumstances of a statement made by a person in a document, but a computer was not regarded as a person. The Computer Evidence Act 57 of 1983 was thereupon placed on the statute book to regulate the admissibility of computer evidence. This Act did not achieve its purpose mainly due to an over-cautious approach in placing a high premium on authenticity and reliability. Additionally, this Act need several approaches for admissibility and it did not apply to criminal proceedings. Consequently, a statutory relief came in the form of the Electronic Communications and Transaction Act 25 of 2002 (hereafter referred to as the ECT Act)[59]. It provides various legal issues including electronic issues also. However, section 15 of the ECT Act provides for the admissibility and evidential weight of a data message as electronic evidence. On this point, it is clear from the wording in section 1[60] that it sets to facilitate rather than inhibit the admissibility of data messages as electronic evidence.

8. Notable Foreign Judgments on E-evidences

To understand the gradual development of using and accepting electronic evidence, other countries have many laws and judicial decisions which need to be

[56] The Illegal Evidence Exclusion Guide of Criminal Cases for Defense Lawyer (tentative) Article 11, the Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China, 2015 article 116.

[57] See, <http://www.pkula.cn/Case/ > accessed on 21st September, 2021.

[58] Prof. Murdoch Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position' (2009) Journal of Information, Law & Technology <[PDF] Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position | Semantic Scholar > accessed on 31 May 2022.

[59] Electronic Communications and Transaction Act 2002.

[60] Section 1 defines a data message means data generated, sent, received or stored by electronic means and includes (a) Voice, where the voice is used in an automated transaction and (b) a stored record. Data is defined as the electronic representation of information and will not offend best evidence rule. Consequently, electronically produced data did not require special procure to be admissible.

discussed for the better implementation of electronic evidence in our judicial activities.

In India, primarily the judiciary was not prepared to appreciate the connotation of section 65B. And consequently, in the *Navojot Sandhu* case, [61] the Supreme Court opined that there is no bar in the case of producing electronic evidence as secondary evidence under sections 63 and 65 without fulfilling the prerequisites under section 65B. Further, it is stated that a certificate containing the details of sub-section (4) of Section 65B is not needed to be submitted. Departing from its earlier ruling, the significance of section 65B in the case of electronic evidence was recognized in the *Anvar* case[62]. Henceforth, it was observed that any documentary evidence by way of electronic moods in view of sections 59 and 65A can only be proved after satisfying the conditions prescribed under section 65B. The tenacity of the provisions is to sanctify secondary evidence in electronic form, spawned by a computer. The same view was also observed in the *Rakes Kumar* case.[63] Admissibility of Hard discs and CD recordings as electronic evidence was recognized in the *Dharmbir* case[64] and the *Jagjit Singh Case*[65]. Additionally, video conferencing and the legality of evidence obtained therein were observed in the *Parful Desai* case,[66] the *Boloda Murali Krishna* case[67], the *Bagchi* case,[68] and the *Anwar* case.[69] However, the court in the *Twentieth Century Film Corporation and NRI Film Production Associates (P) Ltd.* Case,[70] has given some guidelines in case of recording evidence through the audio-video link.

In the USA, three judicial decisions are significant regarding the admissibility of electronic evidence. Among these two are related to different moods of tests for being the electronic evidence admissible. In *Frye vs United States Case*, it was recognized that scientific evidence was allowed if the science upon which it rested was generally accepted by the scientific community which is also known as Frye Test.[71] However, a gatekeeping obligation to assess the reliability of scientific evidence by the court was recognized later in another case in the *Daubert vs, Merrel Dow Pharmaceuticals*, which is also known as Daubert Test. The Supreme Court proposed five criteria to determine the admissibility of scientific evidence which are, whether the technique has been tested; whether has undergone peer review; whether there is a known error rate; and the existence and maintenance of

[61] [2005] AIR SC 3820.
[62] [2015] AIR SC 180.
[63] [2009] Cri. appeal no19/2007, High Court.
[64] [2008] 148 DLT 289.
[65] [2007] AIR SC 590.
[66] [2003] AIR SC 2053.
[67] [2007] (2) ALD 72.
[68] [2005] AIR Cal. 11.
[69] [2012] (Civil Appeal 4226).
[70] [2003] AIR Kant. 148.
[71] *Frye vs. United States* [1923] F. 1013 (D.C. Cir. 293).

standard controlling its operation (like Frye) whether the technique is generally accepted by the scientific community.[72] Another landmark case[73] decision set an instance as to which party pays for the unearthing of e-evidences. For data in a handy format, the usual rules of discovery apply, which means that the responding party is required to pay for production. When inaccessible is at issue (categories 4 and 5), the judge can contemplate costs to the requesting party.

9. Contemporary Issues on E-evidences in Bangladesh

***Digital Forensic*:** Digital forensics (DF) is a tract of Forensic Science. With roots in the personal computing revolution of the late 1970s and early 1980s, the discipline advanced haphazardly during the 1990s, and it was not until the early 21st century that national policies appeared. It covers the retrieval and examination of evidence found in digital media often conducted as a response to computer crime.[74] Palmer defined Digital Forensics (DF) as "The use of scientifically derived and proven methods towards the preservation, collation, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."[75] According to the present evolution of ICT in Bangladesh, digital instances and crimes are snowballing proportionately. As perceived from the studies done in the three government organizations, there was no common and comprehensive digital forensic framework in our country. In Information Security Policy Guidelines, the Ministry of Posts, Telecommunication, and Information Technology suggested a risk management process but no digital forensic guideline was provided.[76] On this point, in 2017, M. Mahfuzul Haque and Sayed Akhter Hossain referred to a proposed comprehensive digital framework module in their research paper.[77] his framework was prepared for the government of Bangladesh. Though the legal relevancy and admissibility of electronic evidence can be assured by bringing some amendment or enacting a comprehensive and contemporary evidence law, the weight and authenticity of electronic evidence can only be ensured by a strong and effective digital forensic system. For this, we have to develop a culture of modern technology equipped with digital forensics both in

---

[72] [1993] Inc., 509 U.S. 579.

[73] *Zubulake vs. USB Warburg LLC,* [2003]217 F.R.D.309.

[74] M.A. Pichan, Lazarescu and S.T. Soh, "Cloud Forensic: Technical Challenges, solution and comparative analysis." (2015), Volume-13, 38-57, Digital Investigation.

[75] G. Palmer, 'A road Map for Digital Forensic Research,' (2001) DFRWS., Utica, NY, Tech. Rep. DTR-T-001-01 Final.

[76] Bangladesh, Ministry of Post, Telecommunications and Information Technology, "Information Security Policy Guidelines," The ICT Division Website., Apr. 6 2014 < http://ictd.gov.bd/main/policy > accessed on 31st May 2022.

[77] M Mahfuzul Haque and Sayed Akhter Hossain, 'National Digital Forensic framework for BD', Conf. Paper, Dec 2017 <file:///C:/Users/SR%20IT... PID51315 39.pdf >last accessed on 4 July 2023.

civil and criminal cases for better functioning of justice. Consequently, Bangladesh established its Digital Forensic Lab in 2018 to investigate digital evidence. Its team is capable of recovering and investigating material found in digital devices including mobile, PC, Drone or any IOTs or computational devices. The objectives of the CIRT LAB are to build the capacity of students and government officials aiming to assist in Criminal prosecution, Civil Litigation, Financial Organizations and law enforcement officials. Bangladesh Government's e-government Incident Response Team BGD e-GOV CIRT, currently serving as the National CIRT on Bangladesh (N-CIRT). It has a very strong tie with international organizations and cyber security communities and works as a focal point for Bangladesh for trans-border cyber issues.

***E-evidence and Right to Privacy*:** The right to privacy as one of the fundamental rights is enshrined in our supreme law under article 43. Besides these, as a part of core human rights norms, this right is also supported by numerous international human rights instruments[78]. However, a list of regional[79] and national instruments also provides provisions supporting the above-mentioned right. Despite all these backings, human rights and fundamental freedoms may become controversial when it comes to evidence retrieval. Coercive measures, which are used as means of gathering evidence, are closely related to human rights and fundamental freedoms. Nevertheless, these coercive methods in some cases extend to affect the right to privacy of the third party also. On this point, it is accepted that human rights and fundamental freedoms can be restricted in certain circumstances for national security and public safety etc.[80] Despite, having of reasonable restriction clause, the sole purpose of prevention of crime should not be considered sufficient to interfere with individuals' rights as it may cause erroneous assumptions. Additionally, this erroneous assumption sometimes put the rights to privacy at stake. To strike a balance between the interest in effective law enforcement and intrusion on the right to privacy, the application of the procedures shall pursue the

[78] UDHR 1948; Article 12, ICCPR,1966, Article 17, Convention on the Rights of the Child,1984, Article 16, International Convention on the Protection of All Migrant Workers and Members of Their Families,1990, Article 14.

[79] European Convention for the Protection of Human Rights and Fundamental Freedoms,1950, Article 8, American Convention on Human Rights,1969, Article 11, Cairo Declaration on Human Rights in Islam,1990, Article 18, Arab Charter on Human Rights: Articles 16 and 21, African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression in Africa,1987, African Charter on the Rights and Welfare of the Child, 1990, Article 19, Human Rights Declaration of the Association of Southeast Asian Nations,2012, Article 21, Asia-Pacific Economic Cooperation Privacy Framework, 2015, Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 2001, Council of Europe Recommendation No. R (99) 5 for the protection of privacy on the Internet, 1999, European Union Data Protection Directive, 1995.

[80] Council of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), 1950, Article 18.

interest of a democratic society and the principle of proportionality. In other words, the coercive measure may be necessary in proportion to the concrete case.

10. Impending Challenges of Admitting E-evidences in Bangladesh

As a technologically less developed country, use of the of electronic evidence can face some challenges which are discussed under some common headings below-

***Legal Challenges*:** Though recently the Evidence Act 1872 was amended by the Evidence (amendment) Act 2022 which incorporated some new provisions on the admissibility of electronic evidence or digital records, they did not cover all the modern technologies such as cloud records. They talked about general conditions for admissibility and expert opinion in some circumstances but which is not obligatory upon the court. The new Act did not provide any provisions regarding the collection and preservation of electronic evidence or digital record. In some cases, many presumptions was incorporated into some digital records which will prolong the trial. However, 30+ crime and punishment-defining statutes exist in Bangladesh, and only a few of these contain digital evidence provisions. However, the inclusion and non-inclusion of digital evidence in some criminal statutes also created misconceptions among the investigators and prosecutors. Additionally, included provisions are scattered, not technologically neutral, and failed to draw the line between data and device which creates confusion. More on, rules regarding digital evidence can be traced in numerous case laws rather than contained in a single comprehensive case law.

***Infrastructural Challenges*:** Introducing digital evidence in our judicial system will also face some infrastructural challenges. Firstly, our courtrooms are not well-resourced to support digital evidence. Secondly, our judges and court staff are not enough acquainted with such matters. It will be a challenge to train them all. Thirdly, the common people who are oblivious to technology may face hurdles with such variation. Fourthly, digital evidence can easily be modified, altered, or transmitted. It may create a latitude of altering important evidence unless precautionary measures are taken. Fifthly, the required number of quality IT experts may not be available. Sixthly, unlike criminal cases, in our country civil laws are not enforced by separate agencies like police who can help to carry out forensic investigation. Thus, this job needs to be done by different agencies of the state at the expense of the parties which can prolong the procedure. Lastly, complexity regarding the evidence collected from social media sites on its authenticity.

***Procedural Challenges*:** In most of criminal cases, the exclusive responsibility to investigate lies in the police. However, the reality is most police officers do not have sufficient experts on how the different types of digital evidence need to be collected and preserved for further inquiry, such as the rare use of the Faraday

Bag[81], and the unprofessional description of different injuries present in the dead body even after death. Another procedural problem is, that the concerned forensic expert has to appear before the court to be undergone examinations like a conventional witness. Such practices discourage the experts to be involved in the process of preparing a forensic report by collecting and comparing samples. Due to the adversarial system, sometimes they have to face many irrelevant questions from the adverse party. Sometimes, the court rejects the forensic report without showing any proper cause which prolongs the prosecution. More on, maintaining the chain of custody and handling digital evidence by investing officer (IO) are other great challenges. As the I.O. may be transferred or the investigation procedure may be transferred to another officer.

It can't be denied that technologies are upgraded day by day, hence, the existing laws may turn out to be unexhausted to tackle the upcoming issue. However, the curricula of our law schools are not designed with an interdisciplinary approach. Studying forensic science is almost mysterious to our legal education as very few public and private universities offering undergraduate and graduate programs in law include this subject in their curricula. Lack of comprehensive research to address future challenges also.

11. Challenges in Admitting E-evidence in Bangladesh

For finding out the impending challenges in the case of admitting electronic evidence in Bangladesh a personal survey was done by the researcher. In this survey, a total of 50 people were targeted, among them 15 are judges, 20 are advocates,10 are Investigation officers and the other 5 are academicians and researchers. They were provided with a questionnaire previously primed by the researcher on this concern. Their views on a fixed question of 8 nominated diverse points of challenges are presented in the following table 2.

	Challenges in admitting E-evidence	**People Responded**	**Percentage**
1.	Legal Issues	14	28%
2.	Less supportive judges and Advocate	4	9%
3.	Right to privacy	10	19%
4.	Scattered laws on Electronic Evidence	4	9%
5.	Week Infrastructure	3	5%
6.	Week digital forensic system	10	19%
7.	Lack of judicial procedure	4	9%
8.	Others	1	2%
	Total	**50 persons**	**100%**

Table 2: Data from the survey

[81] Faraday Bag, < What is a Faraday Bag? - Faraday Bags - RF Shielded Faraday Bags by Disklabs Faraday Bags – RF Shielded Faraday Bags by Disklabs > accessed on 27th September 2021.

In the above table, eight different vital denominators are selected for showing various ratios of challenges in admitting electronic evidence in Bangladesh. However, 14 participants among a total of 50 believe that complex legal issues would be the most (28%) looming challenges in case of admitting electronic evidence in Bangladesh. After this, the right to privacy concern (19%) and the existing scrawny digital forensic system (19%) would be great defies for us. As well, scattered laws on electronic evidence, less compassionate judges and advocates and a lack of judicial precedence in this arena would affect an identical ratio of (9%). Finally, other miscellaneous features would be accountable for 2% only. Hence, we need to be more vigilant on this issue according to their ratios for safeguarding an effective mechanism for the admissibility of electronic evidence in our court.

12. Prospective Way Forward

As a transitory solution, the government can postpone by order all the scattered provisions regarding electronic evidence or digital record in numerous special criminal laws and circulate the new amendment Act of 2022 for all types of criminal cases. Besides, a comprehensive and technology-neutral legal framework needs to be hosted which should keep pace with the developments of ICT to avoid turning legislation obsolete. Additionally, the law ought not only to be flexible but also be proactive to see to it that it neither leaves people unprotected against new technologies nor pannier the development of technologies themselves. On the depiction of all-inclusive electronic communications, the legislature should ensure four principles[82] of good practice by APCO. To abolish all the provisions relating to Digital Evidence contained in various statutes for avoiding unwanted anomalies. Apprise Police Regulation of Bengal (PRB) and other procedural laws. Our government should also strive to train a sufficient number of personnel and the legal fraternity to avail the fruits of new legislation.

In the case of investigation of digital evidence, each step requires the use of tools or knowledge, the process must be documented, reliable, and repeatable. More on, various laws dealing with forensic evidence are to be adjusted to create uniformity.[83] Mandatorily, there should be created a combination of police, judges, magistrates, lawyers, and forensic experts to ensure a high standard of techno-legal investigation. For the common good, digital forensic needs to be included in the law curricula of every law school's syllabus. However, effective consultation between the prosecutor and forensic examiner to weigh the evidence need to be established. They will decide whether the evidence is enough to tie the accused to the alleged crime. If the answer is yes, the evidence will be presented in a court of

[82] APCO, Good Practice for Compute Based Electronic Evidence, Official Release Version. <Microsoft Word - Revised Good Practice Guide for Digital Evidence_Vers 5_Oct 2011 (digital-detective.net) > Accessed on 27th September, 2021.

[83] i.e., Definition of Documents and section 87 of the Information and Communication Technology Act.

law by connoisseurs.[84] Finally, the government should enact a comprehensive law on digital evidence and digital forensics in our country for eradicating the existing anomalies in the simultaneous running of general and special laws regarding electronic evidence or digital records.

13. Conclusion

Failure of judicial mechanism to ensure justice for want of proof not only deprives the justice seeker of his access to justice but also debases the entire fabric of the society. Additionally, the absence of a legal framework providing the vigorous institutional basis for investigation and trial in criminal cases and maintaining 'the balance of probability in civil cases keeping the scientific evidence (electronic evidence) issues apart may be the catalyst for crime rising and delay of civil suits in our country. In this research, for apposite admissibility of electronic evidence, few lacunas in existing legislations and numerous impending challenges were ascribed along with some effective way-outs. Besides, laws and judicial doctrines from some other jurisdictions were encompassed aiming to support modeling our new law on electronic evidence or to alter our existing special laws for coping with the digital world. Though electronic evidence has its numerous inherent dangers[85], a specific comprehensive law can be legislated for electronic or digital evidence for both civil and criminal cases providing special procedures not only on admissibility but also on authenticity, digital forensics, checking various biases in forensic reports, and preventing format shopping[86] for ensuring functional equivalence between hard copies and electronic copies. However, it is strappingly suggested by the author that interdisciplinary research and discussion need to be organized among IT experts, legal experts, and others. Lastly, the future interested researcher in this area can explore the issues of innumerable biases in forensic reports, prevention of format shopping, right to privacy and digital evidence, and so forth.

[84] This Suggestion was given by Q.M.H. Shupan, Associate Professor of Faculty of Law, Dhaka University, in an International conference organized by the Department of Criminology, Dhaka University.

[85] *S vs. Ndiki and others* [2007] 2 All SA 185 (CK)at 31, 53.

[86] J. Hofman 'Electronic Evidences I South Africa' (2006) <holfman@law.uct.ac.za >accessed on 20 Oct 2021.