NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

VIRTUAL HEARINGS AND DIGITAL EVIDENCE: CHALLENGES IN ENSURING FAIR TRIAL

Ms. Vaani. P[1] and Mr. Swaminathan P.S.[2]

Abstract: *In the era of advancement of science and technology, the innovation of Artificial Intelligence (AI), an intersection between law and technology, generates not only opportunities but also presents significant challenges for investigation agencies and legal practitioner both internationally and domestically. The digital evidence and virtual hearing had a great impact on the legal proceedings. While exploring the term digital evidence and virtual hearing compared to traditional methods of court room practice, a question arises whether the admissibility of digital evidence will render justice and ensure fair trial to the parties. So in order to ensure fair trial, the court has to admit the digital evidence and conduct the court proceedings. But in reality, the lacuna between law and technology makes the fair trial as complex one. In this article the author has explored right of fair trial in constitution of India, and complexity involved in the digital evidence before the court of law. The main theme includes admissibility of digital evidence in legal proceedings and challenges in ensuring fair trial.*

This research aims to discuss the challenges in admissibility of digital evidence in the virtual hearing and ensure fair trial in proceedings. And also provides insights that can guide policy makers and legal professionals to evolve both sides of the coin as law and technology aspects.

Keywords: *Fair trial, Virtual Hearing, Digital Evidence, Legal Frame Work, Admissibility of Digital Evidence, Challenges in admissibility of digital evidence.*

I. INTRODUCTION

"Justice Delayed is Justice Denied"- William Ewart Gladstone

The outbreak of Covid-19 and advancement of technology lead to virtual hearing of cases (i.e.) e-filing of necessary documents, video conferencing, witnessing the parties and thus the justice was rendered. The introduction of e-courts brings a revolutionary change in the system of filing of cases, allotment of cases in every stage has brought the ease of business, especially in the criminal proceedings. In every proceeding evidence plays an important role to render justice and safeguard the rights of victim. The submission of evidence plays a pivotal role to render justice and safeguard fundamental rights of the victim. The evidence is further classified into traditional mode of evidence and digital mode of evidence. To render justice without any bias, evidence must be admissible by the court of law and thus it ensures a fair trial, if not then it will be denial of justice which will affect the fundamental rights of the citizen.

"According to the report provided by National Judicial Data Grid (NJDG), nearly 82 thousand cases are pending in Supreme court , about 10 lakh cases are pending in Allahabad High court, nearly 7 lakh cases are pending in Bombay High court and nearly 1 lakh cases are pending in Calcutta High court mentioned as 'Pendency of cases' (Drishti Judiciary, 30 May 2024)"[1] which shows that there are huge number of pending cases from years which will affect rendering of speedy justice.

To resolve huge pending of cases, the technological advancement, introduction of e-court system, virtual hearing of cases and admissible of digital evidence will aid as an anchor to the Indian judicial system. The virtual hearing of cases has become an effective mean to conduct court proceeding with debarring territorial jurisdictions and geographical barriers and uplift the court room proceedings. The admissibility of evidence plays an important role in virtual hearing but faces a lot of challenges in proceedings before the Court.

[1] The author is a Post graduate student, pursuing LL.M. Taxation law at Government Law College, Coimbatore. She may be reached at vaani.aries@gmail.com.

[2] The author is as Post graduate student, pursuing LL.M. Taxation law at Government Law College, Coimbatore. He may be reached at swaminathanupscmail@gmail.com.

[1] 'Pendency of cases' (Drishti judiciary,30 May 2024), <https://www.drishtijudiciary.com/editorial/pendency-of-cases>, accessed 28 February 2025

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

The author of this article aims to discuss the challenges in admissibility of digital evidence in the virtual hearing and ensuring fair trial in legal proceedings.

II. RESEARCH METHODOLOGY

The author of the research article has employed doctrinal research. The author has analyzed various research papers (i.e.) dissertation, law journals, legal articles, legal columns and various landmark judgments of High Court and Supreme Court. The relevancy and creditability of various secondary sources were taken into account.

III. REVIEW OF LITERATURE

There are many studies about the digital evidence and virtual hearing and most of reviews are related to challenges faced by the virtual hearing. In this section the author of this research article allows the paper findings and the previous literature to conclude it. The important literature related to virtual hearing and fair trial procedure is reviewed.

Mr. Dhannjay Singh Pundir, Vratika Singh, Anuvrat Singh (2021)[2], this paper "Examined and assessed the legitimacy of digital evidence within a judicial context, considering the implications of judicial rulings and the objectives of legal proceedings". The paper found though there were amendments in the information technology act and evidence act regarding the usage of digital evidence, various judicial decisions highlighted the importance of certification and concluded that besides the change in pace over the technology, the court had also kept the pavement along with cyber space and promoted the usage of electronic records.

Shubham Singh Bagla, (2021)[3], the study "Examined the complexities inherent within the system and identified the possible remedies for these obstacles in order to facilitate expeditious justice". The paper found that cyber forensics was in nascent stage and supreme court interpreted the existing law on the electronic evidence in the most and best possible ways and found that still there was an need of reform in the existing laws and technology.

Vanshika Shukla, (2023)[4], This paper deals about the "Essentiality for legal practitioners to engage in a collaborative partnership with technological specialists, in addition to revising existing rules and regulations and instituting a comprehensive legal framework that upholds the integrity of the judicial system". This paper concludes the importance of digital evidence and its role in the judiciary to ensure the fair trial process and also found that if the challenges are not addressed it will eventually lead to failure and undermine the credibility of the legal system and erode trust among the public regarding the trial process.

Pooja Gaur, (2024)[5], analyzed the "Importance of forensic evidence, If the forensic evidence is provided in the court, there is a high probability that the judgement will not be in defendants side as scientific evidence is un destroyable and unalterable. Regarding the scientific evidence, the expert serves as consultants and also plays a crucial role. On the basis of decision by the court and also based on court conclusion which it is supported by the legal practitioners are depended on the opinion of the experts". This paper finds that integration of forensic science into criminal prosecution made a great progress and also found that forensic technologies have evolved to a greater extent and there are some challenges which still have to addressed.

Ganguli, Prithwish, (2024)[6], in this paper it discussed on "Digital governance, cyber

[2] Mr. Dhannjay Singh Pundir, Vratika Singh, Anuvrat Singh, 'Critical Analysis of Admissibility of Digital evidence' (December, 2021), 8(12), JETIR, f1, < https://www.jetir.org/papers/JETIR2112501.pdf > accessed 27 February 2025.

[3] Shubham Singh Bagla, 'Electronic Evidence and Cyber Forensics in India' II HPNLU. L. J. 33 (2021), < https://doi.org/10.70556/hpnlu-lj-v2-2021-02>, accessed 27 February 2025.

[4] Vanshika Shukla, 'The Admissibility Of Digital Evidence: Challenges And Future Implications' Journal (9), Commonwealth Law Review < https://thelawbrigade.com/wp-content/uploads/2023/09/Vanshika-Shukla-CLRJ.pdf>, accessed 27 February 2025.

[5] Pooja Gaur, 'New Technologies in Forensic Evidence Law in India: An Analytical Study' (2024) 4(3), International Journal of Advanced Legal Research, <https://ijalr.in/wp-content/uploads/2024/04/NEW_TECHNOLOGIES_IN_FORENSIC_EVIDENCE_LAW_IN_INDIA-rp-REVISED.pdf>, accessed 27 February 2025

[6] Ganguli, Prithwish, 'Admissibility of Digital Evidence under Bharatiya Sakshya Sanhita: A Comparative Study with the Indian Evidence Act' (October 06, 2024). Available at SSRN: <https://ssrn.com/abstract=4977238 or http://dx.doi.

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

security and privacy law, providing great insights to the policy makers and legal professionals, shifting the evolving technology". This paper concludes that bridging the gap between the law and technologies involves a multi faced approach the comprises of legislation, providing the proper education, collaboration and innovation.

IV. OBJECTIVE OF THE RESEARCH

The main objective of this research paper is to discuss the challenges in admissibility of digital evidence in the virtual hearing and ensuring fair trial in the legal proceedings.

V. FAIR TRIAL

A famous quote by the English Jurist William Blackstone that, "It is better that ten guilty escape than one innocent suffers" which clearly explains that even one innocent should not be punished or become a victim. Under the constitution of India Right to get a fair trial is a basic Fundamental Right. The Indian constitution, by Article 21 provides "the protection of life and personal liberty for both citizens and foreigners except enemy aliens and the above said fundamental right can be bereaved only based on procedure established by law". Article 21 is sine quo non for true and fair trial. Each person has a right to be dealt with fair trial, further denial of fair trial leads to injustice to victim as well as society[7].

VI. VIRTUAL HEARING

The term virtual hearing suggests that hearing of cases by using of remote working system. With the help of various prescribed software's and tools including video conference, and means of the audio-visual mode as hybrid hearing instead of the physical mode. The cases in the court are progressed, dealt, investigated without the need of legal counsels for both side that is petitioners and respondent to attend the court in person. The section 2 sub clause (1)(a) of the Bharatiya Sakshya Adhiniyam, 2023, describes the term "court which includes all judges and magistrates of all courts and all persons with one exception (i.e.) arbitrators who legally authorized to take evidence on the both sides". The term "court includes not only a physical court and also virtual court or tribunal" [8] where the case proceedings are takes place and justice is rendered.

The virtual court a judicial forum where both parties that is litigants and lawyers not present physically and thereby judicial services are rendered electronically through computer software technology.

VII. VIRTUAL HEARING AND PROCEDURAL ISSUES

A. Allotment of Cases

The administrative bias which was existing has to be evaluated and has to resolve. As the judiciary was last resort, but in some extent still there was issues in case allotment including transfer of case too. The Madras High court declared that "the transfer of case from Villupuram to Vellore is ex facie illegal and not *non-est* in the eyes of law" [9], which evidently shows that bias in transfer of cases. Not only High court facing these kind of issues, even top apex court (i.e.) Supreme Court had faced a similar issue in the allocation of matters and cases to the judges. Where the Supreme court dealt all kind of cases including writs, public interest litigation and special leave petitions, "while allocation of cases including writs, public interest litigation and special leave petitions the chief justice of India decided to keep the public interest litigation cases to himself and not to allocate it to other judges which clearly shows that there was a bias in allotment of cases"[10].

B. Maintining of E-Record

Another issue in the virtual hearing is maintaining e-record, for respective cases where paralegal staff is not equipped and trained to handle the documents and evidence, make accessible while in the proceedings.

C. Technological Handicap

org/10.2139/ssrn.4977238> , accessed 27 February 2025

[7] Zahira HAbibullah Sheikh and Ors. V. State of Gujarat and ors, [2004] INSC 256

[8] Model Rules for Video Conferencing for Courts, 'video conferencing rules', 2, < https://cdnbbsr.s3waas.gov.in/s388ef51f0bf911e452e8dbb1d807a81ab/uploads/2020/08/2020082629.pdf>, accessed 23 January 2025.

[9] Suo Motu RC v. Vigilance and Anti-Corruption wing, [2023] SCC OnLine Mad 5304, [1]

[10] PTI 'Supreme Court adopts roster system for allocation of matters, CJI keeps PIL cases' Wionews (India, 1 February 2018) < https://www.wionews.com/india-news/supreme-court-adopts-roster-system-for-allocation-of-matters-cji-keeps-pil-cases-31488>, accessed 28 January 2025.

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

The technological illiteracy in India is a challenge has to tackle in the system of virtual courts viable in India. At present, many of advocates are practicing nationwide where an urgent relief is needed but technological handicap prevents them approaching the court and urgent seek the disposal of cases.

D. Prisoner Appearance

All jurisdictions have a legislation allowing to an accused person to appear before the court within certain matters like adjournment, subsequent remand process and bail application process. In the virtual hearing, the prison has to equip to meet their counsel and conduct the court proceedings. The digital divide made as a barrier to equip to meet their counsel and conduct the court proceedings.

VIII. DIGITAL EVIDENCE

A. The Information Technology Act, 2000

According to the Section 2 sub clause (1) (t) of the Information technology Act,2000, Electronic record means "that data which is recorded or otherwise data generated as in the form of image format or sounds which are stored, which is received or even sent in any electronic form as micro film or computer-generated micro fiche". Further the Section 2 sub clause (1) (o) of the Information technology Act, 2000, provides that "Data is the one which represents the collection of well-defined information, knowledge, collection of facts, concepts or instructions which are prepared or have been prepared in the formalized manner and is intended to be processed in the computer system or computer system network may be stored in computer internally or externally in any form including computer printouts or any other storage media devices".

B. The Bhartiya Sakshya Adhiniyam,2023

Under the Section 2 sub clause (1) (e) of the Bhartiya Sakshya Adhiniyam Act,2023 , "Evidence that includes all the statements which are presented electronically before the court of law and also the court has to permits or required to be made before it by witnessing the relation to matters of fact under inquiry and such statements are called oral evidence and all documents including electronically or digital records produced for the court inspection, those documents are called as documentary evidence".

The definition of document under Section 2 sub clause (1) (d) of the Bhartiya Sakshya Adhiniyam act,2023 which clearly provides that document includes both electronic and digital records (.i.e.) "document means any matter of content expressed in any form or described in any form or otherwise, which is in any form of substance of letters, figures or any sign marks or any other means which is used to recording any matter that includes electronic and digital records". In other words, an electronic record on email, server logs, and documents stored in the computer, laptops, mobile phones, messages, location evidence and voice mail stored in digital devices are documents.

IX. TYPES OF DIGITAL EVIDENCE

Due to technology advancement digital evidence forms also takes different dimensions. There are various types of digital evidence. They are communication through text message, emails, instant messaging apps and other platforms. Digital documents include spread sheets, presentations and other types of files. Even the digital financial records for transactions also to be considered as digital evidence.

X. LEGAL RECOGNITION OF DIGITAL EVIDENCE TO ENSURE THE FAIR TRIAL

In the virtual hearing, the digital evidence plays a crucial role to ensure the fair trial. The provisions for recognition of legal status of digital evidence to be examined based on legislative provisions of The Information Technology Act,2000, The Indian Evidence Act,1872 and The Bhartiya Sakshya Adhiniyam, 2023.

A. The Information Technology Act, 2000

Regarding the legal recognition of electronic records, under the Section 4 of the Information Technology act, 2000 which provides that "any information or any other matter which shall be in any form of writing or in any form of typewritten or in any form of printed format then irrespective of any law, such requirement has to be presumed to have been satisfied the following essential ingredients,

a) The collection of information which is to be provided, produced are even made in the electronic form,

b) Provided that such information to be used in subsequent future reference.

NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

Further any electronic records and electronic signatures are used for government and its agencies as prescribed by the law".

According to section 6 of the Information Technology Act, 2000 it is to be understood that "the usage of electronic records and electronic signatures within governmental bodies including their associated agencies, where the law says that any electronic records mandated for use in and with the regulations established by the governmental bodies including their associated agencies for purpose as specified, for example completion of forms or permission issuance shall be deemed to fulfilled. Those records should confirm the regulations prescribed and set forth by the government, and they will be considered as admissible evidence" before the court of law to conduct the trial proceedings.

Central government may appoint the experts to examine the electronic form of evidence, for getting an opinion on the evidence which is in electronic form before any court or any other authority[11] as in the Section 39 of the Bhartiya Sakshya Adhiniyam, 2023. The explanation for electronic form evidence means "any information which is used for corroborative, confirmation, probative value either stored as in any electronic format or the information which is stores is transmitted to any electronically form which includes computer evidence, digital audio format, digital video format, cellular phones, digital fax machines"[12]. All these forms are admitted by the court during civil and criminal trials.

B. The Indian Evidence Act,1872

According to Section 65 of Indian Evidence Act shows the keen intention of drafters to uphold the principle of natural justice. Generally, primary evidence is accepted in the court. But in certain conditions, secondary evidence is also admissible. The term certain conditions have the broad sense of nature, (.i.e.) "where the original documents belong to the one party (petitioner or appellant) but it appears to be the opposite party (defendant or respondent) or existence of original documents for the relevant case is admitted by the opposite party or where the original documents which is difficult to move and difficult to be produced before the court of law, then the secondary evidence is admissible before the court law". For example, cell phone records, WhatsApp chats are stored in massive servers and cannot be moved and produced before the court of law. Based on Section 63 and Section 65 of the Act, those recordings and chats are permitted as secondary evidence and produced before court of law in the prescribed form.

The contents in the electronic record are proved as in the Section 65B of the Indian Evidence Act,1872. Admissibility of electronic records, that is any data which is in electronic format is printed on paper, stored, recorded and copied in the optical storage devices or copied in any electronic form as considered as the document. It is submitted in the prescribed form of certificate and it is used as corroborative evidence in the court of law. The admissibility of electronic recorded which directly provides that electronic records are admissible for evidence before the court of law to conduct civil and criminal proceedings. The admissibility of electronic records which directly provides that electronic records are admissible for evidence before the court of law to conduct civil and criminal trials.

C. The Bhartiya Sakshya Adhiniyam,2023

The Section 60 of Bhartiya Sakshya Adhiniyam, 2023 provides that in certain conditions secondary evidence is admissible before the court of law. The term certain conditions have the broad sense of nature, (i.e.) "where the original documents belong to one party (petitioner or appellant) but it appears to be the opposite party (defendant or respondent) or existence of original documents for the relevant case is admitted by the opposite party or where the original documents which is difficult to move and difficult to be produced before the court of law, then the secondary evidence is admissible before the court of law". For example, cell phone records, WhatsApp chats are stored in massive servers and cannot be moved and produced before the court of law. Based on Section 58 and Section 60, those recordings and chats are permitted as secondary evidence and produced before the court of law in the prescribed form.

While examining the provisions of admissibility of electronic records[13] any data which is in electronic format is printed on paper, stored, recorded and copied in the optical

[11] Section 2(1)(o) The Information Technology Act, 2000 (Act 21 of 2000)

[12] Section 79A The Information Technology Act , 2000 (Act 21 of 2000)

[13] Section 63 The Bhartiya Sakshya Adhiniyam, 2023

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

storage devices or copied in any electronic form as considered as the document. It has to be submitted in the prescribed form of certificate and it is used as corroborative evidence in the court of law.

The admissibility of electronic records which directly provides that electronic records are admissible for evidence before the court of law to conduct civil and criminal trials.

D. Interpretation of the Section 65b and Section 63

While interpretation the Section 65 of the evidence act, first have to trace back the amendments carried out in the Information Technology Act, 2000, "subsequently the amendment made an impact to the provision of Indian evidence Act and Indian penal code of 1860"[14]. While reading the Section 4 of the Information technology Act, the concept of electronic record and Section 92 of the Information Technology Act was amended to include the term electronic record which allows the admissibility of the digital evidence. While exploring the provisions, the author of article encountered a contrasting factor that is between the electronic data (i.e.) magnetic digital data contained on the device which was original and the copies produced before the court of law. Further, the electronic device which had retrieved by the investigation agencies and it is examined by cyber forensics laboratory, which deemed to be the original document and which was printed and reproduced the same as secondary evidence. In case of the secondary evidence, certificate of authenticity is very essential, while submitting before the court of law at that time of cross examination.

While microscopic analysis of Section 65B of the Evidence Act it consists of technical and non-technical reasons for acceptance of the electronic evidence. Section 65B (2) of Evidence Act provides the technical reasons and circumstances in which a duplicate copy of an electronic record may be used and utilized. Any electronic record which are taken from any computer system or any computer network system, at the time of production of the electronic records, the above said computer system produced before the court must be used properly in regular manner. The information contained in the electronic record must be entered regularly in a computer system. The essential part in computer has to work properly and a duplicate copy must be reproduced of the original electronic record.

As provided in provisions it mandates the need of authentic certificate which needs to be proved and person who is the in charge of the device (where the data is stored) must be signed. Further, the certificate must identify the question in records and how It is to be produced before the competent authority and the details that are provided while the production of electronic records, for the purpose of proving that the electronic record was generated by a computer system. The core part is regarding authenticity of source, and how the provided information is accurate as so much when placed before the court of law. The reason behind it is that there is a chance that electronic data can be interfered, modified and manipulated which affects the whole trial process and affects fair trial process. But still there are issues and problems in producing the electronic evidence.

The certificate is given by a person who has recorded the electronic evidence. But in some cases, obtaining of certificate is a challenging process because it was recorded by the accused himself. As per Article 20 of the constitution of India the accused cannot be compelled to give evidence against himself. Some situations are even more challengeable and worsen as the person cannot be traced who created the video or recorded video or cannot come before the court of law while conducting the trial process and also denies the given certificates.

In some criminal cases accused gets acquittal and released due to absence of certificate or not produced in the court. While micro analysis and trace back the drafter's inspiration, it is evident that Section 65B of the Indian Evidence Act and Section 63 of the Bhartiya Sakshya Adhiniyam act are drawn from Section 5 of The United Kingdom Civil Evidence Act, 1968. But, based on the United Kingdom Law Commission report, UK civil evidence act was repealed by the Civil Evidence Act 1995 which clearly shows significant changes in the former act.

The recent enactment of the Bhartiya Sakshya Adhiniyam, in 2023, provided ample opportunity and it is almost a copy of section 65B of the Indian Evidence Act with some minor changes. But the minor change brought

[14] Ashwini Vaidialingam, 'Authenticating Electronic Evidence: §65b, Indian Evidence Act, 1872', (January-June,2015) ,8(43) (2015) ,Nujs Law Review,45, <Http://Docs.Manupatra.In/Newsline/Articles/Upload/86fce7db-49e9-44f4-9941-Dd9d4bdb2aca.Pdf>, Accessed 28 February 2025.

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

the huge impact in the fair trail process under Section 65B of the Indian Evidence Act, certificate was required only from the owner or in charge of the device concerned, but under Section 63 of The Bhartiya Sakshya Adhiniyam, two certificates are required as given in the Schedule i.e. one from the owner or the in charge of the device concerned and another from an expert.

XI. ROLE OF INDIAN JUDICIARY

Admissibility of digital evidence has evolved in recent days in the court of law. Opinions are provided by technical expert to ensure evidence is free from tampering and manipulation and to render the justice with fairness. Judicial interpretation was done for digital evidence to find the creditability, integrity and authenticity.

In the case of *Anvar. P.V. v. P.K.Basheer* [15], the judgment of case highlighted importance of certification of digital evidence for its authenticity. Further the case had underscored importance of section 65B of Indian Evidence Act, while producing digital evidence.

In the case of *Manu Sharma V. State (NCT of Delhi)*[16], digital evidence plays an important role in the conviction of Jessica murder case. It is one of the cases that court had underscored the importance of the digital evidence and allowed the admissibility of digital evidence in the court of law and upheld the rule of law ensuring justice.

In the case of *Shafhi Mohameed V. State of Himachal Pradesh* [17], the supreme court of India had addressed the issues in the admissibility of digital evidence specifically pointed out that the party presenting evidence is not in possession of device that generated documents and discussed applicability of Section 65B of the Indian Evidence Act. It was held that "the certificate is not necessary, while producing electronic evidence by a party, who is not in possession of a device. The court had allowing electronic evidence without certificate instead of procedural requirement of the certificate under Section 65B(4) and replaced procedural requirement to uphold the justice" (para 12).

In the case of *Tomaso Bruno V. State of Uttar Pradesh*[18], the court highlighted the importance of the digital evidence especially in absence of direct evidence and direct witness testimony. The court emphasized CCTV footage played a crucial role in criminal investigation and handled with more care regarding admissibility and accuracy of evidence.

A. Can WhatsApp messages be admissible as digital evidence?

In the case, *National Lawyer campaign for judicial transparency and reforms V. Union of India*[19], The High Court of Delhi held "that document received in WhatsApp forward is not considered as a document in term of provisions of Indian Evidence Act 1872, that is neither the original nor the copy of original has been produced". But later in the case of *M/S. Karuna Abhushan Pvt. Ltd V. Shri Achal Kedia* [20], The High Court of Delhi in this case discussed the validity of WhatsApp messages as legal evidence. The court held "That messages sent through WhatsApp also are valid as legal evidence and the blue tick over the messages is a valid proof that the recipient read the sent message. It also held that the mobile WhatsApp and Facebook chats are taken as valid evidence proof in the court of law during trial proceedings". Further, the court iterated those purposes of proving the WhatsApp chats, the section 65B of the Indian Evidence Act should be followed.

In the case of *Rakesh Kumar Singla V. Union of India* [21], The Punjab and Haryana High Court cited the judgment of *Arjun Panditrao V. Kailash Kushanrao*[22] and held that "Certificate under Section 65B of The Indian Evidence Act is required when party wishes to produce WhatsApp messages as electronic device". Thus, the court concluded the WhatsApp messages can be relied upon after due compliance with section 65B of The Indian Evidence Act.

B. Analysis of Judicial Interpretation

From the judicial interpretation, it is very clear that in the case of *Anvar. P.V. v. P.K.Basheer* [23], which highlighted the importance of certification of digital evidence for its authenticity. *Manu Sharma V. State*

[15] (2014) 10 SCC 473
[16] (2010) 6 SCC 1
[17] (2018) 2 SCC 801, (12)
[18] 2015 INSC 52
[19] Writ Petition (C) No.191 of 2019
[20] M/S. Karuna Abhushan Pvt. Ltd V. Shri Achal Kedia (2020), (8.2)
[21] Rakesh Kumar Singla V. Union of India (2021)
[22] Arjun Panditrao V. Kailash Kushanrao (2020)
[23] (2014) 10 SCC 473

(NCT of Delhi)[24], where digital evidence played an important role in the conviction of the accused in Jessica murder case. *Tomaso Bruno V. State of Uttar Pradesh*[25], the court highlighted the importance of the digital evidence especially in absence of direct evidence and direct witness testimony and emphasized CCTV footage played an important role in investigation.

In the case, *National Lawyer campaign for judicial transparency and reforms V. Union of India* [26], The High Court of Delhi had rejected WhatsApp forward and not considered it as an document in terms of provisions of Indian Evidence Act, 1872, but court reiterated its earlier decision in the case of *M/S. Karuna Abhushan Pvt. Ltd V. Shri Achal Kedia* [27], The court held that "Messages sent through WhatsApp are also be valid legal evidence and the blue tick over the messages is a valid proof that the recipient read the sent message. It also held that the mobile WhatsApp and face book chats are taken as valid evidence proof in the court of law during trial proceedings. Further, the court iterated those purposes of proving the WhatsApp chats, the section 65B of the Indian Evidence Act should be followed (Para 8.2)".

Further in the case law *Rakesh Kumar Singla V. Union of India* [28], The Punjab and Haryana High Court in this case cited "the judgment of *Arjun Panditrao V. Kailash Kushanrao*[29] and held that certificate under Section 65B of the Indian Evidence Act is required when party wishes to produce WhatsApp messages as electronic device (Para 11)".

Thus, the judicial decisions are concluded that WhatsApp messages can be relied upon after due compliance with Section 65B of The Indian Evidence Act.

XII. FAIR TRIAL AND ADMISSIBILITY OF DIGITAL EVIDENCE

As we know that fair trial is the right of the victim, if not it will affect the victim and the society. The court will render justice based on the production of documents and safeguard the rights of victim. In order to ensure the fair trial reasonable opportunity has to be given to both parties for production of documents on each side. For admissibility of evidence before court of law it has to meet out essential ingredients.

A. Relevancy

Based on the Golden rule of evidence, it is said that i) Evidence must be confined to the matter in the issue, ii) Hearsay evidence must not be admitted, iii) Best evidence must be given in all cases. The first rule implies that evidence produced for the trail proceedings must be confined with issues concerned with the respective case which means the relevancy factor. Based on the principle it is said that relevancy of evidence not only play an important role in traditional court also in the virtual hearing. So, it is said to be "every evidence of the matter of issues must be directly or indirectly connected to person who were involved in the crime"[30]. For example, if a crime conducted by a person and call records are submitted as evidence to the court of law. Then, it is crucial factor whether that call records of a person are connected and involved in the crime and makes him as suspect. So, relevancy of an evidence plays a pivotal role and is one of the main ingredients.

B. Legality

Every evidence which is collected must follow proper legal procedure and should involve adhering to search and seizure laws and validating rights against self-incrimination. In the case of *Selvi vs. State of Karnataka* [31] the court highlighted the interrelationship between Article 20(3) and Article 21 of Indian constitution, analyzing how collection of data is against self -incrimination and how it complements each other. The judgment made a paradigm shift in the criminal process nature for conducting trial criminal proceedings. In this article author has highlighted and addressed the gadgets concern over collection of evidence and its legality.

C. Reliability

[24] (2008) 5 SCC 230
[25] 2015 INSC 52
[26] Writ Petition (C) No.191 of 2019
[27] M/S. Karuna Abhushan Pvt. Ltd V. Shri Achal Kedia (2020), (8.2)
[28] Rakesh Kumar Singla V. Union of India(2021) (11)
[29] Arjun Panditrao V. Kailash Kushanrao (2020)
[30] Pooja Gaur, 'New Technologies in Forensic Evidence Law in India: An Analytical Study' VOLUME 4, INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH, FEBRUARY 2024, availableat < https://ijalr.in/wp-content/uploads/2024/04/NEW_TECHNOLOGIES_IN_FORENSIC_EVIDENCE_LAW_IN_INDIA-rp-REVISED.pdf>, accessed 23 January 2025
[31] (2010) 7 SCC 263

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

The scientific methods which have been employed in gathering and examining of evidence must be validated by expert community and court also carefully.

D. Authenticity of the Digital Evidence

The digital evidence which was collected and produced for corroboration before the court of law must be authenticated and it should show that claim to the relevant case[32]. The authenticity which shows the origin of evidence that is when and where it is collected from.

E. Data Collection Methods

The methods used for collection of data are such that it will impact the admissibility of the evidence. The collection of data must comply with the law and privacy, if it violates then it cannot be admissible before the court of law.

F. Privacy and Data Protection Law

In the digital evidence, collection of evidence must comply with privacy and data protection law, if any evidence while obtaining is unlawful then it is not to be accepted in the court of law.

G. Relevance to the legal proceedings

The digital evidence which was collected and produced for corroboration before the court of law is relevant to the civil or criminal proceedings.

H. Integrity of the digital evidence

The digital evidence which was collected and produced for corroboration before the court of law must be protected and free from tampering or alteration.

I. Fairness and due process

The court considers whether the admission of digital evidence would violate defender's right of fairness and due process.

Admissibility of digital evidence is more complex. The legal professionals have to often interact with experts and obtain an expert opinion regarding evidence obtained to comply with relevant legislations and also properly preserve and produced it before the court of law.

XIII. FINDINGS AND ANALYSIS

The author has highlighted the recent initiatives by the e-court projects which makes a quantum leap in fair trial. The inter-operable criminal justice system (ICJS) which said to be completed in the year of 2026. The platform which "enables integration on the main IT systems and it is used for delivery of criminal justice system through the nation. It comprises of five pillars viz. Police (crime and criminal tracking and networking system), e- forensics, e- courts, e- prosecution for public prosecutors and e-prisons for prisons"[33].

The inter-operable criminal justice system (ICJS), has both side merits, and demerits. The merits are as follows.

"Reduces errors and times consuming while in the process of sharing the necessary information between different pillars of criminal justice system and thereby enabling speedy justice. Improving the investigation quality, by use of scientific technologies and analytics which had inbuilt in the platform and effective tool for the case and court management as one click solution that is all the relevant information regarding of a case will be available in real time which is used by the courts. Issue of summons, witnessing the parties and Compliance of judicial orders for the trail proceedings are achieved easily through this process and there by productivity is achieved, reduce the wastage of time"[34].

The author of the research had encountered demerits in the inter-operable criminal justice system (ICJS) and shortcoming in the admissibility of digital evidence before the court of law during virtual hearing. The shortcomings are as highlighted below:

A. Operational challenges

The challenge of the digital evidence about its origin and its authenticity. In the digital world, origin of data is questionable. Generally digital data are stored in different servers in the computer networking system. For example, the cell phone records, messages in the

[32] Vanshika Shukla, 'The Admissibility Of Digital Evidence: Challenges And Future Implications' Journal (9), Commonwealth Law Review < https://thelawbrigade.com/wp-content/uploads/2023/09/Vanshika-Shukla-CLRJ.pdf>, accessed 27 February 2025.

[33] Inter-Operable Criminal Justice System Project,(drishtiias,19 February 2022),<https://www.drishtiias.com/daily-news-analysis/inter-operable-criminal-justice-system-project>, accessed 28 February 2025

[34] Inter-Operable Criminal Justice System Project,(iasbaba,3 April 2022),< https://iasbaba.com/2022/04/inter-operable-criminal-justice-system-icjs/ >, accessed 28 February 2025

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

WhatsApp application are stored in large servers and it is difficult to retrieve it from different servers. In case it is retrieved from different servers then the first question arises how to determine territorial origin and its authenticity. It causes a negative result in investigation, and also affects the fair trial in the court of law.

The operational challenges faced by the inter-operable criminal justice system (ICJS), crime and criminal tracking network systems (CCTNS), aimed to "inter link all police stations under common application software for the purpose of investigation, data analytics, research policies, providing citizens to raise a complaint and tracking an compliant status and request to police verification"[35]. Though the criminal tracking network systems aims to inter connect with nationwide police stations.

By analysis the demand of grants 2023-24 of PRS India report it is clearly shown that "Rs 3,800 crore has been allocated for modernization of police forces, which is a 56% increase from the revised estimates for 2022-23. There has been a 73% increase in allocation towards the Modernization of State Police Forces Scheme and the crime and criminal tracking network systems scheme which clearly provides that crime and criminal tracking network systems has move further ahead"[36].

B. Cloud computing issues

In general, that data are stored in massive servers in the computer system network. In recent days, cloud computing system is getting more advantageous. As it offers massive resource protocol. It is a cost-effective solution and it is dynamic and it offers a wide access of storage. Most of the companies had transferred their data to cloud storage systems. Most of the governments and companies have accepted cloud storage system. The service provider accepts data from various jurisdictions and stores it in its systems. Moreover, retrieval of data from cloud computing is more complex.

While addressing the cloud computing in the e-courts systems, other systems that is e-prison, e- prosecution and e- forensics are to be analyzed here the data is collected from crime and criminal tracking network systems which are linked to all other police stations and also linked to e- forensics and linked to e-prison. But the in one umbrella systems, if any of one of the systems fails, then entire ecosystem will affect and eventually affect the fair trial.

By analysis the demand of grants 2023-24 of PRS India report it is clearly shown that "forensic labs are not uniformly distributed across states and also in the union territories. While comparing the states, Uttar Pradesh and Bihar have four and two functional regional forensic science laboratories on the other hand Andhra Pradesh and Tamil Nadu have five and ten, respectively. The Committee on Home Affairs (2022) recommended that the Ministry should set up one forensic laboratory in every state capital within a two-year timeframe and every city with a population over one million person and further states that lack cyber cells compared to the states such as Rajasthan, Goa, and Punjab, do not have a single cybercrime cell"[37].

C. Complex technology

Presence of various types of digital evidence (i.e.) communication through text message, emails, instant messaging apps and other platforms and also digital documents like spread sheets, presentations and other types of files makes its complex. Even the digital financial records for transactions are to be considered as digital evidence, which involves different technology, Such as data encryption, data recovery and digital forensics. Also add to the complexity. The court might struggle to understand complexity involved in the data to determine the relevancy and admissibility for the trials.

D. Data protection and its privacy

Another challenge is be data protection and its privacy. Information which is stored is either personnel or confidential. However, it is also a threat to people's right to privacy. Such rights are protected under Article 21 of Indian constitution. So, there is need of balance between collection of evidence and privacy concern.

E. Collection of data

[35] Ministry of Home Affairs, Inter-operable 'Criminal Justice System (ICJS)', <https://www.mha.gov.in/en/commoncontent/inter-operable-criminal-justice-system-icjs>, accessed 28 February 2025.

[36] Demand for Grants 2023-24 Analysis Home Affairs, PRS legislative research, < https://prsindia.org/files/budget/budget_parliament/2023/DFG_MHA_2023-24.pdf> accessed 19 February 2025.

[37] id., at p. 16

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

The challenges faced by investigation officer with respect of collection of evidence in What's App. In today's world many applications like What's App, Telegram are used for communication. It is always a question whether What's App documents are admissible as evidence before the court of law. As it is evident clearly that any data that can be obtained must follow the legal procedures. Applications like What's App are widely used for communications and data are stored in different servers. The main challenge is the collection of data.

Reason behind this is Article 20(3) it provides that no person should be compelled to accused himself. But in the case of What's App, compelling of accused to unlock his phone to access What's App chats is a violation of the above said article. But in some cases, police can unlock or accused the phone.

The Indian court observed that forcing to unlock mobile is violation of Fundamental Right of Article 20(3). The Indian law on self – incrimination can be summarized based on the *Selvi vs. State of Karnataka* [38] , the court highlighting the interrelationship between Article 20(3) and Article 21 of Indian constitution, analyzing how collection of data is against self -incrimination shares as a complement each other. But there is an exception for Article 20(3) that is testimonial evidence can be compelled from accused if the material is already with the investigation officers.

F. Search and seizure authority

The court will accept when the evidence was collected and admissible based on the legal procedure. Any data which is collected against law is invalid. It is also challengeable when the evidence is collected without valid warrant. If the collection of evidence does not follow procedural safeguards, protocols it leads to challenges regarding reliability of evidence.

G. Cross-border implications

Collecting of digital evidence in case of international and domestic cases are difficult to find and define and definite boundary. When there is a data transfer between the countries jurisdictional conflicts and authenticity are to be considered before producing it in the court of law.

H. Issues in chain of custody

The acquisition and processing of electronic evidence must be adhered by rigorous chain of custody. The section 65B of Indian Evidence Act provides admissibility of electronic records and section 63 of Bhartiya Sakshya Adhiniyam, 2023 Act provides admissibility of electronic records. The state has to frame rules and regulations to prevent violation of collected data to be produced as evidence in the court of law. Here the vulnerability of data in all stages is due to computerized technology.

I. Ethical aspects

Conscientious in collecting and handling of evidence must be followed. Apart from legal aspects and professional aspects, another issue faces ethical issues. Instance of tampering and manipulation, changes of samples are reported from time to time. Apart from the prosecution maintenance of custody plays a vital role.

J. Advancement of digital technology

Advancement of different technology and new forms of documents, methods of manipulation emerge rapidly along with technology. Courts are facing struggle to access the evidence.

K. Challenges in data recovery

The investigation officer faces the data recovery challenges in case of loss of data. Generally, documents are stored internally in the computer system and computer network systems and massive servers. If data stored in the computer system and computer network systems and massive servers are deleted or erased or even hidden. It is difficult to retrieve the data. The investigation officer cannot carry forward investigation and produce the evidence before the court of law.

L. Usage of anti-forensic techniques

The perpetrators of crime involve in anti-forensic techniques to hide their activities and make it more challenging to investigation officers for collection of data and producing it as evidence before the court of law.

M. Digital divide

Moreover, the usage of internet has been widely increased in both urban and rural areas but there is a still existence of digital divide which makes it difficult for the litigants to present the evidence before the court of law.

[38] (2010) 7 SCC 263

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

N. Cryptography and data hiding

The cryptography is a technique which used by perpetrators of crime to hide the data. These hiding techniques make it challenging for the investigation procedure which affects the fair trial process.

XIV. SUGEESTIONS AND FUTURE TRENDS

From the analysis, the author had encountered that there was an intersection between technological innovations and legal proceedings which have become more significant. As the technological innovations evolve, the law also has to evolve in consistent with the innovations. For the bridging of technology with law, proper educational training and collaboration and innovation have to take place. The author of the research has suggested some recommendations which will reduce challenges in the digital evidence and ensure the fair trial in virtual hearings and delivering justice[39]. They are as follows:

A. Improving the digital forensic mechanism

It is necessary to constitute digital forensic laboratories and more training has to be given for investigation officer. The government has to do periodical surveillance and update the security system in order to prevent any loss or any damage to servers and storage capacity systems.

B. Establishing a central networking system

To establish the central networking system to securely store and retrieve all the documents in the server in order to prevent from tampering and manipulation of evidences. For the retrieval of the digital evidence which has been stored in massive servers have to be stored in single repository or formed by the central networking system.

C. Training and updating of software

To address the complex technology, proper training has to be provided to the investigation officers to encrypt data stored in the servers and in the computer systems and forensic laboratories software have to be updated from time to time.

D. Fostering innovation

As technology continues its advancement, there is a need of law to encourage new innovations. More research and developments have to be established to bridge the lacuna between technology and law. Fintech innovations have to be promoted by the legislators and create more public awareness and encouraging innovations will ensure that the legal system will evolve with technological advancement.

E. Collaboration with technological companies

To provided tools and software the government has to collaborate with many companies in order to collect, preserve the digital evidence and to be free from tampering or manipulation of data. The Memorandum of understanding have to be made between the companies for the formation of technical experts committee, software workshops have to be organized which will aid for law enforcement agencies to produce digital evidence before the court of law.

F. International cooperation

Strengthening the international collaboration with law enforcement agencies and formulating information exchange agreement, capacity building and joint investigation on the cross-border implications will eventually ensure the fair trial proceedings before the court of law.

I. Block chain technology

In order to prevent from tampering or manipulation of data the block chain technology is used. A distributed ledger system of block chain custody is used to create a fool proof chain of custody for electronic evidence. For forensic laboratories information security management certification have to provided.

J. Artificial intelligence and machine learning

Artificial intelligence and machine learning systems are used to generate more data. Court has to analyze the evidence for its creditability. Policy makers have to consider it and taking to account while making a new policy.

K. Usage of metadata

[39] Ganguli, Prithwish, 'Admissibility of Digital Evidence under Bharatiya Sakshya Sanhita: A Comparative Study with the Indian Evidence Act ' (October 06, 2024). Available at SSRN:< https://ssrn.com/abstract=4977238 or http://dx.doi.org/10.2139/ssrn.4977238> accessed 23 January 2025.

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

Meta data will provide origin of data, which will aid to find the authenticity and chain of custody. Artificial intelligence and machine learning systems are used to generate more data. Court has to analyze the evidence for its creditability. Policy makers have to consider it and taking to account while making a new policy.

L. Integration of virtual reality in evidence

The virtual reality and Augmented reality play an important role in presenting evidence in the court of law. Virtual reality technologies are used to recreate crime scenes and visuals of the crime scene produce it before the court. So that it is easier to understand complex evidences. As the technology evolves, along the side law has integrated with those technologies. The legislators have to consider necessity of integration and have to update legal frame work.

M. Collection from smart devices

The usage of smart devices which save large amount of data can be produced before the court as evidences. The smart devices which are connected with vehicles and wearables can collect data. By analyzing stored data, the investigating authorities can find any suspicious activity is involved or not without the breach of privacy.

N. Usage of data recovery and data carving

Generally, when the data is erased, its space has been marked for reuse. At that time of another data is stored the space will be swept off. So, in order to recover data, recovering techniques like data carving and data reconstruction techniques are used.

O. Speed and efficiency

In the collection of digital evidence artificial intelligence usage will analysis the data accurately and provide at a greater speed. By this, investigating agencies will investigate and collect the accurate data and produce it before the court in a speedy manner.

P. Digital evidence preservation

The preservation of digital evidence plays a crucial part in the virtual hearing. The block chain technology, chain of custody and algorithms prevent from tampering and manipulation of evidence.

XV. FUTURE TRENDS IN DIGITAL EVIDENCE

The advancement of technology and its blend with the legal field makes it easy to the investigating agencies and litigants to produce the evidence before the court of law. The future trends in digital evidence are as follows:

A. Big data analysis

Big data analysis is easier for the investigating agencies to process and analyze massive data which are stored in the computer system and computer system servers. By using these kinds of advancement tools, advanced analytics can detect the hidden files. These technologies are used to solve the complex structures in data base. These are very useful for cyber investigations.

B. Automated forensic technologies

Automated forensic technologies which streamline the investigation process by automatic repetitive tasks that is collection of data and analysis of data. These automated forensic technologies focus on more complex cases and makes it easy for the investigating agencies and litigants to produce the evidence before the court of law.

C. Quantum computing

Quantum computing helps to resolves the complexity like cryptographic analysis and accelerating data analysis. This quantum computing performs the advanced stimulations and helps to understand cyber incidents.

D. Cyber deception

Cyber deception is detection and analysis of cyber threats in real time. These technologies are integrated into digital forensics studies for the tactics, training and its procedure.

XVI. CONCLUSION

The evolving technological advancement makes handling of digital evidence in the court room more contrast to the traditional method. The digital evidence plays a vital to decide the truth. The admissibility of evidence plays a crucial role to prove a case. The section 65B of the Indian Evidence act provides admissibility of electronic records and also recent enactment of the Bhartiya Sakshya Adhiniyam, in 2023, provided ample opportunity and it is almost a copy of section 65B of the Indian Evidence Act with some minor changes.

JFJ
Volume: 3, Issue: 1
January-June 2024
E-ISSN: 2584 - 0924

But the minor change brought the huge impact in the fair trail process under Section 65B of the Indian Evidence Act, certificate was required only from the owner or in charge of the device concerned, With this context, the digital evidence admissibility over the proceedings ensure the fair trail and the recent introduction of a new act The Bhartiya Sakshya Adhiniyam, 2023 provides which explicitly provides for admissibility of digital evidence and two certificates are required as given in the Schedule i.e. one from the owner or the in charge of the device concerned and another from an expert and who will expert is not explained in the Bhartiya Sakshya Adhiniyam.

The judiciary has highlighted the importance of certification of digital evidence for its authenticity, in the case of *Anvar. P.V. v. P.K.Basheer* [40], *Tomaso Bruno V. State of Uttar Pradesh*[41], the court highlighted the importance of the digital evidence especially in absence of direct evidence and direct witness testimony and emphasized CCTV footage played an important role in investigation.

PRS India report also highlighted to increase the Modernization of State Police Forces Scheme and establish the cyber forensic labs. Further, the law makers also considered the ransom attacks, cyber security threat in order to prevent digital evidence from tampering or manipulation.

The government has to reduce the digital divide, providing the computer network systems to court room for effective function. Further the supreme court interpreted existing legislation systems as possible ways along with advancement of technology and also it framed guidelines for virtual hearing and production of the evidence before the court of law and also it revised the guidelines time to time. Improving the digital forensic Mechanism, Establishing the central networking system, Training and Updating of Software, Fostering Innovation, Collaboration with Technology Companies, International Cooperation will ensure that the legal system will evolve with technological advancement.

The Indian approach over the digital evidence had over coupled with different investigating agencies which need to be looked on to ensure the fair trial.

[40] (2014) 10 SCC 473

[41] 2015 INSC 52