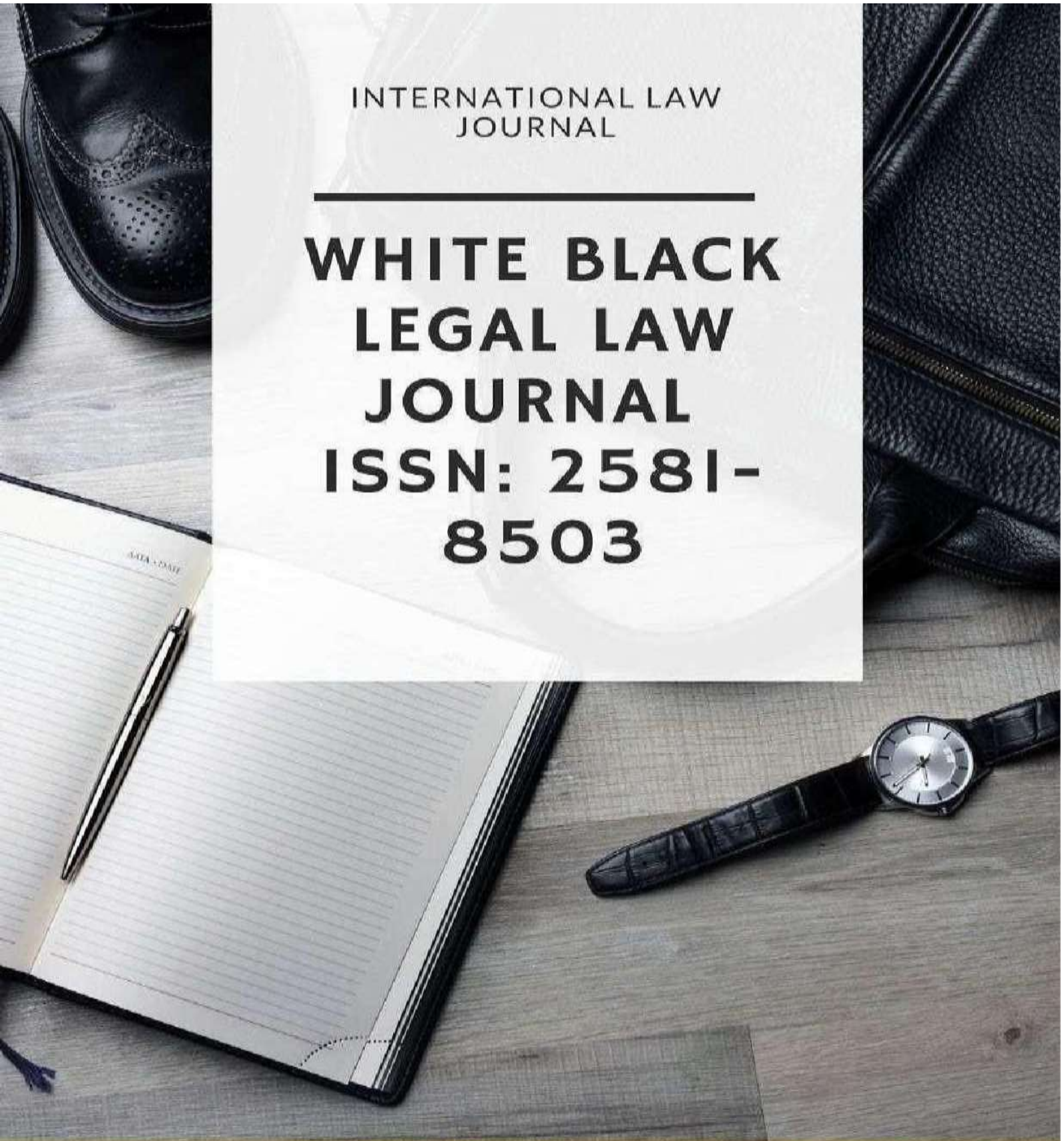




INTERNATIONAL LAW
JOURNAL

**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.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and

a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has successfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal



Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat



Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University. More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.



Subhrajit Chanda



BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

THE BHARATIYA SAKSHYA ADHINIYAM, 2023: A COMPREHENSIVE ANALYSIS OF CHANGES TO ELECTRONIC EVIDENCE

AUTHORED BY - SAMARTH SAXENA

*The rapid advancement of technology has significantly transformed the way evidence is presented and evaluated in courts of law. Under the **Indian Evidence Act, 1872**, provisions for handling electronic evidence were introduced but the rapid development demanded a more robust framework. The introduction of the **Bhartiya Sakshya Adhinyam, 2023** marks a pivotal change in how electronic evidence is treated. This paper examines the key modifications introduced by the 2023 legislation, comparing them to the provisions of the old Indian Evidence Act, and explores how the updated law has adapted to address the complexities of digital records.*

INTRODUCTION

The Bharatiya Sakshya Adhinyam, 2023 (BSA, 2023) marks a significant milestone in Indian jurisprudence, ushering in a new era for the admissibility and probative value of evidence. This comprehensive overhaul of the Indian Evidence Act, coupled with amendments to the Code of Criminal Procedure and Indian Penal Code, aims to modernize the legal framework in the face of rapid technological advancements. The BSA, 2023 has significantly revised the laws governing electronic evidence in India which will have far-reaching implications for the Indian judiciary and the administration of justice.

A basic perusal of BSA, 2023 would point out that a paradigm shift has been made in the concept of electronic evidence by changing the nature and mode of proof of such electronic evidence.

DEFINITION OF TERM DOCUMENT

One of the first changes which have been brought out is in the definition of the word ‘document’. In the Indian Evidence Act, 1872 the word ‘document’ was not defined to include the electronic record.

It is important to note that the definition of 'document' was not even amended in the year 2000 when the Information Technology Act was enacted. What was changed was the definition of the word 'evidence' to include the electronic record but the definition of 'document' per se was not changed. But the BSA, 2023 specifically amends the word document to include electronic and digital records.

Electronic and digital record

Under Indian evidence act only the word electronic record was used but section 2(1)(d) of BSA, 2023 deliberately includes both the terms 'electronic' and 'digital records,' emphasizing that these two terms are not synonymous and each carries a distinct meaning. Both these words have been joint by use of a conjunctive word "and". This choice indicates a clear intent to differentiate between the two concepts. Justice G.P.Singh observes "*The word 'or' is normally disjunctive and 'and' is normally conjunctive but at times they are read as vice versa to give effect to the manifest intention of the Legislature as disclosed from the context. As stated by SCRUTTON L.J.: "You do sometimes read 'or' as 'and' in a statute. But you do not do it unless you are obliged because 'or' does not generally mean 'and' and 'and' does not generally mean 'or'".*". Thus the conscious usage of conjunctive word 'and' denotes that these two words are two different concepts. No attempt has been made to define the words 'electronic record' and 'digital record' under the BSA, 2003. Even Information Technology Act, 2000 also only defines electronic records.

Digital records are, broadly speaking, either digital copies of physical documents or materials that were originally created in a digital format. This could be a scanned paper form or a word document created by a computer. Conversely, electronic records are those that are created and kept solely within computer systems. These are typically created by the system or entered by the user from databases or other electronic systems. One type of electronic proof is emails.

EXPERT EVIDENCE

Next, Section 45 of the Indian Evidence Act, 1972 deals with expert evidence. Under BSA, 2023 the section has been renumbered as section 39. The change that has been incorporated is that earlier what was section 45A which pertained to examination of an electronic record has now been subsumed in section 39(2). No material changes have been incorporated in the BSA, 2023.

PRIMARY AND SECONDARY EVIDENCE

The Indian Evidence Act had three categories of evidence - oral evidence (ss. 59 and 60), documentary evidence (ss. 61- 65) and electronic evidence (65A and 65B) and modes of proving these were different from one another.

In Navjot Sandhu, a division bench of the Supreme Court took the view that secondary evidence of electronic records could be covered under Sections 63 and 65 of the Indian Evidence Act and can be proved in the same manner as the secondary evidence. Then came a series of judgements, and the law was finally settled by the Hon'ble Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & others. by holding that sections 65-A and 65-B are code in themselves and electronic evidence can only be proved under these sections. It was also held that the electronic records are a class in themselves and they cannot be proved as primary or secondary evidence.

Primary Evidence

The inclusion of electronic records in definition of document under BSA, 2023 has major consequences when we study chapter V of BSA, 2023 dealing with Documentary Evidence. Section 56 of BSA, 2023 which is pari materia with section 61 of Indian Evidence Act, 1872 provides that the contents of documents may be proved by primary or secondary evidence. Under BSA, 2023 documents includes electronic records thus by virtue of action 56 of BSA, 2023 the contents of electronic records may also be proved by primary or secondary evidence which was not permitted earlier.

Now, a major conceptual change has been brought in the BSA, 2023. Earlier Section 62 of the Indian Evidence Act provided definition of primary evidence and included only documents. It is pertinent to remember that the definition of 'document' did not include electronic records under the Act of 1872 and thus electronic records were neither impliedly nor expressly included in the definition of primary evidence. Under the BSA, 2023 section 62 has been renumbered as section 57. Section 57 of BSA, 2023, still defines primary evidence. But now that the definition of 'document' in Section 2 of BSA has been expanded to include electronic and digital records, consequential amendments have been made by introducing explanations 4 to 7 in the definition of primary evidence. Under section 57 of BSA, 2023 original electronic or digital records which are produced for inspection of the court are defined as primary evidence. Explanation 4 to

Section 57, says when the electronic or digital record is stored simultaneously in multiple files each file is a piece of primary evidence. For example, if I click a picture on my phone, it would also get saved in my Google Drive (if granted permission). This explanation says that not only what my mobile records is primary evidence what is being recorded in the cloud storage is also primary evidence. Under Indian Evidence Act, 1872 such electronic records and simultaneous storage were not covered as primary evidence.

Explanation 5 to section 57 of BSA, 2023 provides that when an electronic record is produced from proper custody, it is primary evidence unless it is disputed. Example if I have footage on my mobile and present it in court, the court will treat it as primary evidence, as it comes from proper custody—since I am the owner of the mobile. This reflects the concept of proper custody, meaning the evidence originates from the person who lawfully possesses the device. However, if I take my wife's mobile and attempt to present footage from it, that evidence would not be considered to come from proper custody because my wife is the rightful owner of the device. As a result, in such a case, the electronic record would no longer qualify as primary evidence. Therefore, the explanation 5 is very important. It must be from proper custody. And if it is disputed that it is not a proper custody, the burden will lie on the person who says that it is not a proper custody. It's a reverse burden of proof.

Explanation 6 is similar to explanation 4 and provides that when the video recording is being simultaneously stored and transmitted, broadcast or transferred to another device then each of the stored recordings is a primary unit. For example, if I record something on my mobile and transmit it to my friend's phone. Explanation 6 says, that even my friend's mobile will be primary evidence because it is a video recording that has been transferred and transmitted to another device and each of the stored recordings is primary evidence.

Explanation 7 is a further extension and provides when an electronic record is stored in multiple storage spaces in a computer resource, each of such automated storage including a temporary file is primary evidence. In simple terms, when you store something on your computer or device, the document or file is often saved in multiple places within the device automatically. For example, if you're typing on a laptop and it suddenly shuts down, when you restart it, you might find the file still available with a prompt asking if you want to save it. One may wonder where this file was saved, since you didn't save it yourself. In this case, it was stored in the RAM. This automatic saving happens without your intentional action, which is why it's

referred to as *automated storage*. This concept is reflected in Explanation 7, as it refers to storage that occurs without the user's direct involvement. Explanation 7 says that this temporary file is also primary evidence as the main file on the window platform so they both have the same status. In copyright suits this evidence becomes crucial as to files stored on RAM can be proved to prove once originality.

Special Provisions as to evidence relating to electronic records

Section 61 of the Adhiniyam of 2023 provides that electronic or digital record shall have the same legal effect, validity and enforceability as paper records, subject to satisfaction of the condition referred in section 63 of the Adhiniyam of 2023. There is no corresponding section for section 61 in the Evidence Act, 1872.

The BSA, 2023 firstly expands the scope of primary evidence to bring a device at par with actual paper and section 61 further reinforces this position by saying that nothing in this adhenium shall apply to deny the admissibility of an electronic record for being an electronic record so one cannot discriminate against the electronic evidence and treat it as a paper document.

Now after incorporating electronic records into definition of primary evidence one could come to an inference that earlier 65A and 65B would lose its relevance. However earlier 65A and 65 B make their reappearance in the form of Section 62 and 63 in the Adhiniyam. Section 62 of the adhiniyam is *pari materia* to section 65-A of the Indian Evidence Act 1872.

Section 63 begins with the word, notwithstanding anything contained in this adhiniyam, exactly the same word that the Honorable Supreme Court in the case of Arjun Pandit Rao used to give an overriding effect to 65-B over other sections dealing with documentary evidence.

Now if we have a closer look at the scheme of the adhiniyam we will find that section 61 which says that admissibility of electronic or digital record will not be denied only on the ground that it is an electronic or digital record is subjected to conditions imposed in section 63 of the adhiniyam which starts with a non obstante clause- 'notwithstanding anything contained in this adhiniyam'. Thus it can be fairly concluded that section 61 makes every electronic record admissible in evidence but such record will have to satisfy the conditions of section 63 (hitherto 65B of the Indian Evidence Act) to have any legal effect.

Section 63 of the Adhiniyam has undergone some changes. Sub-section 1 provides that any computer output shall be deemed to be also a document if the conditions mentioned in the section are satisfied and such output shall be admissible in any proceedings without further proof or production of the original. The definition of computer output has been expanded to include “*semiconductor memory*” and the means of producing the output has also been expanded to include “*any communication device or otherwise stored recorded or copied in any electronic form.*”. With the inclusion of electronic records under the scope of primary evidence, Section 63 now allows computer-generated outputs to be admissible as evidence in a manner similar to secondary evidence. Just as certain conditions must be fulfilled for the admission of secondary evidence, similar mandatory conditions have been laid down for accepting computer outputs as valid evidence. Introduction of communication device is important as it would include anything from mobile phones to satellite phones or any other mode which could be developed in future.

Subsection 2 of section 63 prescribes conditions that have to be fulfilled before any computer output can be admissible are exactly same as mentioned in section 65-B of the Indian Evidence Act, 1872.

Further the requirement of certificate under section 65-B of the Indian Evidence Act which has been held to be mandatory has been retained under sub-section 4 of section 63 of the Adhiniyam.

Now with these changes the law under BSA, 2023 recognises electronic records as primary evidence which was not the case under Indian Evidence Act and any computer output if satisfies the conditions mentioned in section 63 will also be admissible. This is another form of one can say, secondary evidence of electronic records. To illustrate suppose a photograph is taken from a phone then to prove the contents of electronic record that mobile phone itself will be a primary evidence and if that photograph is printed and submitted as evidence then subject to conditions mentioned in section 63 such photograph will also be admissible in evidence,

Secondary Evidence

Section 63 of the Indian Evidence Act, which isn't directly about electronic evidence, has been updated with a new provision. This change will likely impact how electronic records are proven in court. Section 58 of the Adhiniyam (earlier section 63) provides a clause viii which provides

that any skilled person who has examined the document (including electronic records) can give secondary evidence of such document. Thus if any expert who has examined an electronic record his evidence about contents of such electronic record will be admissible as secondary evidence. Although such evidence about electronic records will be subjected to conditions mentioned in section 60 of the Adhiniyam.

One of the fronts on which the BSA, 2023 has disappointed is the context of manipulation of electronic evidence. With introduction of Artificial intelligence and deep fake there are high chances of a complex form of tampering with electronic evidence. The Adhiniyam does not do anything to curb that. A basic example of such tampering could be following -Suppose if there is a letter written by Mr. A 20 years back it is not easy to tamper because one can immediately note the interpolation and if tampered evidence is being filed as secondary evidence then one has to prove first that the original is missing. But suppose if there is an email written to me by my friend I can immediately edit the contents of the email. And if I take a printout of this email, that would be admissible under section 63 as under that section there is no condition precedent that original must be proved to be lost before filing computer output as evidence.

Challenges and Future Prospects: Deepfakes, AI, and Blockchain Evidence

There is a tall building with twenty-five floors. Yesterday, I went to the fifth floor to meet a friend and called my sister, but she didn't come that day. Today, she came, yet I was on the tenth floor. This small incident reflects what has happened with the replacement of the old Evidence Act by the time the law reached one stage of development, technology had already moved several floors ahead.

The inclusion and modernization of provisions relating to electronic evidence under the Bharatiya Sakshya Adhiniyam (BSA), 2023 was long overdue. In today's digital era, it is not merely a matter of necessity but of survival. With the advent of Artificial Intelligence, the challenges have multiplied from deepfakes to blockchain-based data and AI-generated records the very nature of truth and proof is being redefined.

It is rightly said that *"the wars of the future will not be fought with weapons, but with information."* Today's world may no longer rely on guns and bombs, but it faces battles of a different kind fought through biomedical data breaches, cyber manipulation, and algorithmic deceit. The law must therefore rise to this new battleground with foresight and technological

wisdom.

In the present digital age, appearances can no longer be taken at face value. The advent of *deepfakes* artificially created yet strikingly realistic videos and images has blurred the distinction between authenticity and deception. Whether in the form of fabricated political statements or deceptive identity scams, these AI-generated imitations have begun to erode public faith and destabilize social and legal institutions worldwide. Confronting and exposing such technological manipulations has become a vital task for investigators, media professionals, cybersecurity experts, and forensic scientists, as the preservation of truth and credibility lies at the heart of justice and societal trust.

The rapid advancement of artificial intelligence (AI) has given rise to a new wave of synthetic media, widely known as deepfakes. These are highly realistic images, audio, and videos generated using sophisticated AI techniques such as Generative Adversarial Networks (GANs)¹ and Diffusion Models (DMs)². While offering unprecedented creative possibilities, these technologies have also raised substantial ethical and security concerns, posing risks in domains such as entertainment, politics, and cybersecurity. Deepfakes are often indistinguishable from authentic media, which has led to their misuse in spreading misinformation, impersonation, and other malicious activities. Recent advancements in deepfake technology have enabled highly realistic synthetic media, leading to a surge in fraud cases.³

While the Bharatiya Sakshya Adhiniyam, 2023 represents a commendable step toward modernization, it still falls short of addressing the intricate realities of digital crime. The inclusion of electronic and digital records within the definition of “document” undoubtedly broadens the scope of admissible evidence, but it does not guarantee *traceability* that is, the ability to verify the true origin, integrity, and chain of custody of such evidence. The Adhiniyam prescribes procedural safeguards such as certification under Section 63, yet it remains largely silent on *how* the authenticity of tamper-prone digital data can be scientifically

¹ Goodfellow I., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A., Bengio Y. Generative Adversarial Nets. *Adv. Neural Inf. Process. Syst.* 2014;27.

² Ho J., Jain A., Abbeel P. Denoising Diffusion Probabilistic Models. *Adv. Neural Inf. Process. Syst.* 2020;33:6840–6851.

³ Amerini, I., Barni, M., Battiato, S., Bestagini, P., Boato, G., & Bruni, V. et al. “Deepfake Media Forensics: Status and Future Challenges.” *Journal of Imaging*, vol. 11, no. 3 (2025): 73. doi: 10.3390/jimaging11030073.

established in real time.

Unlike traditional documents, an electronic record can be duplicated, altered, or fabricated within seconds, leaving minimal visible trace. Deepfakes, metadata manipulation, and synthetic voice or image generation challenge the very foundation of evidentiary reliability. The critical question therefore arises: even if an electronic record is admissible, can it truly be traced back to its original and unaltered source? The current legal framework provides recognition but not the technological infrastructure or forensic standards necessary to ensure that recognition translates into reliability.

Thus, while the BSA, 2023 has opened the doors for digital evidence, it has yet to build the corridors of verification through which truth can securely pass. Without robust digital audit trails, cryptographic validation, and standardized forensic protocols, the promise of technological inclusion risks being reduced to procedural symbolism rather than substantive justice.

Ethical Concerns and Governance in Deepfake Detection

The emergence of deepfake detection technology marks a crucial advancement in the preservation of digital integrity, yet it simultaneously presents complex ethical and legal challenges. Among these, privacy remains the most immediate concern. The effectiveness of deepfake detection depends heavily on the analysis of facial structures, voice signatures, and other biometric identifiers forms of data that are inherently personal and sensitive. The storage, transmission, and analysis of such biometric information pose significant privacy risks, particularly in cases of unauthorized access or misuse. Paradoxically, while these tools are designed to protect individuals from deception, they also expose them to the risk of biometric surveillance, identity theft, and breaches of personal autonomy.

Beyond privacy, the problem of disinformation presents a deeper moral dilemma. Deepfakes, through their ability to craft highly realistic yet false narratives, have already demonstrated their potential to distort public discourse and manipulate democratic processes. Even with advanced detection technologies, false content can spread faster than it can be verified, eroding public trust in digital communication. Moreover, an unsettling paradox exists each improvement in detection technology fuels the creation of more sophisticated deepfakes, as malicious actors adapt and evolve, exploiting algorithmic vulnerabilities. This escalating

digital arms race undermines the very foundation of authenticity in media and threatens the credibility of information ecosystems.

In the context of Indian evidentiary law, the Indian Evidence Act, 1872 offered no framework to address such ethical or technological dilemmas. It was conceived in an era where digital manipulation was inconceivable. The Bharatiya Sakshya Adhiniyam, 2023, however, has begun to bridge this gap by recognizing *electronic and digital records* as admissible documents and by setting procedural standards for their verification under Sections 61 to 63. Yet, the Adhiniyam still falls short of addressing the *ethical dimension*—it does not lay down specific principles governing the collection, verification, or protection of biometric and digital data used in forensic detection. Without explicit legislative guidance, the admissibility of AI-generated or AI-analyzed evidence may lead to questions of privacy violation, consent, and reliability.

To mitigate these concerns, the BSA, 2023 could evolve further by incorporating ethical governance standards similar to those found in international privacy regimes such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These frameworks emphasize informed consent, data minimization, and the right to erasure principles that could safeguard individuals whose biometric data are analyzed for deepfake detection. The law could also mandate independent oversight bodies or accredited digital forensic authorities to ensure accountability, prevent misuse, and maintain transparency in the forensic process.

Projects such as FF4LL (Forensics for Lifelong Learning) have underscored the need for robust and interpretable AI models those that not only detect synthetic media but can explain *how* conclusions are reached. Such *explainable AI (XAI)* frameworks are vital in a legal setting, where the probative value of digital evidence depends not merely on accuracy but on traceability and fairness. If the spirit of the BSA, 2023 is to modernize the evidentiary process, it must extend beyond procedural inclusion to encompass ethical and technological accountability.

Ultimately, while deepfake detection technology is indispensable in preserving the authenticity of digital communication, its deployment must be guided by a balanced framework of ethics, privacy, and legal oversight. The future of digital evidence law in India will depend not only on recognizing new forms of data but also on ensuring that truth, technology, and human rights

remain harmoniously aligned.

Comparative Study of Evidentiary Flexibility in India, the UK, US, and Canada

The evolution of evidentiary law across jurisdictions reveals a common struggle, the need to reconcile technological progress with the enduring principles of fairness, authenticity, and reliability. While each legal system retains its distinctive procedural philosophy, a comparative analysis shows that the flexibility and responsiveness of evidence law directly determine how effectively justice systems adapt to the digital age.

India: From Rigidity to Recognition

India's journey, from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023, epitomizes a legal transformation shaped by necessity rather than foresight. The colonial-era Evidence Act was drafted in a world of paper, signatures, and witnesses not pixels, algorithms, or metadata. The 2023 Adhiniyam, by incorporating "electronic and digital records" within the definition of "documents," signifies a long-awaited acknowledgment of technological realities. Yet, the Indian framework remains procedurally stringent but technologically incomplete.

The BSA retains the certificate requirement (earlier Section 65B, now Section 63), which though essential for authenticity often becomes a barrier in cases involving foreign servers, dynamic data, or AI-generated evidence. Unlike common law jurisdictions that rely more on judicial discretion and contextual evaluation, India's system still favors codified admissibility over interpretative flexibility. The result is a framework that recognizes electronic evidence but does not yet fully trust it.

United Kingdom: Judicial Pragmatism and Technological Adaptability

The United Kingdom, as the cradle of the common law tradition, has demonstrated remarkable adaptability in integrating technology within evidentiary practice. Under the Police and Criminal Evidence Act (PACE) 1984⁴ and subsequent reforms, the British approach emphasizes *judicial discretion* and *procedural fairness* rather than rigid statutory formalities. The Civil Evidence Act 1995⁵ abolished the hearsay rule in civil proceedings and embraced

⁴ Police and Criminal Evidence Act 1984 (UK).

⁵ Civil Evidence Act 1995 (UK).

electronic records as admissible, provided their authenticity and reliability can be reasonably established.

British courts rely on the principle of “best evidence available” meaning the court may admit electronic evidence if the source and integrity can be demonstrated, even without a rigid certification requirement. The judiciary’s confidence in expert testimony, coupled with an evolving understanding of digital forensics, has allowed the UK to maintain flexibility while ensuring reliability. This model places trust in judicial competence and technological literacy, enabling a pragmatic equilibrium between innovation and integrity.

United States: Technology through Constitutionalism

In the United States, the Federal Rules of Evidence (FRE)⁶ provide one of the most dynamic and adaptive models for digital admissibility. Rules 901 and 902 lay down broad standards for authentication and self-authentication of electronic evidence. American courts have recognized email chains, server logs, social media posts, and even blockchain records as admissible, provided a reasonable foundation for authenticity is established.

Crucially, the U.S. approach is constitutional in spirit and evidentiary in substance. The Fourth Amendment’s privacy protections and the Due Process Clause create a moral boundary around data collection and surveillance. This ensures that while courts are technologically accommodating, they remain ethically grounded. The flexibility of the FRE anchored in precedent rather than prescriptive procedure makes the American model one of functional adaptability, balancing innovation with individual rights.

Canada: A Balance between Statutory Precision and Judicial Innovation

Canada’s approach to digital evidence is both methodical and progressive. The Canada Evidence Act⁷, supplemented by judicial pronouncements such as *R. v. Oland*⁸ and *R. v. Cole*⁹, underscores two fundamental criteria: integrity of the electronic system and reliability of the process. Canadian courts require proof that the electronic system was operating properly at the relevant time and that the information retrieved has not been altered.

⁶ Federal Rules of Evidence, Rules 901–902 (United States, 2019 edn).

⁷ Canada Evidence Act, R.S.C., 1985, c. C-5.

⁸ *R. v. Oland*, 2017 SCC 17, [2017] 1 S.C.R. 250 (Canada).

⁹ *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34 (Canada).

However, Canadian jurisprudence is also marked by contextual flexibility the recognition that the degree of proof must correspond to the nature of the evidence. Courts have shown a willingness to admit metadata, CCTV footage, and server-based evidence where procedural authenticity aligns with practical necessity. Canada's legal system exemplifies a *hybrid model* anchored in statutory rigor but open to judicial innovation a balance that India's emerging evidentiary framework could learn from.

Cross-Jurisdictional Reflections

A comparative reflection reveals that India's Bharatiya Sakshya Adhiniyam, 2023 is a much-needed leap forward, but its success will depend on how effectively it learns from these global experiences. The UK demonstrates the power of judicial pragmatism; the US showcases constitutional flexibility; Canada balances statutory rigor with contextual fairness; and Singapore exemplifies technological foresight.

For India to achieve comparable evidentiary flexibility, the BSA, 2023 must evolve into a living instrument supported by digital forensic standards, blockchain-enabled traceability, and judicial training in cyber evidence. The ultimate test of a modern evidence law is not how it defines documents, but how it defines *trust* in a world where truth itself can be manufactured. As Lord Denning once observed, "*Law must keep time with the march of modern progress. It must change and adapt to the new society which is emerging.*" The true measure of the Bharatiya Sakshya Adhiniyam will be whether it can keep pace not merely with technology, but with truth itself.

CONCLUSION

In conclusion, the Bhartiya Sakshya Adhiniyam, 2023 represents a substantial shift in the legal treatment of electronic evidence, addressing the limitations of the Indian Evidence Act, 1872 in an era of rapidly evolving technology. By expanding the definition of "document" to include both electronic and digital records, and by setting viiiclear conditions for the admissibility of computer-generated outputs, the new law aligns more closely with modern technological realities. It enhances the legal framework by recognizing electronic records as primary evidence, subject to specific conditions for validity. However, while the changes provide greater clarity and adaptability, the Adhiniyam leaves certain concerns, such as the potential for manipulation of digital evidence, insufficiently addressed. Overall, the Bhartiya Sakshya

Adhiniyam, 2023 modernizes India's evidence law to meet the demands of the digital age, but continued adaptation may be required to fully tackle emerging challenges, such as AI-driven manipulation of electronic records.

The journey of evidence law from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 reflects India's gradual but determined attempt to keep pace with technological transformation. Yet, as this paper demonstrates, the law still stands at a critical intersection where *technological possibility* outpaces *legal adaptability*. The inclusion of electronic and digital records within the evidentiary framework is undoubtedly a progressive milestone, but the deeper challenge lies in ensuring that such evidence remains *authentic*, *traceable*, and *ethically governed*.

The rise of deepfakes, AI-generated records, and blockchain-based media represents a paradigm shift in how truth is created, manipulated, and perceived. Technology today can manufacture not just words, but realities — capable of rewriting history, fabricating identities, and distorting justice. This evolving digital ecosystem demands that our legal system move beyond procedural recognition to embrace a more technologically literate and ethically grounded jurisprudence.

For the Bharatiya Sakshya Adhiniyam, 2023 to realize its transformative promise, it must be supported by a robust framework of digital forensic infrastructure, judicial training, and data governance policies. The establishment of accredited forensic laboratories standardized digital audit protocols, and blockchain-based evidentiary trails can help ensure the reliability of digital records. Equally vital is the introduction of ethical guidelines to regulate the use of biometric data, AI-driven analytics, and deepfake detection tools. Law, technology, and ethics must converge if justice is to retain its moral and factual sanctity in the digital era.

Ultimately, the future of evidentiary law will not be determined merely by legislative reform but by how effectively the judiciary, investigators, and technologists collaborate to uphold truth in a world of algorithmic deception. The evolution of the Bharatiya Sakshya Adhiniyam must therefore continue not as a static document, but as a living framework responsive to emerging digital realities.

A comparative glance at jurisdictions such as the United Kingdom, the United States, Canada,

and Singapore reveals that the strength of modern evidence law lies in its *flexibility and foresight*. While these systems emphasize authenticity and procedural integrity, they also empower the judiciary to interpret technology with contextual sensitivity. India's Bharatiya Sakshya Adhiniyam, 2023 has taken a crucial first step toward this global standard, but it must continue to evolve as a living statute one that not only accommodates technological change but anticipates it. By integrating global best practices in digital forensics, judicial training, and ethical governance, India can transform its evidentiary framework into one that is both technologically robust and jurisprudentially progressive.

As the philosopher Søren Kierkegaard once observed, *"Life can only be understood backwards, but it must be lived forwards."* The same holds true for law. By learning from the limitations of the past and anticipating the challenges of tomorrow, the Indian legal system can ensure that in this age of artificial intelligence, truth remains human, and justice remains real.

