Writer's Pocket

PERSPECTIVES ON JUSTICE

ESSAYS IN CRIMINAL LAW

EDITOR IN CHIEF
Prof. Dr. Anil G. Variath
Professor and Dean,
Amrita International School of Law, Amrita Vishwa Vidyapeetham, Coimbatore

SENIOR EDITOR
Dr. Vinod Kumar
Associate Professor,
Amity Law School,
Amity University Rajasthan, Jaipur

EDITORS
Dr. Kunal Rohira
Associate Professor,
School of Legal Studies and Governance, Career Point University, Kota

Dr. Abhijay Chakraborty
Assistant Professor,
Amity Law School, Amity University Rajasthan, Jaipur

First published by Writer's Pocket in 2026

email: editor@writerspocket.com

Cover Design by Pooja Wadiya

ISBN-13: 978-93-7248-021-4

www.writerspocket.com

FOREWARD

Prof. (Dr.) Lalit Kumar Deb
Member, Odisha State Law Commission
Formerly Professor, Maharashtra National Law University, Mumbai
& Behrampur University, Odisha

I am happy to learn about the publication of this significant and timely volume on the evolving landscape of criminal law. At a moment when India is witnessing a historic transition in its criminal justice framework, this book serves as a valuable scholarly contribution that reflects both the urgency and the depth required to understand such transformative shifts.

The journey of criminal law reform in India has been shaped by a long-standing reliance on colonial-era statutes laws crafted primarily for administrative control rather than for securing justice in a democratic society. The recent move toward decolonising these foundational legal texts marks a decisive step toward aligning the justice system with constitutional values, societal realities, and contemporary challenges. Against this backdrop, this book offers an insightful examination of criminal behaviour, legal developments, and the broader socio-legal forces that influence crime and justice.

What distinguishes this work is its interdisciplinary and forward-looking approach. It not only analyses historical foundations and emerging doctrines but also addresses pressing issues posed by technological advancements, globalization, and new categories of crime. Equally important, the book underscores the interplay between criminal law and human rights, offering a balanced view of the rights of the accused, the needs of victims, and the role of institutions in delivering justice.

The editors and contributors have also thoughtfully identified new and emerging areas that merit deeper exploration, such as crimes

legal lens, tracing its historical roots, analyzing its evolution, and exploring the multifaceted nature of crime in a maturing democracy. By engaging with classical and contemporary theories of criminal behaviour from biological and psychological models to sociological and economic explanations it offers a comprehensive understanding of why individuals commit crimes and how societies respond to wrongdoing.

Further, this book evaluates the strengths and limitations of emerging regimes of criminal law, highlighting how human rights norms and institutions can serve both as safeguards for the accused and as avenues of relief for victims. In doing so, it underscores the ongoing tension between enforcing the law and ensuring fairness, between protecting society and protecting individual liberties. The chapters also delve into pressing issues such as policy reforms, technological challenges, and the expanding scope of criminal liability, while identifying areas for future research and doctrinal development.

Designed for students, scholars, practitioners, and policymakers, each chapter is enriched with pedagogical features discussion questions, curated web links, and pathways for deeper inquiry to encourage learning both within and beyond the classroom. As India stands at the threshold of a newly envisioned criminal justice landscape, this book seeks to contribute to the discourse by providing clarity, context, and critical insights.

As the Editor in Chief, I am deeply indebted to each and every scholar who has supported us and contributed their valuable chapters to this book. While it is not possible to individually name everyone who has played a role in shaping this work, I would be failing in my responsibility if I did not acknowledge the remarkable dedication and unwavering efforts of my Co-editors, Dr. Vinod Kumar, Dr. Kunal Rohira and Dr. Abhijay Chakraborty. Their commitment to nurturing the idea, refining its vision, and tirelessly working to bring

this book to fruition has been instrumental in transforming a concept into reality. I also extend my sincere thanks to the publisher for their consistent support, guidance, and professionalism, which have been crucial in ensuring that this volume reaches its readers in its finest form.

My sincere appreciation also goes to the readers, whose curiosity, engagement, and commitment to understanding the evolving dimensions of criminal law give genuine purpose to this work. If there are any suggestions for improvement or areas that deserve deeper exploration in future editions, I warmly welcome such feedback. Through shared dialogue, constructive reflection, and collective inquiry, scholarship continues to grow, adapt, and remain relevant.

- **Prof. (Dr.) Anil G. Variath**

CONTENTS

Chapter 12

The Role of Digital Evidence: In Culminating Crimes in Cyberspace

- L.Keerthana

Abstract:

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."

- Newton Lee

In the 19th century, people were connected to various online platforms relating to commerce, communication, education, entertainment, social mobility, etc. The original goal of the Internet's development was to improve and promote human society. But it can also be applied negatively. At first, the crime took place by physical threats or danger to property of humans and their belongings, etc. But, after the evolution of the computer era, crimes started occurring through online platforms without the actual knowledge of the victims and users. When in the physical form of a crime, the identification of the offender or wrongdoer can easily be made by the victim or parties who see the crime that takes place. But it's non-viable to identify the criminal on online platforms, he who was protected under the veil of different network connections or hacking knowledge. He can easily escape from its liability. Due to the constant growth of cybercrimes, Indian legislators planned to prevent and safeguard the interests of common people by introducing the Information Technology Act, 2000, and amending it in 2008 by adding the validity of electronic evidence and e-transactions of online users. After this amendment, we are visibly able to catch the criminals, frauds, and hackers controlling the anonymity of netizens, cyber bullying, etc. In this paper, we are going to discuss the vital role of digital evidence and how it's helpful

to identify the wrongdoer and punish them before the appropriate court of law.

Keywords: *Cyberspace, Crimes, Technology, Digital, Evidence, Data Privacy.*

Introduction:

The rapid advancement of technology has dramatically transformed the way we communicate, conduct business, and interact with the world around us. However, a new type of criminal activity is known as "cybercrimes" has also emerged as a result of this digital revolution. From the early days of hacking and virus propagation to the rise of sophisticated cyber-attacks targeting individuals, businesses, and even governments, cybercrimes have evolved alongside technological innovations.

As these crimes have grown in complexity and scope, traditional methods of investigation have become less effective, necessitating the integration of digital evidence into modern forensic practices. The Digital evidence become indeed in technology era. Generally, it comprised of electronic data such as emails, server logs, digital footprints, and even metadata, etc., has become a cornerstone in the fight against cybercrime. It plays a pivotal role in identifying perpetrators, tracing criminal activity, and securing convictions. With cybercrimes often leaving little physical trace, digital evidence provides a vital link between the criminal act and its perpetrator, offering investigators the tools necessary to navigate the intricacies of the digital world. As the methods and tactics of cybercriminals continue to evolve, so too must the techniques used to gather, preserve, and present digital evidence in the pursuit of justice.

Evolution of cyber law:

In 19th century, the UK government has introduced laws for the implementation to monitor cybercrime - The Computer Fraud and Abuse Act of 1986 was the first cyber law and subsequently the computer misuse act 1990also enacted to protect computer related crimes and to prevent (prohibits) unauthorized access to computers as well as the misuse of digital data. In India, cybercrimes are governed by the Information Technology Act of 20003 and the Indian Penal Code of 1860. The legislation that deals with issues related to online crime and internet trading is the Information Technology Act of 2000. However, a term and penalty for cybercrime were added to the Act in 2008. The Reserve Bank of India Act and the Indian Penal Code 1860 were also amended. Evidence Act, 1872 (Amendment) 2000 were made a drastic change in the history of cybercrimes, this evidence act give special provisions to as to evidence relating to e- records and admissibility of electronic records. S.2(1)(t) of Information technology Act 2000 defined about *"Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;* The Information Technology Act's stipulates that it is forbidden to produce or distribute any electronic content that depicts youngsters acting in a sexually explicit manner, anonymity, restriction of pornographic content in e – platforms, penal provisions for offence against women and children's, identity theft,, cheating by personation., etc. After the introduction of IT act 2000, it mainly focused on the protection and promotion of e-commerce, digital transactions, validation of electronic signature and e- contracts. But the rapid growth of crimes starts blooming just because of developments in the field of online commercialization. This paved way for many fraudulent transactions, theft, misappropriation of money, personalized cheating and terrorist used the internet platform to escape from his liability. In E-platform is so hard to identify the wrongdoer, synchronous of multiple network and lack of security

issues. To avoid this major threat, Ministry of information technology has introduced the amended bill on 2008. It was drafted with penal provisions and liability of the wrongdoer is clearly mention.

Recent Developments: IT Rules 2021

The Indian Parliament introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, focusing on regulation of social media, digital media oversight, and enhanced cyber security measures to ensure ethical standards and data protection[363].

Digital Evidence:

The Indian Evidence Act recognizes references to records, documents, and entries in books of account as evidence. Under IEA, 1872 (new Bharatiya Sakshya Adhiniyam act, 2023) defines the *S. 2(e) "evidence" means and includes all the statements including statement given electronically which the court permits or requires to be made before it by witness in relation to matters of fact under enquiry and such statement are called oral evidence, subsequently all documents including electronic or digital records produced for the inspection of the court such documents are called documentary evidence.*

The Act has been amended through the second schedule to the Information Technology Act to include electronic records in supporting documentation. The new act BHARATIYA SAKSHYA ADHINIYAM S. 61 deals with e- records which is subject to section 63 of BSA, 2023 (Sections 65A is replaced with 62 of BSA, 2023 and 65B of evidence act, 1872 replaced with S. 63 of BSA, 2023) which provide accurate computer output with the same evidentiary

[363] https://lawbhoomi.com/evolution-of-cyber-law-in-india/

value as the original without requiring further evidence or creation. The Indian Penal Code includes offenses for various documents and records. Handling digital evidence requires preliminary statements, detailed information about computer hardware, operating systems, software, topography, users, passwords, manuals, and physical evidence.

Need Of Digital Evidence

Digital evidence play a vital role in uphold the rights of common public by culminating the cyber - crimes. Because of the rapidity at which technology is developing, many crimes on e-platforms are also growing at a quick pace. Indeed to identification of criminals and to prevent them from doing this. The need for digital evidence has grown significantly with the rise of digital technology and cyber activity. Here's a breakdown of why digital evidence is important. especially in legal, security, and business contexts.

1. Especially in Crime Investigation –

Hacking, identity theft, fraud, and phishing leave digital footprints. Traditional Crimes: Even in cases like homicide or burglary. suspects may leave clues via texts, calls, GPS, or social media. Digital Forensics: Tools and techniques can recover deleted data. track activity logs, or link devices to criminal acts.

2. Legal Proceedings

Courts increasingly accept digital evidence, like emails, CCTV footage, or phone records, as admissible. It provides objective and time stamped proof that can support or refute testimonies.

3. Workplace and Corporate Use

Employee misconduct, IP theft, data breaches, and compliance issues often require investigation using digital logs and communications. Companies need it for internal audits and defending themselves during litigation.

4. National Security and Law Enforcement

Surveillance and intelligence gathering depend heavily on digital evidence to prevent or respond to threats. Tracking communications, analyzing devices, or examining online behavior are all key.

5. Civil Disputes like Divorce, custody battles, or harassment claims may involve texts, emails, or social media as evidence.

6. Regulatory Compliance

Industries like finance, healthcare, education institutions and corporate sectors are required to maintain digital records for audits and legal requirements.

Importance Of Admissibility Of Digital Evidence:

Through the Amendment Act of 2000 to the Indian Evidence Act, 1872, the Indian judicial system integrated technology into its processes in response to the internet revolution. The object of the change was to add sections 65A and 65B[364] *(S. 62& 63 of BSA, 2023)* to the act while maintaining the concerns about the reliability of electronic records and guaranteeing their flexibility in courtrooms. Since then, there has been much debate over the admission of electronic evidence in Indian courts, with the prevalent ambiguity in the laws incorporated therein being one of the main causes. A number of significant issues about the admissibility of electronic

[364] Indian Evidence (Amendment) Act, 2000, Act No. 45 of 2000 § 65A, 65B (2000).

evidence have been raised by its designation as a supplementary category of admissible evidence in court. Whether Section 65B is required for the admissibility of electronic evidence is one important question. One important question is whether Section 65B is required for electronic evidence to be admissible, and if so, when the certificate should ideally be produced. Furthermore, there is still uncertainty regarding the reliability of the evidence and the suitability of various approaches in both criminal and civil situations[365].

Facilitating the use of electronic evidence in court proceedings is the aim of these act. Additionally, they are an exemption to the best evidence rule, which normally calls for the original document to be produced as primary evidence. Section 65B (4) does not, however, specifically address the certificate's evidentiary value, whether meeting the requirements outlined in subsection (2) is required, or when it should be presented. The Supreme Court has made an effort to elucidate the legislative intent underlying these laws through a number of rulings. It has been established as a history of considering a certificate following any of the three conditions mentioned in Section 65B (4) to hold more weight than oral or documentary evidence.In 2005[366], the court ruled that printouts of phone records could be considered admissible evidence even without a certificate under Section 65B (4). However, this judgment was later overruled in the case of *Anvar P. v. P. K. Basheer*[367]. In the latter case, The Hon'ble Court ruled in the latter case that Section 65B is a comprehensive code and that evidence from any other source would not be accepted. It underlined that a certificate under Section 65B (4) is required and that the Indian Evidence Act prohibits the use of oral testimony to prove an electronic record. The Supreme Court in *Mohammed Ajmal Mohammad Amir Kasab v State of Maharashtra*

---

[365] Astha Jain, Faculty of Law, Jagran Lakecity University, Bhopal (M.P.).
[366] State (NCT of Delhi) v. Navjot Sandhu, 2005 SCC 16 208
[367] Anvar P. v. P. K. Basheer & Ors., (2015) 10 SCC 473.

& Ors[368]. Acknowledged the use of electronic evidence such as CCTV footage, mobile devices, memory cards, data storage devices, and IP addresses.

The Honourable Supreme Court ruled in Tukaram S. Dighole v. Manikrao Shivaji Kokate that the "standard of proof" for electronic evidence has to be "more accurate and stringent" than that of conventional documentary evidence. After reevaluating the certificate requirement in 2017, the court determined that certifications under Section 65B(4) are merely a "mode of proof." Consequently, failing to produce a certificate at an earlier time can be seen as a fixable flaw. Another 2018 ruling, which held that the need for a certificate is procedural rather than mandatory, further reinforced this point of view. It can be relaxed in some instances, such as when a party does not have control of the original device. Section 65B is therefore not regarded as a comprehensive code.

Upon analyzing these judgments and the associated contradictions, it becomes evident that there is a gap in the interpretation of the law. The case of *Arjun Panditrao Khotkar v. Kailash Kishanrao* addressed and resolved these contradictions comprehensively. The court examined that Section 65B of evidence act have operates independently of the rest of the Indian Evidence Act.

Over the years, various cases such as *Navjot Sandhu*, *P. Anvar* and *Shafhi Mohammad*[369] have attempted to address the ambiguity surrounding these provisions. However, due to the differing circumstances and related factors in each case, there was no unified stance on these issues. As a result, the legal landscape remained unclear, and doubts persisted.

---

[368] [2012] 8 S.C.R. 295

[369] Navjot Sandhu, 2005, Anvar P., 2015, Shafhi Mohammad, 2018.

Interpretation Of Section 65b (4)

In distinguishing between primary and secondary evidence, the court highlighted that the original information contained within a computer is considered as primary evidence. Copies derived from it, on the other hand, are inherently secondary evidence. The court also clarified that the phrase "any of the conditions" in Section 65B (4) should be interpreted as "all." Therefore, since an electronic record, as mentioned in subsection (1), is considered secondary evidence, the requirement of a certificate in accordance is mandatory.

In cases such as *Shafhi Mohammad*, where the parties involved do not have first-hand possession of the data and are unable to obtain a certificate, the said court provided some relaxation.[14] It stated that an application must be presented to the judge to seek relaxation of the mandatory requirement under Section 65B (4). However, the subsequent judgment in *Arjun Panditrao* overruled this decision. It held that the portion of Section 349 of the Criminal Procedure Code (CrPC) stating "...who are not in possession of an electronic device" is entirely incorrect. The court clarified that an application can always be made to a judge for the production of such a certificate from the relevant person under Section 65B (4), even if the person refuses to provide it at the first instance.

Core Areas: Focus On Digital Evidence.

These rulings raise important issues about how Section 65B should be used, whether to submit a certificate (immediately or later in court), how to prove it in court, and what should be included in the certificate. In fact, these questions are addressed in the Arjun Panditrao Kotkar case. It makes it clear that only when presenting electronic evidence as secondary evidence is a certificate required. The submission of a certificate is not necessary if the original electronic record which functions as main evidence is presented. By attesting that they are the owner or operator of the device where the

information is initially saved, the owner of the computer, tablet, or cell phone can immediately present the original electronic record as evidence[370].

Perspective Of Digital Evidence Varies From Civil & Criminal Cases

In interpreting Section 65B, the court also distinguishes between the use of certificates in criminal and civil cases. When a demand is made to the relevant authority in a civil matter and no certificate is supplied, the judge presiding over the trial should summon the person or people in question and demand that they produce the required certificate. This occurs when an electronic document is used as proof without the necessary certification. The trial judge has the ultimate discretion in these situations.

Electronic evidence must be provided no later than prior to the start of the trial, in accordance with Section 65B(4) read with Sections 207, 91, and 311 of the Criminal Procedure Code (CrPC). However, the court has the authority to allow the filing of electronic evidence later, before the trial is over. However, in accordance with Section 65B's requirements, CDs, VCDs, chips, and other comparable storage media must be accompanied by a certificate that was acquired at the time the document was taken. The secondary evidence pertaining to that electronic record is no longer admissible in the absence of such a certificate.

As technology develops, the Indian legal system must remain adaptive and flexible, using electronic evidence while upholding the principles of justice and equity in its courts. This ruling sets a precedent that will continue to influence and direct the admissibility

[370] https://articles.manupatra.com/article-details/ADMISSIBILITY-OF-ELECTRONIC-EVIDENCE-UNDER-THE-INDIAN-EVIDENCE-ACT-1872

of electronic evidence in Indian courts for many years to come, making it a lighthouse for the future.

Challenges In The Collection And Preservation Of Digital Evidence

1. **Volatility of Digital Evidence:**
   Digital data is highly volatile - it can be easily altered, deleted, or overwritten, especially in live systems. Temporary data like RAM contents or cache files may be lost if not captured immediately[371].

2. **Problems with the Chain of Custody:**
   Evidence must have a continuous, documented chain of custody in order to be admitted into evidence. Evidence may be contested or omitted if there is a failure to keep track of who accessed or handled the data.

3. **Password protection and encryption[372]:**
   To keep incriminating files from being accessed, suspects frequently employ encryption, hard passwords, or hidden partitions. It is practically impossible to recover this data without the right decryption tools or authorized access.

4. **Barriers to Jurisdiction:**
   Because cybercrimes frequently transcend national boundaries, gathering evidence kept in foreign jurisdictions can be challenging. Different privacy and data access rules might make international cooperation more difficult.

---

[371] https://vidizmo.ai/blog/handling-digital-evidence
[372] Noland, Alec (2024) "Current Challenges of Digital Forensics," Themis: Research Journal of Justice Studies and Forensic Science: Vol. 12: Iss. 1, Article 1. DOI: https://doi.org/10.55917/2324-6561.1120, https://scholarworks.sjsu.edu/themis/vol12/iss1/1

5. **Large Sums of Information and Insufficient Standardization:**
   To locate pertinent evidence, investigators must sort through enormous volumes of data, including emails, logs, films, and backups. Significant effort, technical resources, and experience are needed for this. There isn't a single, accepted rule for gathering, storing, or presenting digital evidence in court. Inconsistent results from various equipment and techniques can cast doubt on their authenticity.

6. **Anti-Forensic and Tampering Methods:**
   Anti-forensics tools can be used by suspects to conceal, alter, or remove data, making it more challenging to piece together the original evidence. Even after seizure, evidence can be destroyed using malware or remote wiping programs.

7. **Legal and Ethical Concerns:**
   Privacy laws and civil liberties must be balanced against the need to access data. Overstepping can lead to lawsuits or evidence being dismissed for violating rights[373]. Data stored in the cloud or on third-party servers may be difficult to access without cooperation from service providers. Dynamic and decentralized storage models complicate data retrieval.

Conclusion

Generally speaking the digital evidence does not have a statistical data that it may prevent or prohibits cyber-crimes. But it act as a tool to identify crimes and its background of technologies involved can be easily exposed. The ability to analyze and preserve this evidence is crucial for the successful culmination of cybercrimes in the digital age. However, the complexity of digital evidence presents significant challenges in terms of legal, technical, and ethical

[373] https://globalcybersecuritynetwork.com/blog/benefits-and-challenges-of-digital-forensics/

considerations. Ensuring the authenticity, integrity, and admissibility of digital evidence is critical, and therefore requires robust protocols and collaboration between law enforcement agencies, cybersecurity experts, and legal professionals.

Furthermore, the global nature of cyberspace necessitates international cooperation to address cybercrimes effectively. As cybercriminals often operate across borders, the role of digital evidence extends beyond local jurisdictions, requiring a harmonized approach to legal frameworks and investigative processes. Ultimately, the evolving landscape of cyberspace demands that digital evidence continues to evolve as well. With advancements in artificial intelligence, machine learning, and encryption technologies, the ability to leverage digital evidence in a timely and efficient manner will remain a cornerstone of cyber security and criminal justice in the 21st century.

References:

1. LawBhoomi. (n.d.). *Evolution of cyber law in India*.
2. *Indian Evidence (Amendment) Act*, Act No. 45 of 2000, §§ 65A, 65B (2000).
3. Jain, A. (n.d.). Faculty of Law, Jagran Lakecity University, Bhopal (M.P.).
4. *State (NCT of Delhi) v. Navjot Sandhu*, 2005 SCC (Cri) 16, 208.
5. *Anvar P.V. v. P.K. Basheer & Ors.*, (2015) 10 SCC 473.
6. *State of Maharashtra v. Praful B. Desai*, 8 S.C.R. 295.
7. *State (NCT of Delhi) v. Navjot Sandhu*, 2005 SCC (Cri) 16; *Anvar P.V. v. P.K. Basheer*, (2015) 10 SCC 473; *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 5 SCC 311.
8. Manupatra. (n.d.). *Admissibility of electronic evidence under the Indian Evidence Act, 1872*.
9. Vidizmo. (n.d.). *Handling digital evidence*.

10. Noland, A. (2024). Current challenges of digital forensics. *Themis: Research Journal of Justice Studies and Forensic Science, 12*(1), Article 1.
11. Global Cybersecurity Network. (n.d.). *Benefits and challenges of digital forensics*.

Prof. (Dr.) Anil G. Variath is a highly accomplished legal academic and institutional leader, currently serving as the Professor and Dean of the Amrita International School of Law at Amrita Vishwa Vidyapeetham, Coimbatore, India.

Dr. Vinod Kumar is working as Associate Professor in Law at Amity Law School, Amity University Rajasthan, Jaipur. He has done his B.Com., M.A. (Public Administration), M.Phil., LL.B. and Ph.D. from Panjab University, Chandigarh.

Dr. Kunal Rohira is an Associate Professor at School of Legal Studies and Governance, Career Point University, Kota He completed his LL.B. from University of Kota, LL.M. from the Department of Law, University of Rajasthan and Ph.D. from Career Point University, Kota.

Dr. Abhijay Chakraborty is an Assistant Professor at Amity Law School, Amity University Rajasthan Jaipur. He holds Ph.D., LL.M., and B.A. LL.B. degrees, and has qualified the UGC-NET and SET examinations in law.

Writer's Pocket

www.writerspocket.com

MRP: Rs. 650/-

ISBN 978-93-7248-021-4

9 789372 480214