RPSU RESEARCH JOURNAL

ISSUE - I

ISSN (Print) : 2790-4903 ISSN (Online) : 2959-2305

DECEMBER - 2023

Challenges of the Digital Evidence in Bangladesh: The Evidence (Amendment) Act-2022

Kazi Latifur Reza¹, Niladry Paik², Mitali Rani Das²

¹Associate Professor, Department of Law and Human Rights, RPSU, Bangladesh ²Lecturer, Department of Law and Human Rights, RPSU, Bangladesh **Corresponding Author:** Kazi Latifur Reza, kazilatifur@rpsu.edu.bd

Abstract

This study scrutinizes the challenges posed by digital evidence in the context of Bangladesh, with a specific focus on the recent legislative changes introduced through the Evidence (Amendment) Act-2022. Investigating the Act's responsiveness to the intricacies of digital evidence, the analysis delves into the implications of key amendments, notably the recognition of "digital records." Despite progressive strides, the study unveils certain ambiguities and concerns within the legislation, necessitating a nuanced approach. Recommendations for refinement and proactive strategies are proposed to address these challenges and ensure the seamless integration of digital evidence into the legal framework. The study underscores the critical balance required between legal principles and technological advancements in adapting to the digital landscape.

Keywords: Digital Evidence, Electronic Records, Cyber Forensic, Relevancy, Admissibility.

1. Introduction

The advent of the digital era has brought forth unprecedented challenges and opportunities for legal systems worldwide, and Bangladesh is no exception. In this context, the study meticulously examines the intricacies surrounding digital evidence within the jurisdiction of Bangladesh and India, focusing specifically on the legislative amendments introduced through the Evidence (Amendment) Act-2022. As our reliance on digital information intensifies, the legal framework must adapt to ensure the seamless integration and effective adjudication of cases involving digital evidence. This introduction sets the stage for a comprehensive exploration of the challenges posed by the evolving landscape of digital evidence within the framework of Bangladesh's legal system, aiming to provide insights, recommendations, and a nuanced understanding of the complex interplay between technology and the law. Moreover, drawing insights from the Indian experience becomes particularly relevant, given the similarities in our legal systems. By understanding the challenges and successes encountered by India, the study aims to enhance the ability to effectively navigate the evolving terrain of digital evidence within the context of Bangladesh's legal system.

In Bangladesh, determining the admissibility of digital evidences in legal proceedings is a critical aspect. However, given its inception long before the widespread integration of digital technology, the Act's provisions may fall short in adequately addressing the nuances and challenges posed by digital evidence. This study aims to achieve several specific objectives: first, to scrutinize the provisions pertaining to digital evidence in the Evidence Act of 1872 and other relevant laws, cases laws assessing their effectiveness in confronting the challenges associated with digital evidence and secondly, to elucidate the specific challenges inherent in handling digital evidence in Bangladesh, encompassing issues. Lastly, the review aims to pinpoint the opportunities presented by digital evidence, recognizing its potential to augment the efficiency and precision of investigations and court proceedings. Through a comprehensive analysis, this literature review endeavors to offer an up-to-date understanding of the current landscape of digital evidence in Bangladesh, with a focus on identifying avenues for improvement and providing actionable recommendations.

2. Objective of the Study

To comprehensively understand the modifications introduced by the Evidence (Amendment) Act-2022 to handle Challenges of the Digital Evidence in Bangladesh

3. Research Methodology

The research methodology employed in this article encompasses a comprehensive utilization of secondary sources to scrutinize the challenges associated with collecting, preserving, and presenting digital evidence in the context of Bangladesh. Central to this methodology is an evaluation of the efficacy of the Evidence (Amendment) Act-2022 in addressing these challenges. The approach involves an extensive literature review, wherein existing scholarly works on the subject are examined. Data collection is conducted through the analysis of academic articles, government reports, and policy documents, providing a diverse and multifaceted perspective. Qualitative data analysis techniques are employed to derive meaningful insights from the collected data, facilitating a nuanced understanding of the complexities surrounding digital evidence in Bangladesh. The research methodology emphasizes proper citation and referencing to uphold the accuracy and appropriateness of the sourced information. Through this methodological framework, the research aims to offer valuable insights into the current landscape of digital evidence in Bangladesh and India. The findings and recommendations derived from this study are intended to serve as a beneficial resource for legal practitioners, law enforcement agencies, and policymakers, aiding them in navigating and enhancing the utilization of digital evidence within the country's legal framework

4. Literature Review

Digital evidence has become increasingly important in the legal system of Bangladesh as more crimes are committed using technology. However, several challenges hinder the effective use of digital evidence in the country. This literature review aims to examine the current state of digital evidence in Bangladesh and the challenges that arise in its use in the justice system. A study by the Bangladesh Institute of Law and International Affairs (BILIA) (Ferdaus, 2022) found that a lack of technical expertise is one of the biggest challenges in using digital evidence in the legal system of Bangladesh. Law enforcement agencies, investigators, and judges often do not have the necessary technical knowledge to collect, analyze, and interpret digital evidence effectively. This results in weak cases and poor outcomes in court.

While the Bangladesh Cyber Crime Tribunal has been established to deal with cybercrime, there is a lack of clear and comprehensive legislation regulating the collection, preservation, and admissibility of digital evidence. This makes it difficult for law enforcement agencies to effectively deal with cybercrime and to use digital evidence in court proceedings. Although, the use of digital evidence often requires the cooperation of multiple agencies, such as law enforcement, the judiciary, and technical experts. However, there is a lack of coordination and cooperation between these agencies in Bangladesh, which makes it difficult to use digital evidence effectively. A report by the Bangladesh E-Governance Agency (BEA, 2019) highlights the need for inter-agency cooperation to address this challenge. Digital evidence plays a crucial role in criminal investigations and court proceedings, but its reliability and admissibility in the legal system remain a challenge in many countries, including Bangladesh.

In addition, the quality and integrity of digital evidence can easily be compromised if not preserved properly. A study by the Bangladesh Computer Council (BBC, 2020) found that there is a lack of standard operating procedures for the collection, preservation, and analysis of digital evidence in Bangladesh. This makes it difficult for investigators to use the evidence in court and results in the exclusion of crucial evidence.

Moreover, there is currently a lack of a comprehensive legal framework for the use of digital evidence in Bangladesh. This makes it difficult for the authorities to deal with the challenges posed by digital evidence, including issues such as authenticity, reliability, and admissibility. A report by the United Nations Office on Drugs and Crime (UNODC) (2021) notes that this situation needs to be addressed if digital evidence is to be used effectively in the court of Bangladesh.

Another challenge is the lack of technical expertise among law enforcement agencies. Many officers are not trained in the proper handling and analysis of digital evidence, leading to contamination or loss of evidence and difficulty in presenting it in court. Furthermore, the use of digital forensics tools is limited in Bangladesh, and the infrastructure to support digital forensics is still lacking (Haque, 2015).

Additionally, the issue of data privacy and protection remains a challenge in the collection and use of digital evidence in Bangladesh. The lack of clear and comprehensive privacy laws and the absence of a data protection authority make it difficult to balance the need for evidence with the protection of personal privacy (Khatun, 2015). In this context, our scrutiny extends to the Evidence Act-1872, examining it in conjunction with other

laws and case precedents relevant to digital evidence. Our study is designed for a comprehensive exploration of the Evidence (Amendment) Act 2022, comparing it with its predecessors to gauge its responsiveness to the demands of the contemporary world. Our objective is to meticulously identify any gaps in the new amendment and assess its adequacy in addressing the challenges posed by the evolving legal landscape.

5. Exploring the emulation of digital evidence in other laws in Bangladesh.

Before the Evidence (Amendment) Act 2022, the legal landscape in Bangladesh lacked explicit provisions for digital evidence. The Evidence Act (1872) and Penal Code (1860) provided scope for judicial interpretation, acknowledging the admissibility of digital evidence based on terms like 'substance' and 'matter expressed or described.' The introduction of digital evidence in special laws like the Speedy Trial Tribunal Act 2002 marked the initial steps in recognizing electronic forms of evidence, albeit limited to pictures, movies, and recordings. The ICT Act (2006) and Digital Security Act (2018) addressed some aspects but didn't comprehensively cover the acceptance of digital evidence.

Various legislation, including the Pornography Control Act 2012, dealt with admissibility and punishment related to digital evidence. The legislative landscape displayed a mix of mandatory and discretionary admissibility, with some laws requiring specific conditions such as attestation and certification of digital records.

The repeal of the Bankers' Books Evidence Act 1891 and the introduction of the Bankers' Books Evidence Act 2021, resembling Section 65B of the amended Evidence Act, demonstrated an effort to adapt to the digital era. The new Act outlined conditions for attestation and certification of digital records, emphasizing accuracy and security measures.

Overall, the legal system in Bangladesh experienced a shift towards acknowledging digital evidence, necessitating the subsequent amendments like the Evidence (Amendment) Act 2022. The new amendment attempts to streamline the acceptance of digital evidence by providing explicit definitions and conditions, although concerns persist regarding clarity and potential loopholes.

6. Reviewing the case laws related to digital evidence in Bangladesh

In several case laws, digital evidence was accepted as valid. One such case is *Mrs. Khaleda Akter vs. State*, (37 DLR,1985,275), where the court determined that a video cassette made using technology for the purpose of recording and displaying on television falls under the definition of a document. The court held that audio and video cassettes are admissible as evidence.

In the *Biswajit murder case* (70 DLR (2018) HCD 26), documented in the court held the opinion that video footage, photographs, and paper clippings can be accepted as evidence without the need for support from the creators.

In the *Major Bazlul Huda & Others Vs. The State* (18 BLT (AD) (2010) 7) case, the ruling stated that when attempting to admit digital or electronic evidence, such as statements or admissions recorded on compact disk or video cassette or any interviews conducted by a television channel regarding relevant facts in a case, the party must present the original disk or cassette, along with a certificate from the producer of the program, verifying the date and location of the recording, and the producer's signature must also be proven. However, if the defendant denies the statement or admission, its admissibility will be determined based on the current laws of evidence.

However, In *The State Vs. Yeasin Khan Palash* (29 BLD (HCD) (2007) 469), case, the issue of the admissibility of digital or electronic evidence arose. The court ruled that according to Section 16 of the Druto Bichar Tribunal Ain, 2002, video cassettes, audio cassettes, and still pictures relating to an occurrence are admissible as evidence. Therefore, the judge of the Druto Bichar Tribunal No.1, Dhaka was correct in admitting the tape-recorded conversation in an audio cassette as evidence, given the evidentiary value of audio cassettes specified in Section 16. The court emphasized the need to understand the matter correctly in light of the above section.

In *The State Vs. Qamrul Islam & Others-2017* ((2) LNJ (HCD) (2017)303) case, the defense attorneys argued against the admission of video recording as evidence on the basis that there is no law recognizing video footage

as admissible evidence in the country. The court referred to the case of *Mrs. Khaleda Akhtar Vs. The State* (37 DLR (1985) 275), and ruled that there is no logic to the argument made by the defense counsels for the accused. The court held that a video footage can be considered a document under the Evidence Act and is admissible as evidence in a trial if it is relevant.

7. Analysis of the Evidence (Amendment) Act 2022

The Evidence (Amendment) Act 2022 was enacted to modernize the laws of evidence in legal proceedings and to keep pace with technological advancements. We rely heavily on digital devices and as a result, many, if not all, forms of evidence have become digital or electronic. For instance, video recordings or CCTV footage can play a critical role in criminal cases. Therefore, it is imperative to allow digital records to be accepted as evidence. The concept of "digital records" has been added to sections 17, 34, 35, 36, and 39 of the Act. Additionally, section 22A states that unless the authenticity of the digital record is in question, oral evidence of digital evidence will not be acceptable in court. For example, if the opposing party raises any concerns about the validity of the video footage, only then can the oral testimony of a witness regarding the video be admissible in court. The anomaly is severe as not every digital evidence is a "record". The same anomaly is visible in our Evidence (Amendment) Act, 2022. Digital record and electronic record as well as examples of types of evidence mentioned in the Act create confusion. The Act also includes the term "digital signature." According to Section 3, the definition of digital signature outlined in the Information and Communication Technology Act 2006 will apply. The Act of 2006 defines digital signature as data in electronic form that satisfies the requirement of being uniquely affixed by the signatory, capable of identifying the signatory, and created under the signatory's sole control. The Act includes provisions in sections 67A and 47A to prevent fraud in court through the use of digital signatures. These sections require the subscriber's digital signature to be proven in court. Additionally, if the court has any doubts, it may seek the opinion of the certifying authority that authorized the signature., however, there is no clear explanation of the term "Authority" in the act.

The Act introduced provisions for electronic evidence increased the admissibility of hearsay evidence and expanded the scope of privileged communications. It aims to simplify the rules of evidence and promote the use of technology in the legal system, while still ensuring the protection of individual rights and the reliability of evidence presented in court. The amendment is seen as a positive step towards making the legal system more efficient and responsive to the changing times. However, the act has been criticized for its vague definitions and lack of clarity on the weight to be given to electronic evidence, leading to potential loopholes in the legal system. Additionally, the broadening of the scope of privileged communications has raised concerns over the balance between the right to confidentiality and the need for evidence in criminal proceedings.

In the Amendment Act 2022 the following words have been added to the definition of 'Document' - 'and includes any digital record' According to the previous definition, digital content could not be regarded as documentary evidence let alone oral evidence. As per the newly added definition clearly authorized the inclusion of digital record, the court will be, from now on, exempted from making any further interpretation to make a digital evidence admissible.

The definition of the word 'evidence' is derived from the Latin word 'evidere' which implies "to show clearly; to make plain, certain or to prove" (Gupta, 2005). However, the previous definition of 'evidence' under s3 of the Evidence Act 1872 was not exhaustive. Although, amended definition has included biological components but ignored the digital or electronic matters as they were incorporated in the definition of 'Document' already. The Evidence Act required a broader, inclusive definition, a gap unaddressed by this amendment.

8. Examining the Indian experience within the context of digital evidence

The recently enacted amendment bears significant resemblance to the Indian Evidence Act. The challenges arising from the adoption of digital evidence in India led to recommendations for amendments at the state level. This resulted in confusion concerning electronic records and digital evidence within the Act.

In 2000, the Indian government incorporated a similar provision regarding certification under s65B of the Indian Evidence Act 1872. *The Shafhi Mohammad* (Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801.) and *Anvar P.V.* case (Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.) puzzled the Court of laws regarding the interpretation of the section. Addressing the question regarding the admissibility of video records the Supreme Court of India relied on the *R. v Maqsud Ali* ([1966] 1 QB 688, [1965] 2 All ER 464) and *Ram Singh and Ors. vs Col. Ram Singh* (1986 AIR, 3 1985 SCR Supl. (2) 399) case. Both the cases admired the modern ways of collecting evidence. Complete exclusion of digital records merely because of its technicality has been criticized in the aforementioned cases. However, it is also observed by the Indian courts that digital contents are no ordinary evidence. Such evidences are more prone to be tempered, therefore require stringent standard of proof (Tukaram S. Dighole v. Manikrao Shivaji Kokate).

In the Navjot Sandhu case, the issue was about the admissibility of mobile phone records. The court held that adducing secondary evidence of digital content can be an alternative to the certificate under s63B. However, the observation was discarded in the Anvar P. V. vs P. K. Basheer case. In that case, the Supreme Court of India held that following the procedure under s65B is mandatory as digital records are susceptible. However, the court also watered down the provision in the case of primary evidence. In cases, where a party possess a piece of authentic digital evidence but is barred to admit it only because of the lack of a certificate, the court can let that evidence be submitted. Moreover, the Supreme Court emphasized ensuring the source and authenticity of the digital record. The observation in the Anvar P. V. case has been followed and elaborately debunked. The Supreme Court held that certificate under the s65B is not mandatory in the following two cases: firstly, the device is not in the possession of the person who is willing to submit the document (The court also added that in such cases, the certificate can be added in the later stages of the proceeding) and secondly, the contents of the digital evidence match the testimony of the person against whom it is submitted. The court mainly relied on two Latin maxims- Lex non cogitad impossibilia, meaning- Law does not demand the impossible and Impotentia excusat legem, meaning- disobedience is excused when it is impossible to follow the law. However, the court also observed that when the evidence is related to a computer network impossible to bring into the court, s65B must be followed.

Comparatively, India's legal system underwent a similar shift with the introduction of Section 65B in the Evidence Act 1872. The *Shafhi Mohammad* and *Anvar P.V.* cases posed challenges in interpreting the section. Courts embraced modern evidence collection methods, recognizing digital evidence's significance. However, concerns over tampering led to stringent standards of proof. The Navjot Sandhu case explored the admissibility of mobile phone records, while *Anvar P.V.* emphasized mandatory compliance with Section 65B. The Indian courts acknowledged the susceptibility of digital records, yet allowed for flexibility in certain situations, highlighting the importance of ensuring source and authenticity. Lessons from the Indian experience suggest that while adhering to strict procedures for digital evidence is crucial, the courts also need to balance legal standards with practical considerations. Understanding these nuances becomes imperative for Bangladesh to shape an effective legal framework for digital evidence, learning from India's successes and challenges

9. A Comparative Exploration of Digital Evidence Management in Western Legal Systems

European Union:

Within the European Union (EU), the General Data Protection Regulation (GDPR) imposes strict regulations on personal data, impacting the exchange and admissibility of digital evidence. EU member states, influenced by GDPR principles, have diverse legal frameworks for handling digital evidence. Notably, Germany has stringent laws in this regard. (EU, 2023)

UK:

The United Kingdom governs the use of digital evidence in legal proceedings through detailed rules in the Civil Procedure Rules (CPR) for civil cases and the Criminal Procedure Rules (CrimPR) for criminal cases. The

Crown Prosecution Service (CPS) regulates the use of digital evidence in criminal proceedings, ensuring competence in handling by accrediting digital forensics experts (KOH, 2021).

USA:

In the United States, the Federal Rules of Evidence and Criminal Procedure guide the handling of digital evidence, making electronic records more likely to be admissible and easily authenticated. The U.S. emphasizes rigorous standards for preserving and maintaining the chain of custody for digital evidence. Electronic discovery (e-discovery) procedures contribute to efficient identification and production of relevant digital evidence, particularly in civil litigation (Novak, 2018). The legal system of Bangladesh handling of digital evidence has opportunity to update learning experience from western legal system

10. Findings and Recommendations

The legal landscape in Bangladesh, prior to the Evidence (Amendment) Act 2022, lacked explicit provisions for digital evidence. The existing laws, including the Evidence Act (1872) and Penal Code (1860), relied on judicial interpretation to acknowledge the admissibility of digital evidence based on terms like 'substance' and 'matter expressed or described.' Special laws such as the Speedy Trial Tribunal Act 2002 recognized limited forms of electronic evidence.

Various legislation, including the Pornography Control Act 2012, displayed a mix of mandatory and discretionary admissibility for digital evidence, with some laws outlining specific conditions for attestation and certification of digital records. The repeal of the Bankers' Books Evidence Act 1891 and the introduction of the Bankers' Books Evidence Act 2021 demonstrated efforts to adapt to the digital era by outlining conditions for attestation and certification of digital records, aligning with Section 65B of the amended Evidence Act.

The case laws in Bangladesh showcase a growing acceptance of digital evidence. Precedents such as *Mrs. Khaleda Akter vs. State* and the Biswajit murder case acknowledge the admissibility of video and audio cassettes, video footage, photographs, and paper clippings. *The Major Bazlul Huda & Others Vs. The State* case outlined specific conditions for admitting digital or electronic evidence, emphasizing the need for original disks or cassettes, certificates from producers, and verification of date and location. However, concerns over the admissibility of digital evidence arose in cases like *The State Vs. Yeasin Khan Palash*, where the court ruled based on Section 16 of the Druto Bichar Tribunal Ain, emphasizing the correct understanding of relevant sections.

Subsequent Evidence (Amendment) Act 2022 aimed to modernize the existing evidence laws, acknowledging the increasing reliance on digital devices. While the amendment introduces the concept of "digital records" and addresses issues like digital signatures, hearsay evidence, and privileged communications, criticism has been raised for vague definitions and lack of clarity on the weight given to electronic evidence. The amendment, by adding "any digital record" to the definition of 'Document,' seeks to simplify the admissibility of digital evidence, exempting the court from further interpretation. However, the definition of 'evidence' remains somewhat limited in addressing digital or electronic matters.

Last of all, the legal system in Bangladesh has undergone significant changes, recognizing and adapting to the importance of digital evidence, with the Evidence (Amendment) Act 2022 marking a positive step forward.

Based on the analysis of the legal landscape and recent amendments in Bangladesh's evidence laws, it is recommended that further steps be taken to enhance the clarity and effectiveness of regulations surrounding digital evidence.

1) Clarification of Definitions:

Consider revisiting and refining the definitions related to digital evidence, especially those pertaining to "digital records," "digital signatures," and "Authority". Providing clear explanations and eliminating potential ambiguities will contribute to a more robust legal framework.

2) Awareness and Training:

Implement training programs for legal professionals, judges, and law enforcement personnel to enhance their understanding of digital evidence, its admissibility, and the specific requirements outlined in the amended laws. This will ensure consistent and informed decision-making in legal proceedings.

3) Continuous Legal Education:

Establish a mechanism for continuous legal education on evolving technologies and their implications on evidence. This will help legal practitioners stay abreast of technological advancements and effectively apply updated laws in their practice.

4) Technology Integration:

Explore opportunities to integrate technology within the legal system to streamline the submission, verification, and presentation of digital evidence. This may include the development of secure platforms for the submission of digital records and the verification of digital signatures.

5) Review of Criticisms:

Address the criticisms surrounding vague definitions and lack of clarity on the weight given to electronic evidence. Establish a review process to address these concerns and consider amendments to ensure a more comprehensive and unambiguous legal framework.

6) International Best Practices:

Study international best practices related to the acceptance of digital evidence in legal systems. Drawing insights from successful models can provide valuable guidance on refining existing laws and procedures.

7) Public Awareness Campaigns:

Launch public awareness campaigns to inform citizens about the evolving nature of evidence laws, especially in the digital context. This will foster a better understanding of their rights and responsibilities in the digital age.

8) Collaboration with Technology Experts:

Foster collaboration between legal professionals and technology experts to bridge the gap between legal requirements and technological capabilities. This collaboration can help in creating practical and effective solutions for handling digital evidence.

By incorporating these recommendations, Bangladesh has the opportunity to fortify its legal framework, fostering a seamless integration of digital evidence. This approach ensures the adherence to principles of justice, fairness, and transparency in legal proceedings, thereby meeting the criteria essential for effectively addressing the challenges associated with digital evidence in Bangladesh.

11. Conclusion

In conclusion, the study on the "Challenges of Digital Evidence in Bangladesh: The Evidence (Amendment) Act-2022" sheds light on the transformative landscape of legal proceedings in the digital era. The amendments introduced by the Evidence Act of 2022 signify a positive stride toward modernizing the legal framework to accommodate the nuances of digital evidence. However, the analysis highlights potential areas of concern, such as the need for precise definitions and safeguards to ensure the seamless integration of digital records. Drawing insights from case laws and legislative developments, the study emphasizes the importance of a well-defined legal infrastructure to effectively handle challenges associated with digital evidence. The experience of India in this realm provides valuable lessons, suggesting a nuanced approach to balance the integration of technology while upholding the integrity of legal proceedings. Comprehensively, the study prompts a thoughtful consideration of the dynamic interplay between the law and evolving technologies, urging continuous refinements to meet the demands of the digital age in the context of Bangladesh's legal landscape.

References

- Bangladesh Computer Council (BCC). (2020). The preservation of digital evidence in Bangladesh. Dhaka: BCC.
- Bangladesh E-Governance Agency (BEA). (2019). Inter-agency cooperation in the use of digital evidence in Bangladesh. Dhaka: BEA.
- Barua, A., & Islam, M. R. (2017). Cybercrime in Bangladesh: current scenario and way forward. Asian Journal of Criminology, 12(3), 243-255.
- Haque, M. E., & Banik, S. (2015). Cybercrime and legal framework in Bangladesh. International Journal of Humanities and Social Science Research, 5(2), 102-109.
- Jannatula ferdaus (2022), Emergence of Digital Evidence In Bangladeshi Courts From The Us Based Digital Platforms: Prospects And Challenges, Bangladesh Institute of Law and International Affairs (BILIA), 2(2) Dhaka: BILIA. DOI: https://doi.org/10.58710/bjlv20n2y2022a06
- Khatun, F., & Islam, M. S. (2015). The digital forensics investigation process in Bangladesh. Journal of Digital Forensics, Security and Law, 10(3), 33-47.

KK Shing & H P Gupta, The Evidence Act 1872(Universal Law Publishers, 2011)

United Nations Office on Drugs and Crime (UNODC). (2021). The use of digital evidence in Bangladesh: Issues and challenges. Vienna: UNODC.

Statutes:

- The Bankers Books Evidence Act 2021;
- ICT Act 2006
- Law and Order Deterrent Offence (Speedy Trial) Act 2002;
- Speedy Trial Tribunal Act 2002
- The Digital Securities Act- 2018
- The Evidence Act 1872
- The Narcotics Control Act 2018;
- The Penal Code-1860
- The Pornography Control Act 2012;
- The Prevention and Suppression of Human Trafficking Act 2012;
- The Indian Evidence Act-1872

Case Laws:

- (2) LNJ (HCD) (2017)303
- 1 QB (1966) 688,
- 18 BLT (AD) (2010) 7
- 2 All ER (1965) 464
- 29 BLD (HCD) (2007) 469
- 37 DLR (1985) 275
- 37 DLR (1985) 275
- 70 DLR (2018) HCD 26
- AIR, (1986) 3
- Anvar P.V. v. P.K. Basheer 10 SCC (2014) 473.
- SCR Supl. (2), 1985, 399
- Shafhi Mohammad v. State of Himachal Pradesh 2 SCC (2018) 801.
- Tukaram S. Dighole v. Manikrao Shivaji Kokate