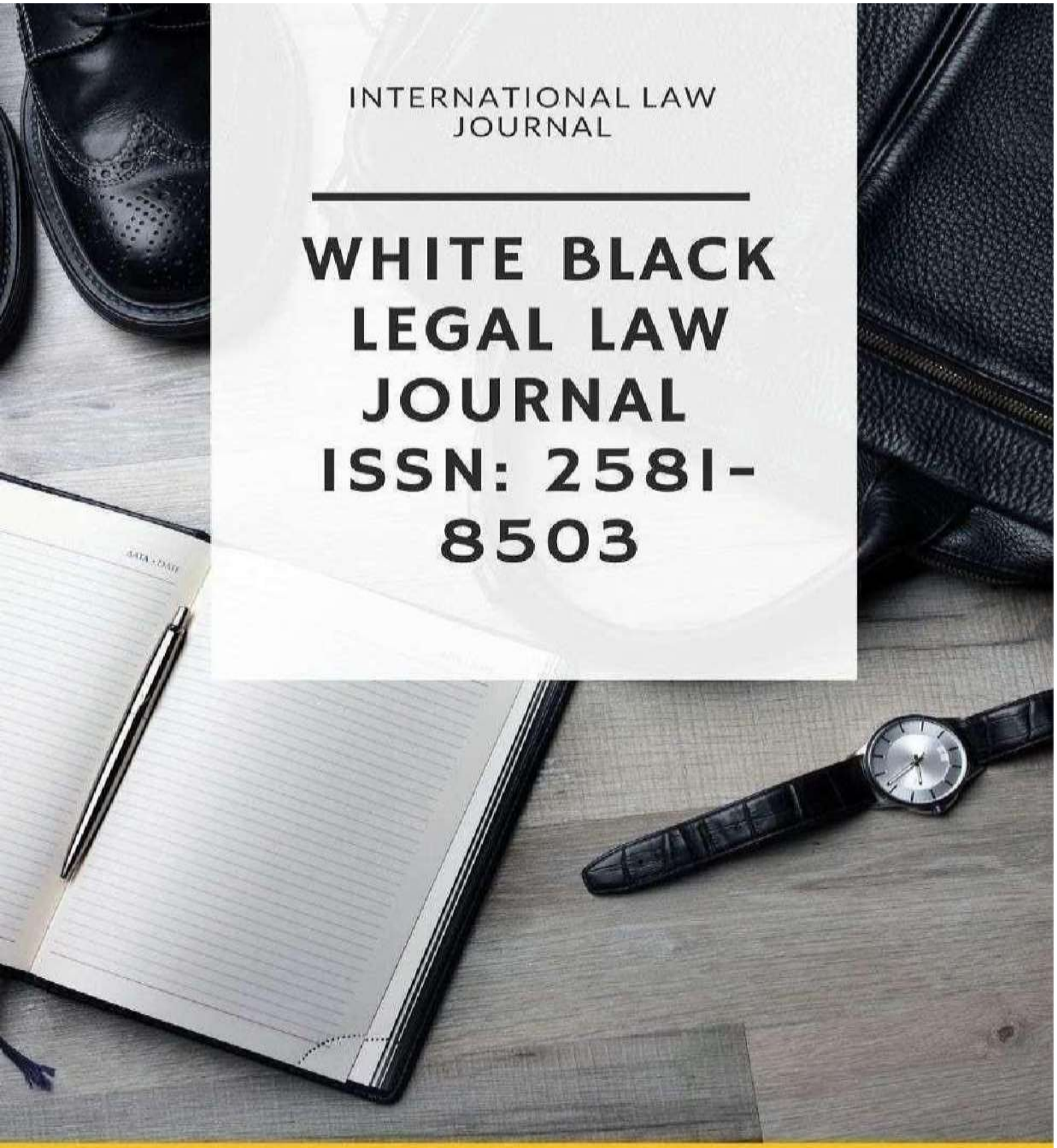

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

LEGAL FRAMEWORK OF DIGITAL EVIDENCE IN INDIAN CRIMINAL JUSTICE SYSTEM

AUTHORED BY - SUHANI
B.A.LLB
Amity Law School, Noida, Uttar Pradesh

CO-AUTHOR - DR. AMIT DHALL
Associate Professor
Amity Law School, Noida, Uttar Pradesh

1.1 Introduction

Initially, digital evidence did not bear any legal recognition before the court. However, amendment of the Indian Evidence Act in 2000 has given legal recognition to the digital evidence as admissible before the court. However, this Act does not consider electronic evidence as primary evidence, though it is admissible as evidence before the Court. The digital evidence is considered as the secondary evidence as per the Indian Evidence Act 1872.[1]

The major issue is as secondary evidence it may affect its credibility in court. Primary evidence is considered as more reliable and has more evidentiary value compared to secondary evidence. The classification of digital evidence as secondary evidence could impact on the outcome of cases. Moreover, treating digital evidence as secondary evidence will place an extra burden on the person to establish their claims. In the legal concept, the burden of proof is something which dictates that the party making a claim must provide relevant and sufficient evidence in order to support their claim. While electronic evidence is admissible before the court as per the Evidence Act it needs to be provided with authenticated certificate to make that evidence admissible before the court. Thus, parties need to overcome additional hurdles for establishing the authenticity of the digital records. In order to combat these issues later some changes were made in the new Act called Bhartiya Sakshya Adhiniyam 2023.[2] The Act has treated digital evidence as the primary evidence.

The Act is lacking in sufficient safeguards to prevent tampering or contamination of electronic

[1] The Indian Evidence Act, 1872, s. 65B.
[2] *Bharatiya Sakshya Adhiniyam*, 2023, ss. 2(1)(d), 57, 61, 63, 85.

records during investigations. This will raise questions about the integrity of digital evidence in legal proceedings. The Act requires the need for an expert's certificate to authenticate specific electronic evidence. While this certification is indeed to ensure the accuracy of digital evidence, it may pose a challenge in terms of the ease of producing such evidence in court.[3] Further, electronic evidence is bifurcated as both primary and secondary evidence. This will often create confusion in court proceedings. This confusion could affect while interpreting the digital evidence. This may impact the outcome of the cases.[4]

1.2 Concept and Meaning of Admissibility

The **Black's Law Dictionary**[3] have given a very important definition to admissibility. According to black's law dictionary having the quality, state, or condition of being admitted as evidence in a proceeding or trial is what is meant by the term "admissibility". It can be said that the term "admissible" refers to something that can be legally admitted, accepted, or permitted as evidence, or that is certainly worthy of admission.

For any evidence to be admissible before the court of law, it must be relevant, material and competent. A piece of evidence, which is relevant, must have a reasonable tendency to facilitate proving or disproving a fact. It need not make the fact certain, but it must tend to increase or decrease the likelihood of some fact. Once relevant evidence is admitted by the court after ensuring compliance with the existing rules, the court will determine the appropriate weight to be given to a particular piece of evidence. When a piece of evidence is used to support a fact that is in dispute in a case, it is referred to as material evidence. If a piece of evidence complies with certainestablished standards of dependability, it is deemed "competent". By making them dependent on the weight of the evidence, courts are progressively weakening the competency rules of evidence.[5]

Evidence is either admissible or inadmissible. Admissible evidence is the evidence that complies with all regulatory and statutory requirements, and has been correctly obtained and handled. Admissible evidence is any document, testimony, or tangible evidence used in a court of law. Evidence that has been illegally obtained or altered after it has been obtained by an investigator or examiner is highly unlikely to be admissible in court. Admissibility of a

[3] "Key Changes in the Law of Evidence: Bharatiya Sakshya Adhiniyam 2023," *LawStreet Journal*, available at:https://lawstreet.co/speak-legal/key-changes-in-the-law-of-evidence-bharatiya-sakshya-adhiniyam-2023 (last visited Apr. 29, 2025).
[4] *Ibid.*
[5] M. A. Henry Campbell Black, *Black's LawDictionary* (St. Paul, Minn. West Publishing Co.,6th edn.,1990).

document is one thing and its probative value another, these two aspects cannot be combined. A document may be admissible and may not carry any conviction and weight, or its probative value may be nil.[6] Even though a document might be admissible, the question of whether or not the information it contains has any probative value should still be evaluated in light of the facts of the case. The authenticity of the entries in the official record by an official or person authorized in performance of official duties would depend on whose information such entries stood recorded and what was his source of information. The entry in the school register or the School Leaving Certificate is required to be proven in accordance with the law, and the standard of proof that is required in such cases hasremained the same as that required in any other civil or criminal cases.[7]

1.3 Admissibility of digital evidence in Indian Laws

In India, the admissibility of digital evidence depends on the different laws, and court rulings. The Indian legal system has given legal recognition to digital evidence and such recognition of digital evidence is covered under different laws that include the following:

1.3.1 Evidentiary value of the digital evidence with reference to Bhartiya Sakshya Adhiniyam, 2023

Recent amendments relating to electronic evidence, the admissibility of electronic records as evidence

The Indian Parliament on August 11, 2023, introduced the Bhartiya Sakshya Adhiniyam that replaced the Indian Evidence Act, 1872. The President of India gave their approval on December 5, 2023. The Act has changed many provisions of the Indian Evidence Act and some of the provisions remain the same. For the admissibility of electronic records or digital evidence, the Act has many provisions. The Act has validated the evidentiary value of the digital evidence. Some of the major changes with regard to electronic records are as follows:

Section 2(e) of the Act has provided the legal frameworks for the admissibility of digital evidence. Accordingly, this Section states that evidence includes two forms of evidence. That includes oral evidence and documentary evidence. Oral evidence involves the statements or information provided electronically, by the witnesses in the court, that contributes to the investigation of facts. Such statements are acceptable and it is termed as oral evidence. On the

[6] *State of Bihar* v. *Radha Krishna Singh*, AIR 1983 SC 684.
[7] *Ram Prasad Sharma* v. *State of Bihar*, AIR 1970 SC 326.

other hand, documentary evidence includes documents that are extended to cover electronic or digital records that are presented to court for the examination. The Section thereby covers the electronic evidence orally as well as through documents.[8]

Section 32 of the Act consists of electronic records in reference to the laws of the other country. Whenever a court needs to understand the laws of another country, any statement about such laws is found in a book claiming to be published under the authority of that country's government, including electronic or digital form which is considered as relevant.

The Act has expanded the evidentiary value of electronic or digital evidence, by considering digital evidence as primary evidence. As per the Section 57 of the Act primary evidence refers to actual documents presented for the court's examination. Section 65B of the Indian Evidence Act 1872, digital evidence was considered secondary evidence. Section 63 of the Indian Evidence Act stated the meaning of the Secondary evidence. However, the Act has provided more importance to digital evidence in the legal proceedings by considering the digital evidence as primary evidence. Section 57 of the Act prescribes the provisions for digital evidence as primary evidence.[9] The Section in its explanation part 4 says that, when an electronic or digital record is created or stored, and this storage happens at the same time or one after another in multiple files, each of these files is considered primary evidence. Explanation 5 states that if an electronic or digital record is produced from proper custody and is not disputed, it is also considered as primary evidence. Explanation 6 states that video is simultaneously stored in electronic form and transmitted, broadcast or transferred elsewhere, each of these stored recordings is considered primary evidence. Explanation 7 further extends the concept to situations where an electronic or digital record is stored in various locations within a computer resource, including temporary files. In such cases, each automated storage space is considered primary evidence.[10]

1.3.2 Provisions for Electronic Evidence under the Bhartiya Sakshya Bill

On 11th August 2023, Union Home Minister Amit Shah presented three bills in the Lok Sabha, one of which is the Bhartiya Sakshya Bill. This bill aims to revoke the current Indian Evidence Act, 1872. The Bhartiya Sakshya Bill comprises a total of 167 section, including 23 sections derived from the existing IEA, one completely new section and the removal of five sections.[11]

[8] The Bhartiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 2(e), 32, 57.
[9] *Id.*
[10] *Id.*
[11] Livemint, Bhartiya Sakshya Bill to replace Indian Evidence Act, here' s what may change, mint, August 11, 2023, at pg no. 1.

The bill establishes the admissibility of electronic or digital records as evidence, giving them the consistent legal weight as physical paper documents. Additionally, the bill suggests modifications to 23 sections and encompasses a total of 170 sections. Within the bill, provisions have been made to broaden the range of secondary evidence, including copies produced through mechanical processes, document, counterparts, and oral depiction of the contents of the document.

Electronic or digital recording is admissible under the new Bill. The legal effect, validity and enforceability of such electronic evidence will be same as that of paper or written records. The content sent of the electronic record shall be in accordance with section 59 of the bill. The produced electronic record must be of such a communication device or computer that was used regularly for the purpose of creating, storing, and processing the information. The person using such a device should have lawful control over the device. The information saved on the computer must be fed to an ordinary course of activity. The computer or the device must be in regular use, if not then the accuracy of the contents must not be hampered. The notice to produce such evidence should be delivered by the court to the party who possesses the evidence in electronic form. In case of electronic signature, the subscriber of the signature must prove that the signature is his or hers.

Section 61 takes admission of the electronic or digital record and states that the electronic or the digital record shall have the same legal effect, validity and enforceability as that of paper records. The contents of electronic record shall be in accordance with the provisions of Section 59 proving them by primary evidence.

Section 63[12] states regarding the admissibility of electronic records as any information contained in an electronic record "*which is printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory which is produced by a computer or any communication device or otherwise stored, recorded or copied in any electronic form (hereinafter referred to as the computer output) shall be deemed to also be a document, if the conditions mentions in the section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible."*[13]

"The conditions in respect of a computer output shall be the following, namely:—

[12] The Bhartiya Sakshya Bill, 2023, No. 47, Acts of Parliament, 2023 (India).
[13] The Bhartiya Sakshya Bill, 2023, No. 47, Acts of Parliament, 2023 (India), s. 63.

(a) the computer output containing the information was produced by the computer orcommunication device during the period over which the computer was used regularly to create, store or process information for the purposes of any activity regularly carried on over that period by the person having lawful control over the use of the computer or communication device;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer or communication device was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities."[14]

Any information that is the form of printed paper, stored, recorder or is copied in optical or magnetic media or semiconductor memory produced by a computer shall be deemed to be a document. Such a document shall be admissible as evidence in the court of law without any proof or production of original documents, only if the person or the owner who recorded the evidence gives a certificate under section 63.

The person or the owner issuing a certificate under section 63 must state the following:

1) The working condition of the computer while recording the document
2) The owner is using the computer legally and in ordinary course of time
3) The owner must provide details if other device or computer is also used in the ordinary course of time.
4) Details of each device or computer should be given by the user if multiple devices or computers are used, construing all the devices as a single unit and their description must also be provided.

The same provisions are stated in the Indian Evidence Act, 1872 as well.[15]

1.3.3 Indian Evidence Act, 1872

The Indian Evidence Act, 1872 is one of the foundational legislation that continues to be highly

[14] *The Bhartiya Sakshya Bill, 2023, No. 47, Acts of Parliament, 2023 (India), s. 63(2).*
[15] *The Indian Evidence Act, 1872*, No. 1, *Acts of Parliament*, 1872 (India), s. 65B.

relevant in the Indian legal system. Under this legislation, certain provisions direct how evidence is treated in the court. Initially, the Indian Evidence Act didn't bear direct provisions for the admissibility of digital evidence. Later in the year 2000, an amendment was made to the Indian Evidence Act, accordingly, Section 65B of the Indian Evidence Act, has given legal recognition to digital evidence. Section 65B[16] specifically addresses the admissibility of the electronic records before the court. As per the section, the electronic records include emails, or digital documents or other documents acceptable as evidence in Court. Those documents can be used as evidence in court without having to show the original digital file, subject to some conditions mentioned in the section that needs to be followed. This allows easier use of electronic information as evidence. Section 65B(2) of the Act prescribes the rules that need to be satisfied for the information stored in the computer to be considered valid in legal proceedings:

The information in the electronic record must be produced by the computer during the regular use of that computer for storing or processing information related to ongoing activities.

During this regular use, the kind of information in the electronic record was regularly input into the computer as part of the usual activities.

The computer must have been working correctly during the relevant time, and any issues with its operation should not affect the accuracy of the electronic record.[17]

The information in the electronic record must match the information that is initially fed into the computer during regular activities.

As per Section 65B (4) of the Act, in order to present a statement from the electronic record in court, a certificate can be used. The certificate should be signed by a responsible official who can confirm how the electronic record was produced, provide details about the devices involved, and address the conditions mentioned earlier. In the case of Anver P.V v/s P.K Basheer,[18] the Honorable Supreme Court decided that a certificate under Section 65B(4) of the Indian Evidence Act is essential for admitting electronic evidence. The court emphasized that this certificate ensures the source and authenticity of the electronic record. However, in the case of Shafhi Mohammad vs. State of Himachal Pradesh,[19] the Supreme Court provided a different decision. They said that the certificate requirement under Section 65B (4) of the Indian Evidence Act is not always mandatory. According to this case, the certificate is only

[16] *The Indian Evidence Act, 1872* (Act 1 of 1872), s. 65B.
[17] I*bid.*
[18] *Anver P.V v. P.K Basheer*, (2014) 10 SCC 473; *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
[19] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.

needed when the person presenting the evidence has control over such a device, not when it's the other party.

1.3.4 Information Technology Act, 2000

The Information Technology Act was enacted by the Indian Parliament on June 9, 2000. The main purpose of the Act is to give legal recognition to electronic records and digital signatures which is enumerated under Section 4 and Section 5 of the Act. Digital signatures and electronic records are the forms of digital evidence. Some of major provisions in this Act that relates to electronic evidence are:

a. Section 4 of the Act states that if any law specifies that information or any other thing must be in written, typewritten or printed form, this requirement is still satisfied if the information is presented in electronic form. Additionally, it should be easily accessible and usable for future reference.[20]
b. Section 5 of the Act states the legal recognition of electronic signatures. If any law mandates that information or any other thing requires authentication through a physical signature, a document must bear the signature of a person. This provision overrides such requirements. It asserts that legal criteria for authentication are fulfilled if the information is authenticated through an electronic signature. The explanation part of section 5 states that if a law requires a person's signature on a document, the term 'signed' means putting a handwritten signature or any mark on it. It also means that the term signature is understood in the same way. The provisions make it clear that electronic signatures are considered just as valid as traditional handwritten. However, electronic signatures are valid as long as they follow the specific electronic signature standards set by the central government.
c. Section 79A of the Act which was amended in 2008 states that, it is necessary for the central government to appoint an examiner of electronic evidence. That person's role is to give their expert suggestions on electronic evidence in court or other authorities.[21]

1.3.5 Legal Recognition of Electronic Evidence under IT Act, 2000

The Information Technology Act of 2000 also aims to provide a legal framework in which all electronic records and other activities carried out through electronic Information Systems

[20] *The Information Technology Act, 2000* (Act 21 of 2000), ss. 4, 5, 79A.
[21] *Ibid.*

Control and Audit means are given legal sanctity. According to the Act, an acceptance of a contract may be expressed through electronic communication means and it will have the same legal validity and the ability to be legally enforced, unless the parties have agreed otherwise.

Various sections under the Information Technology Act 2000 deals with the recognition of electronic records, to what extent they can be used and their scope in today's world. Section 4 of the Indian IT Act of 2000 grants legal status to electronic records. Paper-based documents are considered electronic records if they are made available in electronic form and are easily obtainable for future reference.

Section 3 gives legal recognition to electronic records and digital signatures. The digital signature is generated in two steps. The electronic record is firstly, converted into a message digest using a mathematical function known as the "hash function", which digitally locks up the electronic record, ensuring the authenticity of the intended communication that is contained in the electronic record. Any alteration withthe electronic record's contents will instantly render the digital signature invalid.[22]

Secondly, the identity of the person who is affixing the digital signature is uniquely identified by using a private key that attaches itself to the message digest and which can be verified by anyone who possesses the public key pertaining to such a private key. This is how the identity of the person who is affixing the digital signature is established. Anyone will be able to use this information to verify out whether electronic record has been altered or whether it has been preserved in its original state since it was fixed using the digital signature. Additionally, it will make it possible for anyone who possesses a public key to determine who sent the message in the first place.[23]

1.3.6 Banker's Book Evidence Act, 1891

The Banker's Book Evidence Act came into existence in 1891. It was amended in the year 2000. This amendment introduced specific changes that relate to the admissibility of digital records. Subsequently, the Information Technology Act was enacted, and it served as an update to the Banker's Book Evidence Act. The amendment has made significant changes in the banking evidence. Accordingly, Section 2 of the Act states that evidence that is taken from the banker's book as defined under this section is reliable evidence before the legal proceedings.

[22] *The Information Technology Act, 2000* (Act 21 of 2000), ss. 4, 5, 43, 79A, 340.
[23] *Ibid.*

In addition to this, Section 2A speaks about the use of printouts of electronic data that are also considered as evidence before the court. Thereby, amendment was made to this Act that provides legal frameworks for the admissibility of digital evidence in conjunction with banking evidence.[24]

1.3.7 Role of digital evidence in Cyber crime investigation

Cyber crimes are one of the serious issues in India. As technology is growing, some people are misusing it for fraudulent purposes. As per the report of the National Crime Record Bureau (NCRB), As of 2024,[25] India continues to experience a high volume of pending Cyber crime cases, with significant numbers reported in states like Karnataka, Uttar Pradesh, Maharashtra, and Delhi. In recent years, Karnataka has emerged as a hotchpots, registering over 16% of all Cyber crimes in the nation. Delhi, as a union territory, also faces considerable case backlogs, with fraud and identity theft being some of the most common Cyber offences. The majority of the cases fall under computer related offences as per Section 66 of the Information Technology Act. There is a greater importance for the digital evidence to substantiate the facts and to prove these cases. Digital evidence is often linked to electronic crimes like identity theft, Cyber stalking, and credit card fraud. Digital evidence is important in finding Cyber crimes and proving them in court. The use of digital devices assists in uncovering the evidence related to proof of Cyber crimes, data leaks, hacking, and other digital problems.[26]

1.3.8 Significance of Digital Evidence in Protecting the Intellectual Property Rights (IPR)

Intellectual property is gaining prominence in India as a lucrative source of income. In order to prove the ownership of intellectual property, strong evidence is very essential. The infringement may have occurred due to copying, distributing and modifying digital content without the permission of the authorized person. In these situations, the digital evidence helps to execute the facts that validate the originality of a work. It will help to mitigate the unauthorized copying or distribution of such property. Intellectual property is the product of intellect. Property includes literary, artistic, and scientific works, discoveries, performances, phonograms, broadcasts, industrial design, trademarks, service marks, commercial names and designations.[27]

[24] *The Banker's Book Evidence Act, 1891* (Act 18 of 1891), s. 2, s. 2A.
[25] National Crime Records Bureau, “Crime in India 2024” 29 (2024).
[26] *Ibid.*
[27] K.K. Verma, *Intellectual Property Rights: Law and Practice* 215 (Universal Law Publishing, New Delhi, 2nd edn., 2018).

Property rights are confirmed on the basis of the uniqueness of ideas and creation of the mind. It is essential to prospect the rights of the original owner. Digital copies like journals, publications and books are readily available online. In case of infringement of such assets by electronic means, it is very essential to protect such rights through the use of digital evidence. Digital evidence helps to safeguard intellectual property rights in case of infringement of such rights. In this regard metadata, digital fingerprints, digital certificates and watermarks play a very important role that includes:

Metadata will be used to describe other data by encompassing information like creation, date author and software used for a file. Digital fingerprints also serve a major role. It identifies the integrity of a file. Along with it, identical hash values indicate identical files.

Digital certificates are used to verify the identity of a person or any organization. This will help to prove the specific work that is created by that individual or entity.

The watermarks are considered digital marks which are embedded in a file to show ownership of a work. They are commonly applied to various digital media such as images, videos or documents. The primary purpose of watermarks is to identify and protect intellectual property by visibly and invisibly marking the content.[28]

1.3.9 Importance of Digital Evidence in Forensic Investigation

In India, the role of digital evidence in forensic investigation is phenomenal. Forensic investigation commonly involves scientific methods of investigation. The forensic investigation includes taking physical evidence such as fingerprints, DNA, blood stains, or weapons, autopsy, post-mortem reports, and some other evidence. Along with this physical evidence, digital forensics methods also contribute a significant role in forensic investigations. This is particularly important in dealing with the cases where information is stored electronically. The information may be in any form that includes emails, files and history all are accounted for as digital evidence while conducting forensic investigation. However, in India, digital forensic investigation is still developing.

In 2008, a terror attack occurred at Mumbai in India highlighted that the country was still figuring out how to handle and investigate digital crimes. The investigation into the attack was criticized for missing important digital information from the US that warned about the possible terror attack. After this attack, investigators found that digital evidence played a big role in planning and carrying out these terror attacks. In this regard, the Indian government created a

[28] *Ibid.*

report which pointed out that digital devices are very important. The report also highlighted the importance of information satellite phone, Direct Inward Dialing (DID) facilities, GPS equipment and the tracking of emails/IP addresses.[29]

In the Mumbai train bombings of 2006, terrorists used advanced technology. They used things like masking their IP addresses and using proxy services to hide their communications. After these incidents, India became more conscious of the importance of digital evidence in forensic investigation and many concerns are raised on this behalf. They suggested that there is a need to improve Cyber forensics and Cyber security professionals to protect India's information technology from potential harm.

In Bharat Jatav vs. State of Madhya Pradesh (2021)[30] in this case, the Honorable High Court while hearing the matter with regards to grant of bail under Section 439 of the Criminal procedure Code emphasized the importance of technology in forensic science and held that the scope of forensic science extends beyond the DNA reports and blood samples.

1.3.10 Data protection and privacy

Digital evidence can have both positive and negative impacts. Digital evidence is very important for the investigation of Cyber crimes. However, it can also cause threats to people's privacy rights. Such rights are protected under Article 21[31] of the Constitution that states that every individual has the right to life and liberty. The same contention was upheld in Justice K.S Puttaswamy vs. Union of India case.[32]

For instance, digital evidence is like a detective tool that will be used in order to catch online criminals. It has the capacity to track and analyze activities on the internet. However, this can be misused to the rights of the individual. Because tracking their online movement without their permission is a clear way of violation of privacy. Furthermore, digital evidence can go beyond just identifying criminal activities. It has the power to reveal personal information about individuals. During the investigation if this information are not handled properly this may lead to potential harm to one's own privacy. In order to balance these concerns, it is essential to use digital evidence in an ethical manner. The methods used to collect digital evidence must respect the individual privacy rights. There are so many methods to protect the privacy of the person. Using effective methods like encryption, that act like a secret code to

[29] *National Crime Records Bureau*, "Crime in India 2024" 56 (2024).
[30] Bharat Jatav v. State of Madhya Pradesh, 2021 (MPHC) 2, at para. 15.
[31] *The Constitution of India*, art. 21.
[32] **Justice K.S. Puttaswamy (Retd.) v. Union of India**, (2017) 10 SCC 1, at para. 94.

secure data and makes it difficult for unauthorized individuals to access it. There are privacy enhancing technologies such as virtual private networks, block chain technology, and encrypted messaging apps that will inform individuals to control what personal information is collected about them. The implementation of these tools will safeguard the privacy rights and investigation can be carried in an ethical border. [33]

1.3.11 Search, Seizure and Search Authority

The court will admit the digital evidence if the methods used to obtain digital evidence are in line with legal procedures. The challenge arises when digital evidence is obtained without proper authority. If the evidence is obtained without a valid search warrant is also one of the challenges. In such cases, where the procedural requirements stated in the Code of Criminal Procedure[34] or BNSS are not met, the defense has the right to challenge the admissibility of such evidence. If there is a failure to follow the correct protocols like maintaining a properly documented record of evidence handling, it can lead to challenges regarding the reliability of the evidence.

For instance, law enforcement searches a suspect's computer, without following specific guidelines in the CRPC or BNSS or not getting a valid search warrant. It raises a big question about the legality of the search. The defense can take the point that any digital evidence obtained by the unauthorized search, will not be allowed as evidence before the court. The court will closely determine the legitimacy of the search process in order to maintain a fair investigation.[35]

1.4 The major types of digital forensics are as follows:

a. **Database Forensics** - which helps in checking databases for information.
b. **Network Forensics** - used for the understanding of data flow in networks to prevent issues and find out what happened.
c. **Mobile Forensics**- this will help to get information from phones or tablets to solve cases.
d. **Malware Forensics** - which is used for harmful computer viruses to know who made them and what it will cause.

[33] **Ministry of Electronics and Information Technology, "**Report of the Committee on Data Protection Framework for India" at 19 (2018).
[34]**Code of Criminal Procedure,** s. 100
[35] *Ibid.*

e. **Email Forensics -** using emails to check out its source from whom it is sent and confirming the date and contents of the mail.

Memory Forensics - used for checking hidden memories or information from the computers.[36]

WHITE BLACK LEGAL

[36] Dr. V.K. Singh, *Digital Forensics: A Comprehensive Guide* 45 (LexisNexis, 2021).