UGC & Govt. Approved

Sonargaon University (SU)

সোনারগাঁও ইউনিভার্সিটি (এসইউ)

Research Monograph

On

"Admissibility and Reliability of Digital Evidence in Criminal Trails: Challenges in the Modern Criminal Procedure System."

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of L.L.B (Hon's), Department of Law, Sonargaon University (SU)

Submitted By

Ashraful Islam

ID No: LLB2203027024

Department of Law

Faculty of Arts and Humanities

Sonargaon University (SU)

Supervised By

Sunzida Akhter

Lecturer

Department of Law

Faculty of Arts and Humanities

Sonargaon University (SU)

Date of Submission: 25th June 2026

DEDICATED TO MY BELOVED PARENTS & BROTHER

LETTER OF TRANSMITTAL

To
Sunzida Akhter
Lecturer
Department of Law
Sonargaon University (SU)

Subject: Submission of Research Monograph on "Admissibility and Reliability of Digital Evidence in Criminal Trials: Challenges in the Modern Criminal Procedure System"

Dear Madam,

This is a great pleasure to submit the Research Monograph on Research Monograph on **"Admissibility and Reliability of Digital Evidence in Criminal Trials: Challenges in the Modern Criminal Procedure System"** as a partial requirement for the fulfillment of my LL.B. (Honours) course under the Department of Law of the Sonargaon University (SU). I have given due efforts to make this Research Monograph as fruitful one and to make it as informative as possible. I hope that this paper will not be the formality of academic course completion rather it will be a source of information for other purpose on this topic.

Sincerely yours,

_____

Ashraful Islam
ID No. LLB2203027024
Program: LL.B. (Honours)
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

DECLARATION

I declare that the Research Monograph on the topic **"Admissibility and Reliability of Digital Evidence in Criminal Trials: Challenges in the Modern Criminal Procedure System"** is my original work and that it has been prepared for the purpose of acquiring the LL.B. (Honours) Degree under the supervision of my supervisor. All sources have been cited and references given in the academic style.

_____

Ashraful Islam
ID No. LLB2203027024
Program: LL.B. (Honours)
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

CERTIFICATION

This is to certify that the thesis titled, **"Admissibility and Reliability of Digital Evidence in Criminal Trials: Challenges in the Modern Criminal Procedure System"**, has been prepared by the researcher under my guidance in Department of Law, Sonargaon University (SU).

This thesis is original and has not been previously submitted in whole or in part for any degree.

_____

Sunzida Akhter
Lecturer
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

ACKNOWLEDGEMENTS

I would like to express my special thanks to all those who have helped in the completion of this thesis. I would like to first and foremost express my gratitude to my supervisor for her guidance, constructive feedback and constant support during this research journey.

Thanks to all the judges, legal experts and law enforcement officials of Bangladesh who contributed their expertise on the actual challenges of digital evidence in court proceedings. I would also like to thank the faculty members of the Department of Law for their Academic support and encouragement.

I would like to express my gratitude to my family and friends to their constant support and patience throughout this research process. **"I am especially deeply grateful to my parents and brother; due to whose sacrifices I have been able to reach this position today."** Last, but not least, I accept that some of the defects I'm aware of on this document are my own.

Thank you

Ashraful Islam

Abstract

The mass explosion of information and communication technology and the growing digitization of human activity has made digital evidence a fundamental part of the contemporary criminal justice system. This thesis aims to explore the admissibility and reliability of digital evidence in the criminal trial in the modern criminal procedure system and its applicability in Bangladesh with comparison of some selected countries. The study presents an overview of the concept of digital evidence, the relevant legal and theoretical concepts and a discussion of the changing judicial interpretations in criminal trials regarding digital evidence.

The research reveals that Bangladesh has made remarkable progress with the Evidence (Amendment) Act 2022 that established a statutory definition of electronic records under sections 65A and 65B of the Evidence Act 1872. While this is a legal advancement, there are still practical issues to be addressed to ensure the authenticity, integrity and reliability of digital evidence. A lack of strong chain of custody, forensic infrastructure, technical knowledge, and uniformity in procedures remain challenges to the admissibility of electronic records in criminal cases.

The study also reveals that there are numerous opportunities for digital evidence to be manipulated and tampered with, and that new technologies such as artificial intelligence and deepfakes exist that can interfere with the integrity of digital evidence. The use of expert evidence and forensic analysis in the admissibility and evidentiary weight of the evidence has therefore become a major issue before the court. The practice of other jurisdictions, like India, United Kingdom, and the United States, underscores the significance of established legal norms, evidence collection procedures, and judicial uniformity when dealing with e-evidence. International instruments, especially the Convention on Cybercrime, stress the need for a harmonization of legal standards and cooperation among jurisdictions for the fight against digital crime and electronic evidence issues. The thesis posits that digital evidence can enhance criminal investigations and prosecutions, but can only do so if there is a strong legal reform, developing forensic infrastructure, training judges, and ensuring that procedures are followed correctly in order to make criminal trials fair and reliable.

Keywords: Digital Evidence, Admissibility, Reliability, Criminal Trials, Evidence Act 1872, Chain of Custody, Digital Forensics, Cybercrime, Electronic Records, Authentication, Cybersecurity, Bangladesh Criminal Procedure System, Artificial Intelligence, Deepfake Evidence.

CONTENTS

Chapter 1
Introduction

1.1 Background of the Study

The rapid advancement of information and communication technology has transformed modern society and significantly influenced the administration of criminal justice. Criminal activities are increasingly conducted through digital platforms, while evidence relating to criminal conduct is often stored or transmitted electronically. Mobile phones, computers, emails, social media communications, CCTV recordings, cloud storage systems, GPS data, and digital transaction records have become important sources of evidence in criminal investigations and prosecutions. As a result, courts worldwide are increasingly required to determine the admissibility and reliability of digital evidence in criminal proceedings.

Digital evidence has become particularly significant in the investigation of cybercrime, financial fraud, terrorism, organized crime, human trafficking, and other conventional crimes where electronic devices are involved. The growing dependence on technology has created both opportunities and challenges for law enforcement agencies. While digital evidence can provide accurate and objective information regarding criminal activities, concerns remain regarding authenticity, integrity, manipulation, and chain of custody. These concerns directly affect the admissibility and evidential value of such evidence in criminal trials.[1]

In Bangladesh, the legal framework governing evidence has traditionally been based on the Evidence Act 1872. However, the increasing use of digital technology exposed significant gaps in the traditional evidentiary rules. To address these challenges, the Parliament enacted the Evidence (Amendment) Act 2022, introducing provisions that formally recognize digital records as admissible evidence and establish procedures for proving such records before courts.[2] Despite these developments, practical and procedural challenges continue to exist regarding the collection, preservation, authentication, and evaluation of digital evidence.[3]

[1] George L Paul, *Foundations of Digital Evidence* (American Bar Association 2008) 5.
[2] Evidence (Amendment) Act 2022 (Bangladesh); Evidence Act 1872, ss 65A–65B.
[3] Khandker Tanbir, 'Admissibility of Digital Evidence in Bangladesh' (SSRN, 2022).

1.2 Concept of Digital Evidence

Digital evidence refers to any information of probative value that is stored, generated, transmitted, or received in digital form and can be used in legal proceedings. It includes emails, text messages, social media communications, CCTV footage, audio and video recordings, digital photographs, computer files, metadata, GPS information, and electronic transaction records.[4]

The Evidence (Amendment) Act 2022 defines digital records broadly to include any information generated, prepared, sent, received, or stored in magnetic, optical, electronic, or computer-based systems. Such records are legally recognized as documents and may be admitted as evidence subject to statutory conditions.[5]

Unlike traditional documentary evidence, digital evidence is highly vulnerable to alteration, deletion, duplication, and unauthorized access. Consequently, courts require additional safeguards to ensure its authenticity and reliability before accepting it as evidence in criminal proceedings.

1.3 Evolution of Technology in Criminal Justice

The criminal justice system has evolved alongside technological development. Initially, criminal investigations relied primarily on eyewitness testimony, physical evidence, and documentary records. However, the digital revolution has fundamentally changed investigative methods and evidentiary practices.

Technological tools such as digital surveillance systems, biometric identification, forensic software, mobile device extraction techniques, and artificial intelligence-assisted investigations have become integral components of modern law enforcement.[6] Digital evidence now plays a crucial role not only in cybercrime investigations but also in conventional criminal cases, including murder, theft, fraud, and corruption.

---

[4] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021) 12.

[5] Evidence (Amendment) Act 2022, s 3; digital records include CCTV footage, mobile phone records, audio and video files.

[6] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 28.

Many jurisdictions, including the United Kingdom, India, the United States, and Bangladesh, have amended their evidentiary laws to accommodate electronic records and digital evidence. Bangladesh's 2022 amendments introducing sections 65A and 65B into the Evidence Act represent an important step toward modernizing the country's evidentiary framework.[7]

1.4 Statement of the Problem

Despite legislative reforms, significant challenges remain regarding the admissibility and reliability of digital evidence in criminal trials. Digital data can be altered, fabricated, deleted, or manipulated without leaving obvious traces. Furthermore, inadequate forensic facilities, lack of trained investigators, insufficient technical expertise among legal practitioners, and procedural irregularities may compromise the integrity of digital evidence.

Another concern relates to maintaining an unbroken chain of custody. Failure to properly collect, preserve, and document digital evidence may lead to questions regarding authenticity and reliability. Additionally, courts often face difficulties in evaluating complex technological evidence due to the rapidly evolving nature of digital technologies. These challenges create uncertainty regarding the evidential weight and admissibility of digital records in criminal proceedings.

1.5 Research Questions

This study seeks to answer the following questions:

1. What constitutes digital evidence in criminal proceedings?
2. What legal principles govern the admissibility of digital evidence in Bangladesh?
3. What factors affect the reliability and authenticity of digital evidence?
4. What challenges are encountered in collecting, preserving, and presenting digital evidence in criminal trials?
5. How can the legal framework and criminal procedure system be improved to ensure effective use of digital evidence?

[7] Evidence Act 1872 (as amended), ss 65A and 65B.

1.6 Objectives of the Study

The primary objective of this research is to examine the admissibility and reliability of digital evidence in criminal trials within the modern criminal procedure system.

The specific objectives are:

- To analyze the concept and nature of digital evidence.
- To examine the legal framework governing digital evidence in Bangladesh.
- To identify challenges relating to admissibility and reliability.
- To evaluate the role of forensic and technological mechanisms in ensuring evidential integrity.
- To propose recommendations for improving the legal and procedural framework relating to digital evidence.

1.7 Significance of the Study

This study is significant because digital evidence has become a central component of contemporary criminal investigations and prosecutions. The increasing use of electronic devices in everyday life means that digital records are frequently presented before courts. Consequently, understanding the legal standards governing admissibility and reliability is essential for ensuring fair trials and effective justice.

The study will contribute to academic literature on evidence law in Bangladesh and may assist judges, lawyers, investigators, policymakers, and students in understanding the challenges associated with digital evidence. It may also support future reforms aimed at strengthening the evidentiary framework and enhancing judicial confidence in digital records.

1.8 Scope and Limitations

The scope of this study is primarily limited to the admissibility and reliability of digital evidence in criminal trials. It focuses on the legal framework of Bangladesh, particularly the Evidence Act 1872 as amended in 2022, relevant provisions of the Information and Communication Technology framework, and applicable criminal procedural laws.

The study also incorporates comparative references to selected foreign jurisdictions where necessary. However, due to limitations of time, resources, and access to judicial decisions, the research does not provide an exhaustive analysis of all international approaches to digital evidence.

1.9 Research Methodology

This research adopts a doctrinal legal research methodology. The study relies primarily on secondary sources, including statutes, judicial decisions, scholarly articles, books, law commission reports, journal publications, and electronic databases.

Relevant legislative materials, particularly the Evidence Act 1872, the Evidence (Amendment) Act 2022, and related laws concerning digital records, are examined to analyze the legal framework governing digital evidence. Comparative analysis is also undertaken where appropriate to evaluate international best practices and identify possible reforms for Bangladesh.

Chapter 2
Conceptual and Theoretical Framework of Digital Evidence

2.1 Meaning and Definition of Evidence

Judicial decisions are based on evidence. In legal matters, evidence means anything produced in front of a court that is used to prove or disprove a fact at issue. Evidence may include oral evidence, documents, material objects, and other evidence that helps the court to decide issues that are in dispute. [8]

Traditionally, the law of evidence was created with documents and witnesses in mind under the Evidence Act 1872 of Bangladesh. Technological advances, however, have broadened the types and nature of evidence that are available, while no longer limited to traditional evidence forms.[9]

Rapid adoption of communications, commercial, governance and social technologies has led to the generation of voluminous digitally stored information. As a result, contemporary law systems have acknowledged digital evidence as a valuable form of evidence that is utilized to demonstrate or disprove facts within criminal and civil cases.[10]

2.2 Traditional Evidence vs. Digital Evidence

Traditional evidence normally means any physical or tangible evidence including written evidence, signed contracts, tangible exhibits, fingerprints, weapons and oral evidence. The evidence is typically in a fixed and visible state, and is often directly accessible to the court.[11]

Digital evidence, however, is the information that is stored, processed and sent in electronic format. Digital evidence is not physical evidence and may not exist in any physical form, and may, unlike traditional evidence, require special hardware or software to access and interpret.[12]

[8] Adrian Keane and Paul McKeown, *The Modern Law of Evidence* (14th edn, Oxford University Press 2023) 3.
[9] Evidence Act 1872, s 3 (Bangladesh).
[10] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021) 15.
[11] Adrian Keane and Paul McKeown, *The Modern Law of Evidence* (14th edn, OUP 2023) 8.
[12] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 41.

There are multiple differences between digital and traditional evidence. Firstly, digital evidence may be copied, altered, transferred or deleted without visible evidence of change. Secondly, it could contain the secrets within its secret, including metadata that can be a valuable tool for investigation. Thirdly, digital evidence may be found in various jurisdictions because of cloud computing and Internet-based services, which can lead to jurisdictional and procedural issues regarding collection and presentation.[13]

Nevertheless, there are certain common elements to both traditional and digital evidence that must meet basic legal standards of relevance, authenticity, reliability, and admissibility. Courts should ensure that digital documents presented as evidence are accurate representations of the original documents, and have not been altered during collection or preservation.[14]

2.3 Types of Digital Evidence

Digital evidence can take many forms according to the technology involved and the type of information.

A. Emails

Emails are often a type of digital evidence. They often include information about criminal activity including fraud, conspiracy, cybercrime, corruption and financial offences. Email records can contain the content of the messages, attachments, times and dates, sender and recipient details, and metadata. Information like this can facilitate the investigators in reconstructing events and making connections between suspects.[15]

B. SMS and Chat Records

Records created by text messages and Instant Messaging apps like WhatsApp, Messenger, Telegram, and Signal can be used as evidence in criminal investigations. Such communications may include admissions, threats, directions, or information concerning the criminal liability. Increasingly, these records are being used in court to establish the facts of a case.[16]

[13] George L Paul, *Foundations of Digital Evidence* (American Bar Association 2008) 22.
[14] Mason and Seng (n 3) 28.
[15] Casey (n 5) 176.
[16] Stephen Mason, *Electronic Evidence* (5th edn, LexisNexis Butterworths 2017) 337.

C. Social Media Content

Social media is an important source of digital evidence. The content of a post, comments, photos, videos, private messages and activity on an account can be important to knowing what a suspect is doing, what he or she wants to do, who he or she is connected with, and where he or she is located. Terrorism, hate speech, cyber harassment, fraud and violent crimes have all been cases where social media evidence has been used.[17]

D. CCTV Footage

One of the most common types of digital evidence collected in criminal investigations is Closed-Circuit Television (CCTV) recordings. Witness evidence can be supported and supplemented with CCTV footage, which can give visual evidence of events, establish timelines and identify suspects. Problems with image quality, storage, editing and chain of custody can, however, impact on evidential reliability.

E. Computer Files

Information that is relevant to criminal investigations can be found in documents, spreadsheets, databases, photos, videos and other files stored on a computer. Unusual behavior or financial transactions, communications or attempting to cover up criminal activity can be detected in computer files.[18]

F. GPS Data

Smartphones, cars and navigation systems can generate GPS data to give accurate details about people's movements and location. This information could help determine proof of presence at a crime scene, corroborate an alibi or help reconstruct the crime.[19]

G. Cloud-Based Data

Cloud computing technologies enable users to store data remotely on other servers instead of their own machine. Cloud-based evidence is composed of Internet-based document files, email exchanges, photos, logs, backups and communication records. While cloud storage helps

[17] Eoghan Casey and others, *Digital Evidence and Computer Crime* (Academic Press 2011) 215.
[18] Paul (n 6) 97.
[19] Casey (n 5) 121.

access and storage, it also poses complex questions about jurisdiction, privacy and retrieval of data.[20]

2.4 Characteristics of Digital Evidence

There are a number of elements that make digital evidence different from conventional evidence.

Digital evidence is very fragile and can be modified, damaged or lost easily; and second, digital evidence is often complex and incomprehensible to those without the proper expertise. Even with regular use of a device, there can be changes in important data.[21]

Secondly, digital evidence can be reproduced. Electronic data can be replicated without any alteration of the content. This feature helps investigations, but also makes the contents liable to unauthorized duplication and use.

Thirdly, digital evidence may include metadata. Metadata is information about data, including creation dates, changes to the data, authors, and location information. This is information that may be useful as evidence for the reasons.[22]

Fourth, digital evidence is often found across several systems, devices and locations. This can often make it difficult for investigators to identify, collect and preserve relevant data.

Lastly, digital evidence demands the technology savvy to handle it appropriately in court. Increasingly, judges, lawyers and investigators are turning to forensic specialists to understand the meaning and veracity of electronic records.[23]

2.5 Theoretical Foundations of Evidence Law

The principles of evidence law are grounded in several theories that aim to make the judicial process fair, accurate and efficient. The primary goal of evidence law is to ascertain the truth.

[20] Mason and Seng (n 3) 401.
[21] George L Paul and Jason R Baron, 'Information Inflation: Can the Legal System Adapt?' (2007) 13 Richmond Journal of Law and Technology 10.
[22] Casey (n 5) 45.
[23] Mason and Seng (n 3) 53.

Courts are interested in establishing facts as closely as possible to the "true facts" based on the reliability and relevance of the information provided by the parties.[24]

The other significant theory is procedural justice. Evidence rules govern the gathering and presentation of evidence to guarantee an accused person a fair trial and to prevent wrongful convictions as much as possible.[25]

The theory of reliability is also a key component of evidence law. In general, evidence that has adequate guarantees of trustworthiness is admitted in court. For digital evidence, reliability is dependent on the collection, preservation, authentication, and forensic examination of the evidence.

The best evidence principle also dictates that parties shall present the best evidence that is available. Traditionally, this rule has been in favor of original documents, but with the advent of modern evidence law, electronic records are considered when statutes are met.[26]

2.6 Principles of Authenticity, Integrity, and Reliability

Three related principles – authenticity, integrity and reliability – underlie the admissibility of digital evidence.

Authenticity is the need for evidence to be proven to be authentic and from the claimed source. Before being admitted to evidence, a court must be convinced that a digital record is a digital record. Authentication can be done by witness testimony or by examination of the metadata, forensics, or by statutory authentication procedures.[27]

Integrity is related to completeness and not being altered of digital evidence. Because electronic data can easily be changed, courts require evidence to demonstrate that the evidence has not been altered since it was collected until it is presented at trial. Thus, it is important to maintain an adequate chain of custody.[28]

[24] Paul (n 6) 31.
[25] Mirjan Damaška, *Evidence Law Adrift* (Yale University Press 1997) 12.
[26] John H Langbein, *The Origins of Adversary Criminal Trial* (Oxford University Press 2003) 5.
[27] Keane and McKeown (n 1) 421.
[28] Mason and Seng (n 3) 67.

Reliability is the trustworthiness and accuracy of the evidence. Digital evidence should be collected in a way that is consistent with accepted forensic practices, stored properly, and displayed in a way that reduces the potential for error or manipulation. Reliability of electronic evidence is frequently assessed based on the processes and procedures employed in obtaining, storing, and analyzing the electronic evidence.[29]

These are the concepts that, aggregated together, create the conceptual basis for the admissibility and evidentiary value of digital evidence in contemporary criminal justice systems. The advent of digital technologies continues to cause change in the world and maintaining authenticity, integrity and reliability is as vital as ever for the public to be confident in criminal trials and for the administration of justice to be upheld.

[29] Casey (n 5) 58.

Chapter 3
Legal Framework Governing Digital Evidence in Bangladesh

3.1 The Evidence Act, 1872

The Evidence Act 1872 is the most important legislation that governs admission of evidence in Bangladesh. The Act was passed in the colonial era and originally applied to traditional methods of evidence, but new laws have been passed which include digital and electronic evidence.[30]

A major change has been brought by the Evidence (Amendment) Act 2022 which officially enables digital records to be used as evidence in court. A section—65A—was added to the Evidence Act to create the legal regime for admissibility of digital records, and section 65B imposes the conditions for the admissibility of electronic records.[31]

With Section 65B, digital records like emails, text messages, CCTV footage, digital photographs, computer-generated documents and electronic communications can be presented as evidence provided it meets the following procedural conditions. The requirement for proof in the provision must relate to how the electronic record is created, kept and maintained.[32]

This change in the evidence system is a major step in modernizing the system in Bangladesh. Unfortunately, there are still challenges that need to be addressed in terms of authentication, certification, forensic examination, and judicial review of electronic records. For this reason, courts need to take a nuanced approach in determining the source and authenticity of digital evidence before assigning it a value.[33]

3.2 Code of Criminal Procedure, 1898

In Bangladesh, criminal investigations, prosecutions and trials are conducted by following the procedure laid down in the Code of Criminal Procedure (CrPC) 1898. The Code does not

[30] Evidence Act 1872 (Bangladesh).
[31] Evidence (Amendment) Act 2022, ss 65A–65B.
[32] Evidence Act 1872 (as amended), s 65B.
[33] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021) 67.

specifically describe digital evidence but numerous provisions address the collection, preservation and presentation of electronic records in criminal proceedings.[34]

The Code's investigation process typically includes the seizure of electronic devices like computers, mobile phones, storage media and surveillance devices. Investigating officers have powers to search and seize which may be relevant to an offence.[35]

Procedural issues that impact on the admissibility and reliability of digital evidence include investigation, documentation of evidence, examination of witnesses, and report submission. Noncompliance with the procedural safeguards could undermine the evidentiary value of an electronic record and/or create chain of custody and authenticity challenges.

In criminal proceedings, digital evidence has become increasingly relevant and requests have been made for a specific part on Digital investigation, electronic search, Digital Forensic examination and Preservation of Digital evidence in the Criminal Procedure Code.[36]

3.3 Penal Code, 1860

The Penal Code 1860 is essentially the criminal substantive law of Bangladesh. Several offences in the Penal Code, which existed prior to the advent of digital devices and electronic evidence, may require the use of electronic devices or electronic evidence.

Many crimes, including cheating, forgery, criminal breach of trust, defamation, conspiracy, extortion and criminal intimidation, are now committed via digital platforms and electronic communications,[37] with emails, social media communications, digital documents and electronic transaction records often being vital to establishing the criminal liability.

The substantive laws contained in the Penal Code do not give specific rules about digital evidence, but it is clear that many offences for which digital evidence has an important role can be prosecuted using the substantive law in the Penal Code. Digital evidence is therefore often used to establish the elements of offences as outlined in the Penal Code in court.

[34] Code of Criminal Procedure 1898 (Bangladesh).
[35] Code of Criminal Procedure 1898, ss 94, 96 and related search and seizure provisions.
[36] Mizanur Rahman, 'Digital Evidence and Criminal Justice Reform in Bangladesh' (2023) 34 Bangladesh Journal of Law 115.
[37] Penal Code 1860 (Bangladesh).

3.4 Information and Communication Technology Act, 2006

The Information and Communication Technology Act 2006 (ICT Act) was the first all-encompassing law addressing cybercrime and electronic transactions in Bangladesh. The Act acknowledged the use of electronic records and electronic signatures and created offences for the interference with data, hacking, unauthorized access and cyber related misconduct.[38]

An important aspect of the enactment of the ICT Act was the acceptance of electronic records as legal records of information. The Act also gave law enforcement powers to investigate cyber offences utilizing computers and digital networks.[39]

One such section that sparked much controversy was Section 57 of the ICT act, which was seen as concerning the freedom of expression and possible misuse. The provision made it an offence to disseminate, publish, communicate, make available or share, electronically or otherwise, electronic information that offends or defamates, or is prejudicial to, public order.[40]

Although the ICT Act was a positive step towards the promotion of cyber regulation, it was criticized for being lacking in procedural protections and lags in provisions. Much of its provisions were replaced with future laws, such as the Digital Security Act 2018 and the Cyber Security Act 2023.

3.5 Digital security Act, 2018 (Historical Relevance)

To tackle the growing cyber threat and improve the legal regime of digital activities in Bangladesh, the Digital Security Act (DSA) 2018 was enacted. The Act made it illegal to breach computer systems, commit computer fraud, steal identities, engage in cyber terrorism, harass, harm, disturb or cause annoyance to others online or post destructive information online.[41]

The DSA was given investigative powers concerning digital devices and electronic records, which included search, seizure, examination and preservation, and it was significant in the context of digital evidence. Authorities had the power to gather and scrutinize electronic evidence pertinent to cybercrimes.[42]

[38] Information and Communication Technology Act 2006.
[39] Information and Communication Technology Act 2006, ss 54–56.
[40] Information and Communication Technology Act 2006, s 57.
[41] Digital Security Act 2018 (Bangladesh).
[42] Digital Security Act 2018, chs IV and VI.

But the Act drew significant criticism from human rights groups, the media, lawyers and international monitors. The term 'offences' was used very broadly; restrictions on freedom of expression were noted; and there was a risk of arbitrary enforcement.[43]

Though the DSA was later repealed, its historical value is still significant as it helps understand how Bangladesh adopted the modern attitude towards Cybercrime regulation and Digital investigations.

3.6 Cyber Security Act, 2023

The Cyber Security Act 2023, which superseded the Digital Security Act, is the main law regulating cybercrimes in Bangladesh. The new law was designed to rectify some of the criticisms leveled against the DSA, while keeping the legal systems in place to prevent cybercrime.[44]

The Cyber Security Act maintains provisions on unauthorized access, digital fraud, cyber terrorism, identity theft and computer offences. It also establishes the legal grounds for investigations and prosecution of cybercrime for the purposes of collecting and analyzing electronic evidence.[45]

The Act is significant for digital evidence because electronic records are crucial in cybercrime investigations, digital forensic analysis and technological expertise are essential. Computer logs, Internet records, communication data, cloud-based information and metadata are all commonly used as evidence of criminal responsibility.

While the Cyber Security Act is an improvement on some aspects, issues are yet to be taken care of in relation to implementation, technical capabilities, forensic infrastructure and the protection of fundamental rights in the context of digital investigations.[46]

[43] Amnesty International, *Muzzling Dissent Online: Digital Security Act in Bangladesh* (2021).
[44] Cyber Security Act 2023 (Bangladesh).
[45] Cyber Security Act 2023, relevant provisions concerning cyber offences and investigation powers.
[46] Transparency International Bangladesh, *Review of the Cyber Security Act 2023* (2023).

3.7 Relevant Rules and Regulations

Apart from the primary legislation, there are several subordinate legislations assisting in the regulation of digital evidence in Bangladesh. These include the rules on electronic signature, digital certification, information technology governance and cyber security standards.[47]

The Information Technology (Certification Authority) Rules provide a good framework to enable legal recognition of electronic authentication mechanisms and digital signatures. Such regulations contribute to establishing the authenticity of electronic documents and transactions.

Additionally, digital forensic laboratories, law enforcement and regulatory bodies often use technical standards and operational procedures for the collection, preservation, processing, and presentation of electronic evidence. Adhering to these standards increases the credibility and credibility of digital records in court submissions.[48]

Creating in-depth digital forensic procedures and evidence handling guidelines are still crucial for maintaining uniformity and reliability during the criminal justice process.

3.8 Constitutional Protection Regarding Fair Trial

The Constitution of the People's Republic of Bangladesh contains certain fundamental rights which are directly related to the admissibility and use of the digital evidence in criminal proceedings. Article 31 guarantees protection of law and the right to be treated in a way that is in accordance with law; Article 35 provides for important rights in the field of criminal justice and fair trial rights.[49]

Digital evidence must be used in accordance with constitutional principles of due process, fairness and equality before the law. It is essential that electronic evidence is obtained and used in a lawful manner and that accused persons have the opportunity to question the authenticity, accuracy and admissibility of such evidence.

Unauthorized surveillance, interception of communication or collection of digital information can be in contravention of constitutional protections relating to privacy and procedural fairness. Therefore, the Court is required to strike a balance between the State's legitimate interests in

[47] Information Technology (Certification Authority) Rules 2010 (Bangladesh).
[48] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 58.
[49] Constitution of the People's Republic of Bangladesh, arts 31 and 35.

effective law enforcement and the rights of the individual to a fair trial and protection from arbitrary interference.[50]

In a contemporary criminal justice system, constitutional protections are a crucial way to ensure that digital evidence is used to assist in the administration of justice while not infringing upon constitutional rights. In the ongoing development of digital technologies, principles of the constitution will play an ongoing role in defining the acceptable and fair handling of electronic evidence in Criminal proceedings.

[50] Mahmudul Islam, *Constitutional Law of Bangladesh* (3rd edn, Mullick Brothers 2012) 221.

Chapter 4
Admissibility of Digital Evidence in Criminal Trials

4.1 Meaning of Admissibility

Admissibility is the quality of evidence that is accepted as evidence in court. Evidence is admissible if it meets the requirements of the substantive and procedural laws, and is therefore admissible for the purpose of being considered by the Court in determining the facts of the case.[51] Evidence is distinct from evidential weight. The court may admit evidence, but it may not be very influential or credible if the evidence is unreliable or uncredible.

The use of admissibility in a criminal trial is a way of protecting against the use of unreliable, prejudicial or illegally obtained evidence. The court is obligated to decide whether the evidence meets the legal requirement of relevance, authenticity, reliability and procedural requirements before it can be admitted at trial.[52]

As digital technology has developed, courts have come across more and more of these digital records, including emails, text messages, CCTV footage, social media posts and computer-generated documents. This special character of digital evidence has led to the creation of a number of special legal provisions for its admissibility.[53]

4.2 General Rules of Admissibility

The Evidence Act 1872 is the general law that governs the admissibility of evidence in Bangladesh. Relevance is the preliminary and most basic basis for admissibility of evidence regardless of whether the evidence is traditional or digital.[54]

Along with relevance, evidence should also be legally obtained and properly presented before the court. Typically, evidence that cannot prove a material fact, that is not authentic, or is otherwise barred by law is not available in court.[55]

The general rules of evidence for traditional evidence also apply to digital evidence. But electronic evidence is more easily altered, duplicated, or manipulated than physical evidence,

[51] Adrian Keane and Paul McKeown, *The Modern Law of Evidence* (14th edn, Oxford University Press 2023) 45.
[52] Ian Dennis, *The Law of Evidence* (7th edn, Sweet & Maxwell 2020) 21.
[53] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021) 58.
[54] Evidence Act 1872, ss 5–16 (Bangladesh).
[55] Adrian Keane and Paul McKeown, *The Modern Law of Evidence* (14th edn, OUP 2023) 51.

and courts may have to rely on other evidence to ensure authenticity and integrity before accepting such evidence.[56]

The Evidence (Amendment) Act, 2022 has provided a better ground for admission of electronic record in Bangladesh by introducing digital records as admissible evidence with statutory conditions.[57]

4.3 Conditions for Admission of Electronic Records

The major laws in Bangladesh that regulate electronic evidence are sections 65A and 65B of the Evidence Act 1872 amended by the Evidence (Amendment) Act 2022. These provisions create certain circumstances for presentation of electronic records in judicial proceedings.[58]

Section 65B requires that information in an electronic record be admitted as evidence when the information was created during a period of time from a computer or digital device that was used regularly to store or process information. The information must have been entered into the computer system in the usual course of activities and the computer system must have been functioning in its normal manner at the relevant time.[59]

In addition, a certificate indicating the record, its method of production, and the fact it meets the statutory requirements must accompany the electronic record. The certification is a helpful protection against manipulation and fabrication.[60]

These provisions are based on those in vogue in the international scene and are similar to those provided in the Indian Evidence Act. The statutory conditions are provided to assure that electronic records admitted into evidence have adequate guarantees of authenticity and reliability.[61]

[56] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 44.
[57] Evidence (Amendment) Act 2022 (Bangladesh).
[58] Evidence Act 1872 (as amended), ss 65A–65B.
[59] Evidence Act 1872, s 65B.
[60] ibid.
[61] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021) 74.

4.4 Authentication Requirements

The process of establishing that something is authentic, or is what it claims to be is authentication. The concept of authentication is significant in the realm of digital evidence as electronic evidence can be altered without apparent indicators of alteration.[62]

Digital evidence can be authenticated in different ways in court. Email, text or electronic records can be established by witness testimony to be made by, or received by, a specific person. A forensic analysis by technical experts that data is not altered. Other means of verifying authenticity include using metadata, system logs, IP addresses, times and digital signatures.[63]

In a criminal trial, for instance, evidence of CCTV must be made available which accurately depicts what was recorded on the film and that it was recorded from the appropriate surveillance system. In the same way, social media communications should be connected to the accused by providing adequate evidence that the person owns or controls the account in question.[64]

Failure to authentication may result in significant risk of miscarriage of justice or wrongful conviction, and hence authentication is an essential requirement.

4.5 Best Evidence Rule

The Best Evidence Rule is an old rule of evidence that demands presentation of the most reliable and original evidence to establish a fact. Throughout the past, original documents have been preferred by the courts over copies because of the potential for alteration of copies.[65]

The Best Evidence Rule has come to mean different things over time, due to changes in technology. The digital environment allows for the creation of several copies of electronic records at the same time, which may make it less clear what constitutes an original and a copy. Modern evidence law thus emphasizes the authenticity and accuracy of the electronic record and not the production of a specific physical document.[66]

---

[62] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 58.
[63] George L Paul, *Foundations of Digital Evidence* (American Bar Association 2008) 113.
[64] Mason and Seng (n 11) 91.
[65] Ian Dennis, *The Law of Evidence* (7th edn, Sweet & Maxwell 2020) 383.
[66] Adrian Keane and Paul McKeown, *The Modern Law of Evidence* (14th edn, OUP 2023) 432.

The Evidence Act contains a statutory provision for meeting the Best Evidence Rule for electronic records in Sections 65A and 65B. If the statutory requirements are met, certified electronic records are considered to be as reliable as evidence provided by paper records.[67]

The modern approach thus focuses more on authenticity, accuracy and reliability, rather than on close adherence to the traditional understanding of originality.

4.6 Hearsay Issues in Digital Evidence

An out-of-court statement offered to prove the truth of its contents is called hearsay. Traditionally, hearsay is prohibited from being used in evidence unless it falls within one of the well-settled hearsay exceptions.[68]

Digital evidence often poses hearsay issues since electronic communications may include statements from people not present at trial. As a result, emails, text messages, social media postings and internet conversations might therefore be hearsay, depending on the intent of being introduced.[69]

The admissibility of such evidence depends on what it is used to prove, for instance, a text message that states someone committed a crime may be prohibited if it is only to prove that statement. The same message can, however, be used for other purposes, for example, to prove communication between two or more parties or the intentions of the sender.[70]

Courts must thus exercise great diligence in reviewing the nature and purpose of digital communications before deciding whether the hearsay rules apply, because the nature of digital communication may not be what it was in the past. This is an important issue in contemporary criminal trials, particularly in light of the growing reliance on electronic communications.

4.7 Burden of Proof

The burden of proof is the duty on a party to prove facts in support of their claims. The prosecution does not have to prove guilt beyond reasonable doubt in criminal cases.[71]

---

[67] Evidence Act 1872, ss 65A–65B.
[68] Dennis (n 15) 129.
[69] Mason and Seng (n 11) 245.
[70] Dennis (n 15) 136.
[71] Evidence Act 1872, ss 101–103.

If digital evidence is offered, the party using the evidence must prove its admissibility and authenticity. The prosecution has the burden of proof that the electronic record was lawfully obtained, properly maintained and an accurate representation of the information it claims to contain.[72]

If there is any question of tampering with, alteration of, fabrication of, or chain of custody for the evidence, additional proof may be required by the party introducing the evidence. This burden frequently is met through expert testimony, forensic reports and statutory certificates.[73]

If the authenticity is not established or compliance with statutory requirements are not met, the evidence may be excluded or its evidential weight may be reduced.

4.8 Judicial Discretion in Admitting Digital Evidence

Judicial discretion is an important factor in accepting digital evidence. While there are general rules in the statute, judges have discretion to determine the reliability, relevance, and probative value of the evidence before them.[74]

The court shall decide if the electronic records are properly authenticated, if the requirements of the statute are met, and whether the admission of the evidence would promote the interests of justice. The judges can exclude evidence, if there is a significant danger of unfair prejudice, unreliability or procedural irregularity.[75]

The lessons to be learned from comparative jurisprudence are useful in this regard. In Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal, the Supreme Court of India reiterated the necessity of complying with the requirements of the certificate, but also noted that there would be “limited” exceptions where certificates could not reasonably be obtained.[76]

The decisions are significant for Bangladesh as sections 65A and 65B of the Evidence Act are similar to the corresponding provisions in India. The interpretation of provisions related to electronic evidence, therefore, may be convincing for Bangladeshi courts.

---

[72] Casey (n 12) 60.
[73] Paul (n 13) 125.
[74] Keane and McKeown (n 16) 67.
[75] Dennis (n 15) 48.
[76] *Anvar PV v PK Basheer* (2014) 10 SCC 473 (India).

In the end, the discretion of the judge plays a fundamental role in preventing the introduction of unreliable digital evidence and at the same time preserving technologically relevant information that is necessary to effectively carry out criminal justice.

Chapter 5
Reliability and Evidentiary Value of Digital Evidence

5.1 Meaning of Reliability

Reliability is about the extent to which evidence is believed to be a true reflection of the facts at issue in a legal case. Reliability is a "fundamental" requirement in criminal trials, in which court decisions can have a significant impact on the rights, liberty and reputation of people. Inaccurate evidence can result in miscarriages of justice, whether for conviction or acquittal.[77]

In the field of digital evidence, reliability has to do with the fact that an electronic record faithfully captures the information that was originally created, transmitted, received, or stored. Digital evidence can be copied, altered, deleted or manipulated without much difficulty, so that courts must be cautious as to the authenticity of evidence presented.[78]

The reliability of digital evidence relies on a number of factors such as how it was collected, preserved, the chain of custody, authentication, forensic examination and the competency of the persons who are dealing with the evidence. Therefore, the reliability of an electronic record may rely on more than just the information contained in the record, it can also depend on the means by which the information is acquired and placed before the court.[79]

5.2 Integrity of Electronic Records

Integrity is the condition of the electronic records from their creation or collection until they are presented in court that they are complete and unchanged. An electronic record is integrity if there is reasonable assurance that the record has not been altered, corrupted, or tampered with.[80]

Integrity is a key concept as digital information is easily altered. The impact of one change in a computer file, image, email or database can have a huge impact on the evidence. Thus, it is important for courts to have confidence that electronic evidence has not been altered in the investigative and judicial process.[81]

---

[77] Ian Dennis, *The Law of Evidence* (7th edn, Sweet & Maxwell 2020) 21.
[78] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021) 61.
[79] George L Paul, *Foundations of Digital Evidence* (American Bar Association 2008) 114.
[80] Mason and Seng (n 2) 75.
[81] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 57.

Digital Evidence is protected in various ways through technological mechanisms. These range from cryptographic hashing, digital signatures, access control, secure storage and forensic imaging. A hash value is a special value that is generated from the electronic data and is different for each value. As long as there is any minor change, the hash value will be different, which means that something may have been changed.[82]

The integrity of electronic records is important because evidence that cannot be presented that it is complete and unaltered can be deemed unreliable and possibly inadmissible or less weighty before the court.

5.3 Chain of Custody

Chain of custody is a documented process which documents the collection, handling, transfer, storage, examination, and presentation of evidence from the time it is collected until it is introduced into evidence before a court.[83]

A proper chain of custody is especially critical for digital evidence as electronic data is often easily able to be altered and there is no obvious evidence that it has been altered. A thorough documentation of the procedure in which evidence is handled is therefore necessary, including who collected the evidence, when, how, who stored it, who retrieved the evidence, and the procedure for evidence handling.[84]

A chain of custody assists in establishing that evidence presented at trial is the same as the evidence collected during the investigation, and that the evidence has not been altered or tampered with. However, loopholes or discontinuities in the chain of custody can create problems as far as authenticity and reliability. Defense counsel can challenge electronic evidence if there is a deficiency in recording of handling or if there is no way to exclude unauthorized access.[85]

Chain of custody is receiving greater attention in Bangladesh, especially since the digital evidence was recognized in the Evidence (Amendment) Act 2022. Thus, it is critical to implement sound evidentiary management procedures to help secure judicial confidence in e-records.

---

[82] ibid 62.
[83] Casey (n 5) 71.
[84] George L Paul, *Foundations of Digital Evidence* (American Bar Association 2008) 131.
[85] Casey (n 5) 75.

5.4 Metadata and Digital Footprints

Data that provides information about data. Information in metadata may also include important information that is not obvious from the content of the document or communication.

Some examples of metadata are the date and time that an email was sent, the author of a document, where a photograph was taken, the device on which a file was created, and records of further changes to a file. This information can help investigators determine timelines, known individuals, and to see if the image has been altered, as well as verify authenticity.

Digital footprints are a residue of what a user does with digital technologies. Digital footprints include things like Internet activity, login information, search history, communications, GPS tracking, social media, and transaction history.[86]

Metadata and digital footprints can often be significant circumstantial evidence in criminal investigations. The location data of a mobile phone could bring a suspect close to a crime scene, for instance, and metadata can indicate that a document was made after a suspected event took place. As a result, the metadata is now an increasingly crucial source of evidence in today's criminal trials.

5.5 Risk of Manipulation and Alteration

Manipulation and alteration of the digital evidence is one of the biggest issues with digital evidence. The electronic records are not as tangible as physical evidence and can be altered, duplicated, deleted or created without any physical trace.[87]

Technologies have developed to make digital information more manipulated. It is difficult for courts to decide whether the documents are authentic because they can be edited, video manipulated, false emails sent, altered documents and even those that are AI generated.[88]

There's another worry with the arrival of “deepfake” technology. Deepfakes are videos and audio recordings created with AI that appear to be authentic but are produced by someone else, and thus can be used to impersonate a person in order to portray them as doing something they

[86] Casey (n 5) 145.
[87] Mason and Seng (n 2) 81.
[88] George L Paul (n 8) 118.

did not actually do. These technologies raise significant issues of criminal investigation and judicial proceedings.[89]

To meet these challenges, digital forensic analysis, expert testimony, metadata analysis, and technical verification procedures are becoming tools for courts to turn to. But one of the largest challenges for digital evidence reliability is the possibility for manipulation.

5.6 Digital Forensics & Expert Testimony

Digital forensics experts use unique tools and techniques to recover deleted files, review communications history, scrutinize metadata, trace illegal access, and confirm the authenticity of electronic records.[90] Digital forensic experts can recover deleted files, examine communications history, review metadata, trace illegal access, and confirm the authenticity of electronic records using unique tools and techniques.

Digital forensics has become a major part of the criminal justice system in today's world. A court often relies on a forensic expert to present matters of great complexity and technological knowledge to the general witness and court that do not necessarily know how to. Expert testimony can help the court to understand how digital evidence has been acquired, if and how it has been altered, and if it has been altered, whether accepted forensic procedures were followed.[91]

The Evidence Act allows for the opinions of experts in science, technology and specialized knowledge. As a result, the digital forensic specialist is able to offer opinion on the authenticity, integrity and reliability of electronic evidence.[92]

But there is a need to carefully check expert evidence. The selection of the expert, the means by which he or she arrived at his or her conclusions, and the findings' agreement with scientific norms must all be considered. The value of digital evidence will be compromised if it is relied upon based on an expert who is unqualified or on faulty forensic processes.

[89] Robert Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753.
[90] Casey (n 5) 3.
[91] Mason and Seng (n 2) 112.
[92] Evidence Act 1872, s 45.

5.7 Standards for Evaluating Reliability

Different standards may be used by courts to assess the reliability of digital evidence. The evidence has to be authenticated, in that there must be credible evidence that the evidence is what it claims to be. Authentication may include testimony, forensic analysis, verification of metadata, and satisfy statutory requirements.[93]

Second, courts review evidence of the integrity of the electronic record. Any evidence that has been tampered with, altered or not sufficiently preserved may be considered unreliable.[94]

Third, judges are mindful of legal and procedural issues related to the collection, storage and presentation of digital evidence. Non-compliance with statutory requirements could impact admissibility and evidentiary weight.

Fourthly, the credibility of the expert testimony and forensic reports relied upon for evidence are judged. Scientific procedures used in forensic analysis should be transparent, reproducible and in line with accepted professional standards.[95]

Lastly, courts determine the evidence based on the circumstances and other evidence available. Digital evidence is seldom the sole evidence; rather, evidence from witnesses and physical evidence and other electronic evidence should corroborate the reliability of digital evidence.[96]

Thus, legal, technical and procedural considerations are all factors that contribute to the reliability of digital evidence. With the continuing evolution of technology, courts need to establish strict requirements that will allow them to weigh the evidence value of digital information with the potential for manipulation, error and misuse. The success in criminal trials of digital evidence in the future relies heavily on the establishment of strong forensic practices, judicious skills and adequate legal protections.

[93] Evidence Act 1872 (as amended), ss 65A–65B.
[94] Casey (n 5) 60.
[95] Mason and Seng (n 2) 117.
[96] Ian Dennis, *The Law of Evidence* (7th edn, Sweet & Maxwell 2020) 26.

Chapter 6
Challenges in Collecting, Preserving, and Presenting Digital Evidence

6.1 Technical Challenges

With the growth of electronic evidence in criminal investigations, law enforcement agencies and courts are faced with many new technological problems. Electronic data is not stored on a single device, network or platform like traditional evidence. Specialized tools and technical expertise are needed to retrieve, collect and analyze such evidence.[97]

Today's digital devices produce a vast amount of data for investigators to sift through in order to find the relevant information quickly. The smartphone, computer, cloud-based storage systems, and internet-connected devices may have thousands of files, communications and records many of which are encrypted or hidden.[98]

Additionally, the rapid advancement of technology also continually produces new types of digital evidence. Law enforcement has a hard time keeping up with the latest technological advances, software applications, and communications platforms. Technical limitations also can negatively affect the effectiveness of criminal investigations and may diminish the evidentiary value of digital records.

6.2 Data Encryption

Encryption is among the biggest problems in today's criminal investigations. Encryption is a critical component of privacy and cybersecurity, but can also be a barrier to criminal investigations.[99]

End-to-end encryption is used by many communication platforms, such as messaging applications and cloud services. In this system, the sender and the recipient are the only ones who have access to the content of the communications, by means of keys. This can make it difficult for law enforcement to get evidence that is relevant to criminal investigations.[100]

With the ubiquity of encryption, there's been an ongoing debate between privacy groups and law enforcement agencies. Private rights to privacy must be well safeguarded against

[97] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 15.
[98] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021) 102.
[99] Casey (n 1) 287.
[100] Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (Yale University Press 2017) 183.

unwarranted spying but undue limitation on access to encrypted information could hinder criminal investigations and undermine the administration of justice.[101]

The challenge is especially critical for Bangladesh as compared to technologically advanced jurisdictions, where it is evident that capabilities in digital forensics are limited. As a result, encrypted data can pose a significant challenge to the ability to obtain reliable electronic evidence.

6.3 Data Recovery Issues

One of the biggest issues is the recovery of lost, damaged or inaccessible digital data. Often times, evidence is lost or compromised due to the actions of criminal suspects deleting evidence, formatting storage media, or physically damaging equipment.[102]

While modern forensic tools can often recover deleted data, the factors involved with each job can vary greatly between successful recovery and failure, such as the type and condition of the device, the level of damage, and the amount of elapsed time since the deleted file was removed. Sometimes, the recovered data can be incomplete or corrupted, leading to concerns about its authenticity and reliability.

As a result, investigators have to apply advanced forensic tools and techniques to identify and recover data and information that can be effectively used in court proceedings, or to disambiguate the information once recovered, where it has been subjected to encryption, overwriting or advanced anti-forensic techniques designed to hide the trace.[103]

6.4 Cross-Border Data Storage

The globalization of digital technologies has caused a lot of problems with respect to jurisdiction in the context of criminal investigations. A number of digital service providers keep data on foreign servers outside the country where the investigation is taking place.[104]

For instance, communications created in Bangladesh can be saved on servers in the USA, the Republic of Singapore, Ireland or other regions. This information may be difficult to obtain,

[101] Orin S Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106 Georgetown Law Journal 989.
[102] Casey (n 1) 213.
[103] ibid 221.
[104] Mason and Seng (n 2) 401.

and may require international cooperation, mutual legal assistance procedures, or requests to foreign service providers.

Cross-border data access can be a lengthy and complex process. A lack of uniformity in the laws and regulations of various countries concerning privacy, data protection and government access to information can make investigations slower to conduct and make evidence difficult to collect.[105]

The lack of complete international treaties on digital evidence poses further difficulties for Bangladesh. Procedural challenges often arise in trying to obtain foreign electronic records, and can impact the prosecution of cybercrime and transnational crimes.

6.5 Cloud Computing Challenges

Cloud computing revolutionized the way people and companies store data. Instead of data being stored in local devices, more and more people are turning to cloud computing services where data is stored on remote servers that can be accessed via the internet. Users are increasingly using cloud-based services, in which data is stored on a remote server to be accessed via the internet, rather than local devices.[106]

It has many benefits with respect to accessibility and data management, but cloud computing presents complex evidentiary issues. Cloud data can be located in different jurisdictions, copies of the data might be stored in multiple servers, and the data security might differ.

The exact location of cloud-based data can be challenging for investigators to determine, as are the legal access rules when accessing it. In addition, cloud service providers could have their own policies concerning data retention, disclosure, and user privacy.[107]

Ownership, control, and jurisdiction issues are common when cloud evidence is submitted to court. These complexities mean courts must evaluate the authenticity and reliability of e-records from cloud storage.

[105] Council of Europe, *Convention on Cybercrime (Budapest Convention)* (2001).
[106] George L Paul, *Foundations of Digital Evidence* (American Bar Association 2008) 142.
[107] Mason and Seng (n 2) 417.

6.6 Preservation of Electronic Records

It is critical to preserve electronic records to ensure they remain reliable and secure as electronic evidence. Electronic information is easily alterable, corruptible and can be lost. Important data and metadata can change even during normal use of a digital device.[108]

Investigators must adhere to forensic procedures in order to properly preserve. These processes can involve creating forensic copies of storage media, calculating hash codes, allowing only authorized access, and securely storing media.

Lack of proper preservation of digital evidence can affect admissibility and evidential value of the evidence. In cases where investigators are unable to prove that there was no alteration of the evidence from the time collected to the time it is presented at trial, courts may doubt its authenticity when the evidence is electronic.

Preserving electronic evidence in criminal proceedings, and the development of standardized protocols in Bangladesh is a priority concern.

6.7 Lack of Technical Expertise

Digital evidence must be used properly and with a certain level of expertise. All investigators, prosecutors, defense lawyers and judges should be familiar with the basic technical principles of digital devices, forensic techniques, metadata, encryption and electronic communications.[109]

But there are few qualified digital forensic specialists available in many criminal justice systems, especially in the developing countries. It is not an exception in the case of Bangladesh. The quality of investigations and the analysis of electronic evidence may be impacted by a lack of specialized training and forensic resources.

Many judges are asked to deal with complicated technological questions that involve interpretation of technology reports and technical evidence. The authenticity, reliability and importance of digital evidence may be challenging for courts to evaluate if they are not properly trained.

Hence, capacity-building programmers and special education programs are crucial in enhancing the administration of digital justice in Bangladesh.

---

[108] Casey (n 1) 57.
[109] Paul (n 10) 165.

6.8 Cost of Digital Forensic Investigation

Digital forensic investigations can be costly and time consuming. The specialized software, equipment, safekeeping and experts needed are expensive.

Many advanced forensic tools which can recover deleted files, analyze encrypted devices, and large amount of data can be costly for licenses and maintenance. In addition, a complex investigation can involve more than one expert, which can make the investigation process more expensive.

Forensic infrastructure is often constrained by financial resources in developing countries. Resource constraints can impact the availability of advanced forensic technologies and may even slow down the collection of electronic evidence in Bangladesh.[110]

Digital forensic investigations can therefore be very expensive leading to differences in access to justice and the effective prosecution of technologically advanced crimes.

6.9 Procedural Difficulties in Court

There are multiple procedural issues when presenting digital evidence in court. It is the duty of courts to ensure that the electronic records meet legal standards for admissibility, authenticity and reliability. Technical certification and documentation may be required for compliance with statutory requirements, such as under section 65A and 65B of the Evidence Act.[111]

Complicated technological evidence is a problem to many judges and lawyers. Legal practitioners accustomed to the traditional evidentiary concepts may not be familiar with the technical terms, forensic report interpretation, metadata analysis, or digital authentication procedures.[112]

The other issue relates to the assessment of expert testimony. Forensic techniques need to be scientifically sound and any expert statements need to be backed up by evidence for the court. There can also be conflicting expert opinions, which can further cloud the decision-making process in court.

Furthermore, the time needed to secure forensic reports, the lack of technology in the courts, and procedural uncertainties about digital evidence can lengthen the criminal process,

[110] Transparency International Bangladesh, *Cyber Governance and Digital Investigation Challenges in Bangladesh* (2023).
[111] Evidence Act 1872 (Bangladesh), ss 65A–65B.
[112] Mason and Seng (n 2) 112.

degrading the effectiveness of the criminal process and potentially impacting public trust in the administration of justice.[113]

To summarize, there are many technical, legal, and procedural issues that must be overcome when the collection, preservation, and presentation of digital evidence. Technical limitations, financial limitations, courtroom process limitations, cloud computing, failure to preserve, lack of technical skills, cross-border investigations, and difficulties in recovering digital evidence all impact on the admissibility and reliability of digital evidence. To bring digital evidence to the proper and efficient administration of criminal justice in Bangladesh, these challenges need to be addressed.

[113] Ian Dennis, *The Law of Evidence* (7th edn, Sweet & Maxwell 2020) 44.

Chapter 7
Judicial Approach and Case Law Analysis

7.1 Important Bangladeshi Cases on Digital Evidence

Judicial interpretation has largely been the path to the development of digital evidence law in Bangladesh. The Evidence Act 1872 previously had no specific provisions that admitted electronic records as evidence. As a result, the use of traditional rules of evidence had to be understood in the context of technological advances.[114]

The case of Mrs Khaleda Akter v State (1985) is one of the earliest and one of the most important cases relating to electronic evidence in Bangladesh. Here, the court decided if a video cassette recording was a document as per section 3 of the Evidence Act. The court's interpretation was broad and it did not hesitate to consider information on magnetic tapes obtained by technological means as a document.[115] This was an important judicial act of recognition of technologically generated evidence.

The other important case is the trial concerning the assassination of Bangabandhu Sheikh Mujibur Rahman, in the case of Major Md Bazlul Huda v State. In the course of the trial, the prosecution made use of video recordings and televised interviews of some of the accused in which they had given statements. The Appellate Division addressed the admissibility of electronic recordings and noted that electronic recordings could be received as evidence if they could be proved to be authentic. The Court stated however, that the original recording is required and proper certification is required if the authenticity of the material is disputed.[116]

The rulings reflect the judiciary's willingness to make adjustments to the rules of evidence in the age of technology, even before any law was passed to accommodate it.

[114] Khandker Tanbir, 'Admissibility of Digital Evidence in Bangladesh' (2022) SSRN Electronic Journal.
[115] *Mrs Khaleda Akter v State* 37 DLR (AD) 275 (1985). Discussed in academic commentary on electronic evidence in Bangladesh.
[116] *Major Md Bazlul Huda v State* 63 DLR (AD) 1; discussion of video and electronic evidence.

7.2 Judicial Interpretation of Electronic Records

Judicial interpretation was very important in bridging the gap in legislation left by the Evidence (Amendment) Act 2022. The Evidence Act, section 3, which defined the term "document" used the broadest possible interpretation by the courts.[117]

The judiciary was aware of the changes in the ways in which information was stored and communicated by technology. Courts have also come to recognize that data recorded on magnetic tapes, electronic documents and digital media may be used as documentary evidence, not just paper documents.[118]

This interpretative method was based on the notion that the law should adapt to changes in society and technology. The precedent set by judicial recognition of video and audio recordings, and of electronically stored information, set the groundwork for the subsequent statutory recognition of digital evidence.[119]

In 2022, the introduction of sections 65A and 65B, in effect, codified principles which had arisen before through judicial reasoning and practice.

7.3 Use of Digital Evidence in Criminal Convictions

Digital Evidence is increasingly being collected and utilized in Criminal Investigations and Prosecutions in Bangladesh. The use of CCTV footage, mobile phone messages, call details records (CDRs), social media messages, digital photographs and electronic transaction records is now commonplace in investigations and prosecutions.[120]

The role of electronic evidence in the establishment of criminal responsibility has been shown in several high-profile criminal cases. CCTV footage has assisted in the identification of suspects, crime scene reconstruction, providing timelines and corroborating witness evidence. Likewise, mobile phone location data and telephone records have helped investigators trace criminals to their crimes.[121]

But, in most cases, the courts in Bangladesh do not only depend on electronic evidence in making decisions on criminal responsibility. However, electronic records are typically

[117] Evidence Act 1872 (Bangladesh), s 3.
[118] *Mrs Khaleda Akter v State* 37 DLR (AD) 275 (1985).
[119] Rajib Kumar Deb, 'Admissibility of Digital Evidence' (The Daily Star, 2019).
[120] Evidence (Amendment) Act 2022; recognition of CCTV records, mobile phone records and digital records.
[121] Rajib Kumar Deb, 'Admissibility of Digital Evidence' (The Daily Star, 2019).

reviewed with other evidence, such as witness statements, forensic reports, physical evidence, and other supporting documents. This reflects the judiciary's prudence about the possible risks of manipulation, fabrication and misinterpretation from electronic evidence.[122]

As digital evidence has become a more common part of criminal convictions, digital competency has become more prominent in the criminal justice system.

7.4 Analysis of Supreme Court Decisions

The Supreme Court of Bangladesh has played a crucial role in developing the law on electronic evidence. While there are still only a few decisions specifically concerning digital evidence, it is possible to derive some important principles from these decisions.

First, the Court has repeatedly put the emphasis on authenticity. Electronic evidence is only admissible in criminal trials when it is demonstrated to be authentic and from the claimed source.[123]

Second, the Court has held that technological evidence should not be excluded simply because it is not the traditional type of documentary evidence. Rather, courts are urged to review whether there are adequate safeguards to ensure reliability and integrity.[124]

Third, procedural compliance has become a key concern of judicial decisions. This seems to be in recognition of concerns about manipulation or the need to retain confidence in electronic evidence in cases where electronic evidence is challenged, as the Appellate Division has stressed the importance of original recordings and proper certification in Major Md Bazlul Huda v State.[125]

The introduction of sections 65A and 65B have enhanced the existing legal landscape that courts have at their disposal. Going forward, the Supreme Court will likely be concerned with the meaning of certification, standards of authentication, forensic reliability, and the evidentiary weight to be considered for various types of digital evidence.

---

[122] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021) 87.
[123] *Major Md Bazlul Huda v State* 63 DLR (AD) 1.
[124] *Mrs Khaleda Akter v State* 37 DLR (AD) 275 (1985).
[125] *Major Md Bazlul Huda v State* 63 DLR (AD) 1.

7.5 Comparative Study of Selected Foreign Cases

Comparative jurisprudence can be helpful for Bangladesh as the problem of admissibility and reliability of digital evidence have been faced by many jurisdictions.

The Indian Supreme Court Judgement in Anvar P.V. v P.K. Basheer (2014) is one of the most impactful decisions. The Court observed that electronic records would be admissible only if the conditions, as provided in section 65B of the Evidence Act, were fulfilled. The judgment highlighted that the requirements for certification are binding and are a condition precedent to admissibility.[126]

This means that the significance of Anvar P.V. is not confined to India as Bangladesh has passed the Evidence (Amendment) Act, 2022 containing sections 65A and 65B similar to the sections in India's Evidence Act, 1872. In this regard, the justification in Anvar P.V. holds a lot of value to Bangladeshi courts.

Another pivotal case in Indian law is the case of Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020). Supreme court reaffirms the requirement for certificates under section 65B and provides clarity on some of the procedural aspects of producing electronic evidence. The Court noted that electronic evidence is particularly vulnerable to alteration and manipulation and that special precautions should be taken when dealing with it.[127]

British courts have taken a pragmatic stance to electronic evidence. Issues of admissibility have been replaced by issues of authenticity and evidential weight. British courts generally assume that a computer system is functioning properly, unless there is evidence to the contrary.[128]

The Federal Rules of Evidence in the United States dictate that parties must gain admission to electronic evidence by authentication. The authenticity of metadata, expert testimony, system logs and forensic analysis are common means American courts use to establish authenticity.[129]

These are a few themes that emerge from these jurisdictions' experience. First, there continues to be a strong emphasis on authenticity and integrity. Second, there is a more increased reliance by courts on technical expertise and forensic science. Third, there needs to be the reform of legislation to allow for technological innovations and safeguard fair trial rights.

---

[126] *Anvar PV v PK Basheer* (2014) 10 SCC 473 (India).
[127] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1 (India).
[128] Stephen Mason, *Electronic Evidence* (5th edn, LexisNexis 2017) 143.
[129] Lorraine v Markel American Insurance Co, 241 FRD 534 (D Md 2007).

Comparative jurisprudence offers guidance to the interpretation of Bangladesh's recent laws on digital evidence. The history of India, the United Kingdom and the United States indicates that a blend of statutory protections, judicial oversight, and technology skills is necessary for effective regulation of digital evidence. With the advancement of digital technologies, Bangladeshi courts will be more instrumental in the fair and effective administration of criminal justice, contributing to the use of digital evidence.

Chapter 8
Comparative Study of International Practices

8.1 Digital Evidence Framework in the United Kingdom

One of the most sophisticated systems regulating digital evidence in the United Kingdom is in place. Electronic evidence is normally governed by statutory rules, common law and forensic guidelines. British courts, in contrast to many jurisdictions which have specific statutory criteria for admissibility, take a broader approach to electronic evidence, with relevance, authenticity and reliability being the key factors.[130]

The Criminal Justice Act 2003 and the Police and Criminal Evidence Act 1984 (PACE) bring with them significant procedural safeguards surrounding the acquisition and use of evidence in criminal cases.[131] Electronic communications like emails, CCTV footage, digital photographs, mobile phone data and computer files are commonly introduced in criminal trials, provided they can be proved to be authentic.

An important aspect of the UK approach is the assumption that computer systems are working properly, unless there is evidence to the contrary. This principle decreases the need to prove technical reliability of computer-generated evidence in all cases, but if doubts do exist with regard to the integrity or authenticity of the computer system, expert testimony and forensic analysis may be required by the court.[132]

The United Kingdom has also produced in-depth digital forensic standards via ACPO Principles of Digital Evidence, which focus on preservation, integrity and accountability for the management of electronic evidence.[133] These digital forensic principles are regarded as the best practice standards and have been used internationally.

[130] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021) 133.
[131] Police and Criminal Evidence Act 1984 (UK); Criminal Justice Act 2003 (UK).
[132] Stephen Mason, *Electronic Evidence* (5th edn, LexisNexis 2017) 143.
[133] Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence* (5th edn, 2012).

8.2 Digital Evidence Framework in India

The India law on digital evidence has special relevance in the context of Bangladesh, as the Evidence (Amendment) Act 2022 provides provisions that mirror sections 65A and 65B of the Indian Evidence Act 1872.[134]

This was the first major piece of legislation in India to deal with electronic records and cybercrime, the Information Technology Act 2000. It introduced a new section 65B in the Indian Evidence Act that made electronic records admissible as evidence and established conditions for admissibility and formal requirements for certification to ensure authenticity and reliability.[135]

These provisions have been the subject of a significant amount of interpretation by the Indian judiciary. In Anvar P.V. v P.K. Basheer, the Supreme Court made it abundantly clear that the production of electronic evidence must be accompanied with a compliance with the requirements of section 65B as it is subject to manipulation and requires extra protections.[136]

In Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal, the Supreme Court once again reiterated that a certificate under section 65B is necessary and clarified issues of procedure relating to electronic records.[137]

The experience in India has shown the need for harmonization of statutory provisions with judicial interpretation for the consistent treatment of digital evidence. The law in Bangladesh is increasingly similar to the Indian law model, and these rulings could be helpful in leading its courts.

8.3 Digital Evidence Framework in the United States

In the United States, a vast body of legislation and case law has been created to address the issue of digital evidence. The primary rules governing electronic evidence are those of the Federal Rules of Evidence (FRE) that address issues of relevance, authentication, hearsay and evidential reliability.[138]

---

[134] Evidence (Amendment) Act 2022 (Bangladesh).
[135] Information Technology Act 2000 (India).
[136] *Anvar PV v PK Basheer* (2014) 10 SCC 473 (India).
[137] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1 (India).
[138] Federal Rules of Evidence (United States).

In order to be used, electronic evidence must be authenticated, as required by Federal Rule of Evidence 901 Authentication can be by evidence that the evidence is authentic, such as witness testimony, metadata analysis, expert evidence, evidence from a system or by other means.10[139]

The U.S. courts have one of the most flexible attitudes towards digital evidence. Courts do not require specific things to be certified, but will consider the circumstances of each case. Various methods are used to determine reliability, including metadata, digital footprints, email headers, IP addresses, and reports from the forensics. The following are common ways of determining reliability: metadata, digital footprints, email headers, IP addresses, and reports from the forensics.[140]

The case of Lorraine vs Markel American Insurance Co is significant. The Court gave detailed directions on admissibility of electronically stored information and reiterated the criteria for admissibility of E-SI in terms of relevance and authenticity, hearsay, originality and probative value.[141]

The ease with which electronic evidence can be evaluated and the flexibility of the judges emphasizes the need for technology and flexibility in examining electronic evidence in the United States.

8.4 International Standards and Best Practices

There are many guidelines and standards established by international organizations and professional bodies on digital evidence. These standards are designed to provide consistency, reliability and fairness in the management of electronic records in criminal investigations and judicial proceedings.[142]

The National Institute of Standards and Technology (NIST) has created comprehensive guidelines on the collection, preservation, examination and presentation of digital evidence.14[143]

[139] Federal Rules of Evidence, Rule 901.

[140] George L Paul, *Foundations of Digital Evidence* (American Bar Association 2008) 113.
[141] *Lorraine v Markel American Insurance Co* 241 FRD 534 (D Md 2007).
[142] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 85.
[143] National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response* (SP 800-86).

Likewise, The International Organization on Computer Evidence (IOCE) has adopted a set of principles which focus on the integrity of evidence and sound documentation of the investigative process.[144]

Typical good practices found internationally are:

- Handling the chain of custody.
- Utilizes forensic imaging instead of examination of original devices.
- Maintaining system logs and metadata.
- Using recognized forensic tools and procedures.
- Ensuring appropriate evidence of investigative process.
- Using qualified experts in forensic analysis.[145]

The standards seek to increase the trustworthiness and acceptance of digital evidence and reduce the risk of contamination or alteration.

8.5 Budapest Convention on Cybercrime

The most significant international treaty dealing with cybercrime and digital evidence is the Convention on Cybercrime or the Budapest Convention. The Convention, adopted by the Council of Europe in 2001, aims at harmonization of international legislation against cybercrime, more effective international cooperation and electronic evidence collection.[146]

The Convention includes provisions on illegal access, interference with data, computer-related fraud, child exploitation offences and other kinds of cybercrime. Importantly, it also provides procedural procedures in relation to preservation, search, seizure and disclosure of electronic evidence.[147]

One of the greatest merits of the Convention is its focus on cooperation between the international community. Digital evidence may often span jurisdictions, and effective investigations may require inter-jurisdictional teamwork to uncover evidence. The Convention promotes mutual legal assistance, information exchange and efficient preservation of electronic data.[148]

---

[144] International Organization on Computer Evidence (IOCE), *Principles and Guidelines for Digital Evidence*.
[145] Casey (n 13) 92.
[146] Convention on Cybercrime (Budapest Convention) 2001.
[147] ibid arts 16–21.
[148] ibid ch III.

Bangladesh is not a signatory to the Budapest Convention, but its principles offer good guidance to the countries that have not ratified it and are developing national policies on the issues of cybercrime investigation and digital evidence management.

8.6 Lessons for Bangladesh

A comparative analysis of the United Kingdom, India and the United States shows that there are several lessons that might enhance the legal dimension associated with digital evidence in Bangladesh.

First, Bangladesh must keep advancing its evidentiary laws to respond to the introduction of new technologies like cloud computing, artificial intelligence, blockchain systems, and encrypted communication. [149] Technology is advancing at a fast pace and the law should keep pace with the new forms of evidence.

Secondly, Judicial training programmers need to be expanded so as to increase awareness of digital evidence and forensic techniques. Experience in other jurisdictions has shown that judges must be competent in order to be able to evaluate complex electronic evidence.[150]

Third, advanced forensic laboratories and technical equipment should be developed in Bangladesh. Forensic skills are required to ensure that electronic records are created and verified, deleted data included and manipulated data detected.[151]

Fourth, standardized processes should be implemented on how to deal with evidence on a national basis. There is a strong focus on documenting the chain of custody, forensic imaging, preservation of metadata and secure storage in international best practices. These would greatly enhance the certainty of electronic evidence before the Bangladeshi courts.[152]

Fifth, Bangladesh should further enhance diplomatic ties on investigations and cross-border access to electronic evidence in the case of cybercrime. Effective criminal investigations have come to require international cooperation due to the global nature of digital communications.[153]

[149] Mason and Seng (n 1) 412.

[150] Paul (n 11) 165.
[151] Casey (n 13) 325.
[152] ACPO (n 4).
[153] Budapest Convention (n 17).

Last but not least, there are legal changes that need to be made, which must be able to strike a balance between effective law enforcement and safeguarding fundamental rights. Any approach to digital evidence should continue to emphasize guarantees of privacy, due process, and fair trial.[154]

Finally, comparative analysis shows that effective regulation of digital evidence needs to be based on a mix of legislation, judicial oversight, technological skills, forensic capacity and international cooperation. Experiences of the United Kingdom, India and the United States offer helpful lessons for Bangladesh as it evolves into a more modern and reliable system for admissibility and reliability of digital evidence in criminal trials.

[154] Constitution of the People's Republic of Bangladesh, arts 31 and 35.

Chapter 9
Major Challenges in the Modern Criminal Procedure System

9.1 Legislative Gaps

The contemporary criminal procedure system in Bangladesh has one of the most problematic issues regarding the lack of laws pertaining to digital evidence. The Evidence (Amendment) Act 2022 added sections 65A and 65B to accommodate electronic records, but the overall procedural framework of the Code of Criminal Procedure 1898 is largely traditional and did not take into account digital realities. [155]

Consequently, there is little clarity as to procedures for the search, seizure, preservation and forensic examination of digital devices. There are no statutes that comprehensively regulate such questions as how mobile phones should be lawfully imaged, how cloud data should be accessed, and how metadata should be preserved. This leads to inconsistencies in the investigative procedure and judicial interpretation.

The lack of a consolidated digital evidence law contributes to the application of legal principles in an inconsistent and confusing manner that can give rise to procedural irregularities and objections to admissibility in criminal trials.[156]

9.2 Lack of Specific Evidentiary Standards

One particular concern is the absence of detailed evidentiary standards that are specifically developed to address digital evidence. Relevance, admissibility, and best evidence remain the basic evidentiary principles, but are sometimes not enough to deal with the technical issues of electronic records.[157]

There are, for instance, no statutory guidelines for the court to follow in regard to metadata, hash values or forensic imaging reports. Likewise, there is no national consensus on what constitutes an acceptable forensic tool and on the minimum technical requirements for digital authentication.

[155] Evidence Act 1872 (Bangladesh), ss 65A–65B; Code of Criminal Procedure 1898 (Bangladesh).
[156] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, IALS 2021) 112.
[157] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 41.

Other jurisdictions, like the United States and the United Kingdom, have created a set of guidelines and forensic best practices. Lack of similar comprehensive rules in Bangladesh raises doubts for judges and practitioners in respect of electronic evidence.[158]

9.3 Privacy and Human Rights Concerns

The gathering and collection of digital evidence is a serious threat to privacy and human rights. Digital devices usually have a great deal of personal information, such as messages, pictures, financial details, and location info. Access to this information may breach constitutional rights to privacy, dignity and fair trial.[159]

The Constitution of the People's Republic of Bangladesh has guaranteed the right to life, liberty and privacy of correspondence/communication under Article 31 and Article 43 of the Constitution. However, in reality, investigative agencies can gain access to digital data in some instances with inadequate judicial oversight, creating concerns about improper use of such data by these agencies.

An effective investigation of crime and the protection of the fundamental rights is a pivotal issue in present criminal procedure systems. International human rights standards state that any interference with privacy be lawful, necessary and proportionate.[160]

9.4 Cybersecurity Risks

Digital evidence is highly vulnerable to cyber risks, which have a profound impact on its reliability and integrity. Law enforcement data and information systems, criminal court systems, and forensic labs can also be hacked, breached or otherwise compromised.

Digital evidence can be changed or corrupted without being known if it's not properly preserved or transmitted. This raises serious doubts as to its authenticity and court admissibility.[161]

Also, cybercriminals are employing more advanced methods like malware, spoofing and anonymization tools to cover their tracks, making investigation and attribution more

[158] Federal Rules of Evidence (US) r 901; ACPO, *Good Practice Guide for Digital Evidence* (2012).
[159] Constitution of the People's Republic of Bangladesh, arts 31 and 43.
[160] Human Rights Committee, *General Comment No 16: Right to Privacy* (1988).
[161] Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (Yale University Press 2017) 89.

challenging. As cyber threats evolve, law enforcement needs to continually upgrade its capabilities.

9.5 Judicial Capacity Constraints

The capacity constraints of judges are also a significant issue in the criminal justice system in Bangladesh. The court will have to consider very technical evidence that includes digital forensics, metadata analysis, encrypted communications, and expert testimony.

But a significant number of Judges have little formal IT or digital forensic training. This knowledge deficit can create challenges regarding the reliability, authenticity and evidentiary value of electronic records.[162]

Without sufficient technical expertise, judges and juries could either rely too heavily on the evidence of the experts, or they may not adequately challenge the evidence. Therefore, it is necessary to enhance judicial training and ongoing education on cyber law and cyber forensic science.

9.6 Digital Forensic Infrastructure Deficiencies

To ensure the effective handling of digital evidence, they need to have advanced forensic infrastructure, including specialized laboratories, software tools, secure storage systems, and trained personnel. In Bangladesh, the infrastructure is still in a state of development, and unevenly distributed.[163]

Criminal investigations can take a long time due to delays in forensic analysis, equipment and limited facilities in the region. Sometimes evidence may be damaged or rendered unusable by improper storage or by being overlooked until too late for examination.

In addition, differences between agencies can lead to different investigations being conducted. Therefore, there is a need to build the capacity of institutions, which can ensure the reliability of digital evidence in criminal procedures.

[162] George L Paul, *Foundations of Digital Evidence* (ABA 2008) 155.
[163] Transparency International Bangladesh, *Cyber Governance Report* (2023).

9.7 Problems of Authenticity and Tampering

One of the most important questions in digital evidence law is whether the evidence is authentic. Electronic records are far more easily manipulated, duplicated, or invented than are physical records, and leave behind less obvious traces. This is a significant concern for tampering and manipulation.[164]

The use of deepfake technology, image manipulation software, and AI-generated content has also made the chances of false evidence being introduced into the courtroom even more likely. Courts are thus required to be vigilant and scrutinize whether the electronic records are, in fact, from the party's presumed source.

Documenting the chain of custody and verifying the authenticity of documents by means of forensic hashing, metadata and expert testimony is vital. But poor enforcement of the protections can compromise the integrity of evidence used in criminal cases.

9.8 Emerging Technologies (AI, Deepfake, Blockchain Evidence)

Both opportunities and challenges exist with the emergence of new technologies in criminal justice. The use of artificial intelligence (AI) in surveillance and predictive policing and data analysis is growing. AI has the potential to enhance the efficiency of investigations, but it also poses challenges for bias, transparency, and accountability.[165]

In the realm of evidence integrity, deepfakes are a serious threat. It can produce a very realistic but fake audio and video recording, making it hard to tell the truth from the fiction in court.[166]

Concurrently, blockchain technology can be used to achieve data integrity. The decentralized and tamper-proof nature of blockchain records can help ensure the authenticity and chain of custody of digital evidence. The acceptance and use of blockchain-based evidence in court proceedings, however, have not been fully covered in the legal landscape in Bangladesh.

The new technologies are developing at a fast pace and there is a need for ongoing legal change and technological adjustments in the criminal justice system.

---

[164] Mason, *Electronic Evidence* (LexisNexis 2017) 201.

[165] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015).

[166] Danielle Citron and Robert Chesney, 'Deep Fakes: A Looming Challenge' (2019) 107 California Law Review 1753.

Chapter 10
Findings, Recommendations, and Conclusion

10.1 Major Findings of the Research

The current study has explored the admissibility and reliability of digital evidence in modern criminal procedure system particularly in the context of Bangladesh in a criminal trial. The study has shown that digital evidence has become essential to the modern criminal justice system, especially in cybercrimes, corruption, terrorism, and/or organized crime. But its potential is still limited by legal, technical and institutional challenges.[167]

This lack of development of the overall machinery of the procedural framework is prominent, particularly with regard to the search, seizure, preservation and forensic processing of electronic data, and is a key finding.[168]

The study also reveals that chain of custody, forensic integrity and authentication procedures play a significant role in the reliability of digital evidence. The loss or destruction of metadata or chain of custody is a major blow to evidentiary value.[169]

In addition, institutional capacity is a significant problem. There is a lack of adequate digital forensic infrastructure and digital forensics experts and also inadequate standard procedure in investigation and prosecution in Bangladesh.[170]

Last, a comparison of the various jurisdictions reveals that others, like the United Kingdom, India, and the United States, have more advanced sets of laws, judicial interpretation, and forensic standards. These systems can be taken as models for reform in Bangladesh.[171]

10.2 Answers to Research Questions

Key research questions from this study were identified. First, on admissibility, the research has established that e-recording are now admissible under Bangladeshi law, if it fulfills the criteria

[167] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011) 23.
[168] Evidence (Amendment) Act 2022 (Bangladesh), ss 65A–65B.
[169] Stephen Mason and Daniel Seng, *Electronic Evidence and Electronic Signatures* (6th edn, IALS 2021) 77.
[170] Transparency International Bangladesh, *Cyber Governance Report* (2023).
[171] *Anvar PV v PK Basheer* (2014) 10 SCC 473 (India).

prescribed in sections 65A and 65B. But courts continue to have difficulties with the implementation of these provisions equally.[172]

Second, as related to reliability, the study confirms that digital evidence is not necessarily reliable and should be authenticated, validated, and placed in a chain of custody. Process integrity is more important for reliability than content is.[173]

Third, as to challenges, the study points to technical hurdles, encryption problems, cross-border data access issues and a lack of knowledge as significant challenges in a criminal trial where there is digital evidence.[174]

Fourth, in the area of judicial practice, courts in Bangladesh have been increasingly accepting electronic evidence, but there is a lack of uniformity in the interpretation and application of the rules of evidence.[175]

10.3 Policy Recommendations

The study suggests a national digital evidence policy in Bangladesh to provide common standards in all investigative and judicial bodies. This policy should include clear guidelines for the collection, preservation and presentation of electronic records.[176]

Moreover, more stringent regulations should be adopted to regulate the accessing of digital data, taking into account the constitutional rights to privacy and protection against unfair trial (Articles 31 and 35 of the Constitution).[177]

In addition, the government should encourage the collaboration of public and private entities with technology companies to enable legal access to the electronic records without compromising compliance with data protection and security guidelines.[178]

[172] Evidence Act 1872 (Bangladesh), ss 65A–65B.
[173] Mason, *Electronic Evidence* (LexisNexis 2017) 201.
[174] Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (Yale University Press 2017) 91.
[175] *Major Md Bazlul Huda v State* 63 DLR (AD) 1.
[176] George L Paul, *Foundations of Digital Evidence* (ABA 2008) 142.
[177] Constitution of the People's Republic of Bangladesh, arts 31, 35.
[178] Council of Europe, *Budapest Convention on Cybercrime* (2001).

10.4 Legal Reform Proposals

The Code of Criminal Procedure 1898 should be amended to include specific procedural guidelines for digital searches, seizures and Computer Forensics Examination of electronic devices. This includes the requirement to have a warrant and standard imaging procedures and the use of clear rules for handling evidence in the cloud.[179]

Furthermore, the provisions of the Evidence Act on electronic records need to be more refined to address questions concerning metadata, blockchain records and evidence created by artificial intelligence. The law should also cover new risks like deep fake evidence and fake media.[180]

It may be argued that a new Digital Evidence Act should be established to bring together all the relevant legislation on electronic evidence in a single, coherent set.

10.5 Capacity Building Measures

The research highlights the critical need for the development of capacity at all points of the CJ system. The basic digital literacy and forensic principles must be taught to investigators, prosecutors and judges to ensure they are able to effectively process electronic evidence.[181]

Specialized training programs should be implemented in judicial academies and law enforcement training institutes, concentrating on investigation of cybercrime, digital forensics and evidentiary evaluation of electronic records.

10.6 Strengthening Digital Forensic Laboratories

There should be a considerable improvement in the digital forensic infrastructure in Bangladesh. This covers the set-up of regional forensic laboratories with state-of-the-art facilities for data recovery, encryption analysis and malware examination.[182]

Standard Operating Procedures (SOPs) must be put in place for a consistent forensic process in all agencies. Forensic laboratories should also be accredited to ensure scientific credibility and reliability of the expert reports.

---

[179] Code of Criminal Procedure 1898 (Bangladesh).
[180] Danielle Citron and Robert Chesney, 'Deep Fakes: A Looming Challenge' (2019) 107 California Law Review 1753.
[181] Paul (n 10) 165.
[182] National Institute of Standards and Technology (NIST), *Guide to Digital Forensics* (SP 800-86).

10.7 Judicial and Prosecutorial Training

Technology changes in evidence law must be continually training judicial officers. Complex technical issues, like metadata analysis, cloud computing and encrypted communications, are becoming a staple of court proceedings.[183]

In the same way, defense attorneys should be educated on how to effectively challenge technical flaws in defense arguments, review expert witnesses, and present digital evidence. Increased legal capacity will enhance the adjudication of digital evidence cases as a whole.

10.8 Future Research Directions

The future implications for the technologies that are on the horizon, like Artificial Intelligence, Blockchain evidence systems, and Quantum encryption should be explored in further studies. The technologies will have a profound impact on evidentiary rules and new rules will need to be enacted.[184]

Empirical studies also require further investigation to understand the specific ways in which courts in Bangladesh are currently applying digital evidence in practice, such as how they behave in court, how they think about the evidence, and how they treat digital evidence being presented as a record.

10.9 Conclusion

Digital evidence has become the backbone of investigation and prosecution of crimes and is now an integral part of the modern criminal justice system. The legislative reform, especially the introduction of sections 65A and 65B of Evidence Act, 1872, has been the highlight of progress in Bangladesh. But merely granting legal recognition to digital evidence is not enough for its use to be effective in criminal cases.

The study identifies that digital evidence is of great value, but must be subject to procedure, supportive of a strong forensic system and be handled by competent judges if it is going to be admissible and reliable. If electronic records are not authenticated, preserved and maintained

[183] Mason and Seng (n 3) 118.
[184] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015).

in a proper chain of custody, they can be susceptible to manipulation and may be of little evidentiary value.

For the successful administration of criminal justice, Bangladesh needs to implement a comprehensive criminal justice reform program consisting of legislative modernization, institutional strengthening, judicial capacity building and technology investment. The existence of digital evidence is just one of the tools that can help to realize the goal of digital evidence in modern criminal procedure system, which is to ensure justice, fairness, and the rule of the law.[185]

[185] Ian Dennis, *The Law of Evidence* (7th edn, Sweet & Maxwell 2020) 52.

Bibliography

Legislation

- Evidence Act 1872 (Bangladesh).
- Evidence (Amendment) Act 2022 (Bangladesh).
- Code of Criminal Procedure 1898 (Bangladesh).
- Cyber Security Act 2023 (Bangladesh).
- Digital Security Act 2018 (Bangladesh).
- Information and Communication Technology Act 2006 (Bangladesh).
- Penal Code 1860 (Bangladesh).
- Information Technology (Certification Authority) Rules 2010 (Bangladesh).
- Criminal Justice Act 2003 (UK).
- Federal Rules of Evidence (United States).
- Information Technology Act 2000 (India).
- Police and Criminal Evidence Act 1984 (UK).
- Constitution of the People's Republic of Bangladesh

Cases

- *Anvar PV v PK Basheer* (2014) 10 SCC 473 (India).
- *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1 (India).
- *Mrs Khaleda Akter v State* 37 DLR (AD) 275 (1985).
- *Major Md Bazlul Huda v State* 63 DLR (AD) 1.
- *Lorraine v Markel American Insurance Co* 241 FRD 534 (D Md 2007) (United States).

International Instrument

- Convention on Cybercrime.

Books

- Casey E, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011).
- Mason S and Seng D, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021).
- Paul GL, *Foundations of Digital Evidence* (American Bar Association 2008).
- Islam M, *Constitutional Law of Bangladesh* (3rd edn, Mullick Brothers 2012).
- Dennis I, *The Law of Evidence* (7th edn, Sweet & Maxwell 2020).
- Keane A and McKeown P, *The Modern Law of Evidence* (14th edn, Oxford University Press 2023).
- Mason S, *Electronic Evidence* (5th edn, LexisNexis 2017).
- Mason S and Seng D, *Electronic Evidence and Electronic Signatures* (6th edn, Institute of Advanced Legal Studies 2021).
- Landau S, *Listening In: Cybersecurity in an Insecure Age* (Yale University Press 2017).
- Hildebrandt M, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015)
- Landau S, *Listening In: Cybersecurity in an Insecure Age* (Yale University Press 2017)

Journal Articles and Online Sources

- Tanbir K, 'Admissibility of Digital Evidence in Bangladesh' (SSRN 2022).
- 'Evidence (Amendment) Act 2022: An Expert's View' (Dhaka Law Review, 2022).
- 'Changes Brought to Law of Evidence in Bangladesh by the Evidence (Amendment) Act 2022' (BD Law Post, 2022).
- Damaška M, *Evidence Law Adrift* (Yale University Press 1997).
- Keane A and McKeown P, *The Modern Law of Evidence* (14th edn, Oxford University Press 2023).
- Langbein JH, *The Origins of Adversary Criminal Trial* (Oxford University Press 2003).
- Paul GL, *Foundations of Digital Evidence* (American Bar Association 2008).
- Paul GL and Baron JR, 'Information Inflation: Can the Legal System Adapt?' (2007) 13 Richmond Journal of Law and Technology.
- Rahman M, 'Digital Evidence and Criminal Justice Reform in Bangladesh' (2023) 34 Bangladesh Journal of Law 115.
- Chesney R and Citron D, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753.
- Kerr OS and Schneier B, 'Encryption Workarounds' (2018) 106 Georgetown Law Journal 989.
- Citron D and Chesney R, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753

Reports

- Amnesty International, *Muzzling Dissent Online: Digital Security Act in Bangladesh* (2021).
- Transparency International Bangladesh, *Review of the Cyber Security Act 2023* (2023).
- International Organization on Computer Evidence (IOCE), *Principles and Guidelines for Digital Evidence*.
- National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response* (SP 800-86).
- Transparency International Bangladesh, *Cyber Governance and Digital Investigation Challenges in Bangladesh* (2023).
- Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence* (5th edn, 2012).
- National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response* (SP 800-86).