International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Forensics in Cyber Crime Investigations: Legal and Procedural Dimensions

By: Rituporna Das[1], Dr. Jyoti Yadav[2]

[1]Student, LLM in Cyber Laws and Cyber Securities, Amity Law School, Amity University Lucknow Campus
[2]Assistant Professor, Amity Law School, Amity University Lucknow Campus

Abstract
Digital Forensics has become an indispensable tool in contemporary cybercrime investigations, which ensures systematic identification, collection, preservation, and presentation of electronic evidence in a legally admissible manner. As cybercrimes continue to escalate, investigative authorities are required to operate across multiple digital domains, including personal devices, mobile platforms, cloud infrastructures, and transnational communication networks, with strict adherence to the law. Digital forensics is important not only because it can recover the deleted or concealed data, but also because it ensures that the evidence remains authentic and untouched throughout the investigation. Due to its dual emphasis on both technology and law, it effectively bridges the gap between technical accuracy and legal accountability.
Despite being so advanced in the contemporary world, the field of digital forensics still faces persistent challenges. The extensive reliance on data encryption, rapid technological innovations, and the issue of complex jurisdiction in cross-border investigations complicate and hamper the effective use of digital forensics. Moreover, the escalation of data generated in the digital age raises concerns about privacy, transparency, and the timely administration of justice. Addressing these concerns requires some advanced and well-developed standardized forensic frameworks, legal protocols, and greater international cooperation to harmonize investigative procedures.
This paper shall dwell upon the continuous evolution of the role of digital forensics in cybercrimes in the contemporary world. It shall particularly focus on the foundations, challenges, evidentiary value, and implications for law enforcement and global cybersecurity. It shall also emphasize the strengthening of digital forensics so that harmonious international relations and global cybersecurity can be achieved.

Keywords: Digital Forensics, Cybercrimes, investigations, international relations, data protection

1. INTRODUCTION

The constant evolution in the arena of ICT[3] has restructured the thought process of people, leading to a redefinition of the landscape of crimes in society at large. As the accessibility of digital devices and networks increases, it becomes directly proportional to the opportunities for cybercriminals to exploit the

[1] Student, LLM in Cyber Laws and Cyber Securities, Amity Law School, Amity University Lucknow Campus
[2] Assistant Professor, Amity Law School, Amity University Lucknow Campus
[3] Information and Communications Technology

vulnerabilities. The earlier conventional crimes are seen to have acquired a new digital dimension, unleashing an entirely new species of offences such as cyberbullying, ransomware, identity theft, etc. This is the space where Digital Forensics comes into play. During the prosecution of such cases, Digital forensics works in conjunction with the criminal procedural and the evidentiary law.

Digital forensics encompasses the process of identification, collection, preservation, analysis, and presentation of the information that has been stored electronically, that too in such a manner as to justify the authenticity and reliability of the evidentiary value of the ESI[4].

Digital forensics is the spine of contemporary cybercrime investigations due to its effective and accurate nature. There has been a continuous evolution in the legal framework of cybercrime all over the world, with a strong urge to balance the ultimate need for thorough and exhaustive investigation, along with the basic concerns of the public, such as protection and strengthening of privacy rights, individual rights, and identity, as well as due process. The Budapest Convention[5] on Cybercrime is known for setting a foundation for penalising these offences by setting up and establishing comprehensive standards to investigate, cooperate, and influence the legal framework internationally. The domestic legal framework for cybercrimes and cyberspace possesses different qualities and challenges. The Information Technology Act, 2000 and necessary amendments to the Criminal Acts and the latest reforms in the BNS[6] and BSA[7] have provided a legal and evidentiary value to the electronic devices by underlining the standards for admissibility and the major importance of the approved and certified forensic protocols. The landmark judgement in the case of Anvar P.V. v. P.K. Basheer[8], showcases the strict and uptight procedures for admission of electronic evidence, along with proving its role in determining the investigation's chance of success. The US, on the other hand, has blended the Constitution with the specific sectoral laws such as the CFAA[9] and ECPA[10] which requires numerous steps such as putting up of legal warrants, a strong and efficient chain of custody, and tech literacy for handling the digital evidence better. China, too seems to excel at maintaining a balance the rapid advancement of technology, strong regulations, while and the establishment of new standards for handling and managing digital evidence, while putting privacy and transparent procedures as priorities.

Even after so much amelioration in the world, the judicial systems continue to put up and struggle with the issues of cross-border digital evidence collection, international legal assistance, enforcement of technology laws, certifying proper digital forensics labs for checking the authenticity of the digital records, and eradicating the risk of evidence tampering. As time passes, cybercrimes are getting worse, and even the judicial systems all around the world find it difficult to address them and create stronger laws that would support the best international practices to cover the loopholes in the policies and bridge the gap between the technology and the law.

Digital Forensics in itself is a very specific area within the forensic science arena, which intends to focus on identifying, analysing, recovering, and presenting the electronic evidence. It is more or less a

[4] Electronically Stored Evidence
[5] Convention on Cybercrime (Budapest Convention), Council of Europe, ETS No. 185, opened for signature November 23, 2001.
[6] Bharatiya Nyaya Sanhita, 2023
[7] Bharatiya Sakshya Adhiniyam, 2023
[8] Sandra Jini Saju, Anvar P.V v. P.K. Basheer & Ors (2014 10 SCC 473)
[9] Computer Fraud and Abuse Act, 18 U.S.C. Sec 1030 (1986).
[10] *Electronic Communications Privacy Act of 1986*, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. sec. 2510 et seq.).

convergence of law, technology, and the urgent need to put a judicial scrutiny over the digital evidence. Digital forensics covers the domains of computers, mobiles, networks, databases, and cloud forensics. Digital Forensics not only helps in the reconstruction of the modus operandi of cybercrimes but also ensures the proper preservation of evidence, along with maintaining its authenticity and integrity during admissibility.

Despite of being so important, the amalgamation of digital forensics and criminal investigations is seen to be fraught with numerous legal and procedural obscurities. Digital evidence is susceptible to tampering, alteration, and poses challenges in setting up jurisdiction across the geographical borders, which have declared the conventional evidentiary doctrines incapable of dealing with the contemporary world. In the case of Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[11] it was held by the judiciary that the digital evidence has numerous inconsistencies in its own application.

Internationally, this challenge is being dealt with in various ways by different nations. As such as the United States has a strong established legal framework, which constitutes of the Federal Rules of Evidence and the statute as the Computer Fraud and Abuse Act, 1986; on the other hand, the United Kingdom has laid a strong emphasis on the balance of the procedures and privacy known as procedural proportionality using the Police and Criminal Evidence Act, 1984 and the Computer Misuse Act, 1990; and finally China can be seen as a strong state controlled, and has a modern techno legal approach towards the integration of digital evidence in the investigations using its famous Cybersecurtiy Law (2017) and Data Security Law (2021). All of these different models from different nations follow different legal principles relating to privacy, state controlled surveillance and th admissibility of the digital evidences.

Thus this paper dwells upon the comparative legal analysis of the digital forensics in legal system between India, the United States, the United Kingdom and China. It aims at analyzing the investigative efficiency of the digital forensics with respect to constitutional and human rights.

REVIEW OF LITERATURE

The contemporary world has seen the growth of digital forensics with legal admissibility at a very high pace. The following review of literature mentions and speaks about the famous academic papers, judicial interpretations, to identify and understand how digital forensics has been conceptualised, interpreted and is being operated in India and abroad.

- **B.R. Sharma (2020),** stated that digital forensics are here to transform the entire process of the criminal justice system, as it would shift the focus from conventional crimes to digital crimes. He also mentioned that the problems of recovering the data using forensic science would always be a challenge to prove its admissibility and authenticity in court.[12]
- **Vivek Dubey (2021),** mentions the Indian legal institutions do not have uniform digital evidence collecting and managing protocols which is responsible for the weak cyber crime investigations.[13] He emphasizes on the necessity for forensic capacity building along with transnational cooperation for betterment of the Indian cyber judicial system.
- **Elizabeth Johnson (2021) ,** compares the evidentiary laws of United Kingdom and United States and concluded that there must be a flexible judicial vigilance that has to be paired with the digital forensic

[11] Arjun Pandirao Khotkar v. Kailash Kushanrao Gorantyal, Civil Appeals 20825-20826 of 2017
[12] B. R. Sharma, *Forensic Science in Criminal Investigation and Trials*, 6th edn, Universal Law Publishing, 2020.
[13] Vivek Dubey, *Cyber Crime and Digital Evidence: Legal Issues*, LexisNexis, 2021.

standards to gather better procedural integrity and transparency in the judicial proceedings.[14] She also supports the BSA of India as it aims that strike balance between judicial pragmatism and digital forensics.

- **T. Ramachandran (2023),** Clearly states the issue of the chain of custody problem in the Indian investigation system as it tends to form a bitter sweet coordination between the Police Department and the forensic laboratories he also proposed a unified national digital evidence management protocol under I4 C must be adopted to manage the digital evidences and strengthen the digital forensics in India.[15]
- **UNODC'S Global Programme on Cyber Crime** It lead an emphasis on the uniform procedural safeguards which must be used to prevent the digital evidence is from getting manipulated it also advises the member states to integrate a strong forensic authentication tool and maintain a strict auditing system to to preserve the evidentiary value of the digital evidence.

2. CONCEPT AND SCOPE OF DIGITAL FORENSICS

2.1.Digital Forensics

Digital Forensics is referred to as a special scientific discipline that is responsible for the identification, preservation, examination, and presentation of the evidence which are stored or transferred or transmitted digitally. It also plays a pivotal role in the reconstruction of the scenarios which took place during the criminal computing environment, and to do that in a manner that is works consistently with the laws of evidence and the due process of law.[16] Digital Forensics as a specific discipline was provided recognition in the late 1980s, when the world was struck with a new era of crimes that were being committed entirely using computer networks and systems.[17] In the modern day world, digital forensics are seen to have covered a large number of activities, which include thorough analysis of mobile devices, computer systems, digital networks, and various cloud computing systems. Along with providing assistance in the civil matters, investigations in the intellectual property, corporate audits and several cyber crimes which shows its all inclusive reach in the investigations.

Stages of Digital Forensic Investigation

The process of Digital Forensic Investigation involves 4 major stages:

1. **Identification:** Digital Forensics is very helpful in identifying potential sources of the crime committed using computer systems, mobile phones, drives, or network logs, and also provides a better understanding of collecting the evidence without tampering or contaminating the evidence.[18]
2. **Preservation:** After Identification, the next step is of preservation, which has to be done in a scientific manner. This does include creation of copies bit by bit, verification by hashes, and documentation of the chain of custody log.

[14] Elizabeth Johnson, "Procedural Integrity in Digital Forensics: Comparative Legal Perspectives," *Computer Law & Security Review*, Vol. 47 (2021).
[15] T. Ramachandran, "Cross-Border Access to Electronic Evidence: India's Legal Challenges," *Indian Journal of Law and Policy Review*, Vol. 11 (2023).
[16] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Elsevier, 3rd edn, 2011) 5.
[17] Brian Carrier, *File System Forensic Analysis* (Addison-Wesley, 2005) 3.
[18] National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response* (Special Publication 800-86, 2006) 9.

3. **Analysis:** The experts in this field who examine and preserve the data to reconstruct the actions of the user, recovery of deleted files, identification of the malware or even tracing online communications. There are few tools which are available to automate the entire process.
4. **Presentation:** In the end the observation of the analysis are compiled into detailed comprehensive report for the people with lesser technical knowledge which includes judges, lawyers and juries in a case. And this report is presented alongside evidence law governing the expert evidence.[19]

2.2.Characteristics and Relevance of Digital Forensics

The Digital Forensics consists of intangible, easily alterable, and highly replicable which is quite the opposite of conventional physical evidence. Even though the copied data might appear identical to the original, even a minor change in the data can compromise the authenticity of the data collected.[20] Thus, the investigators must be able to put cryptographic hashes to demonstrate that the evidence to be presented in court is similar to that which is collected generally at the crime scene. Another issue with the data is its volatility as some data only exists temporarily either in RAM or network caches, and ceases to exist when the device is turned off. Collection of this kind of volatile evidence requires specialized tools and action in a second. The digital data is often vast and confusing as it consists of a large volume and diversity, which ultimately blurs the boundaries between the relevant and non-relevant material (private). Thus, the courts insisted on setting up a proportionality between the search, seizure, which would ensure the investigation does not hamper the rights related to privacy.[21]

Digital forensics do play an important role in identifying and proving offences like hacking, phishing, identity theft, cyber defamation, and cyber terrorism. The logs and Meta data can be used to establish the mens rea and actus reus which are essential components to conviction. It also is used in cases of financial fraud where starting from the origin of unauthorized transactions to the reconstruction of communication trails between the planners and the victims.[22] The Indian subcontinent uses, digital forensics to investigate the cases being reported to the Central Bureau of Investigation (CBI) and the National Cyber Crime Reporting Portal. The importance of scientific handling of digital evidence was reemphasized in the case of NCT Delhi v. Navjot Sandhu popularly known as (Parliament Attack Case)[23] and for specifying the evidentiary procedure, the decision was made in Anvar P.V. v. P.K. Basheer.[24]

Digital forensics is at the intersection of law, computer science, and criminal procedure. The investigation is not just about strong recovery techniques but is also about understanding the constitutional rights, admissibility of evidence, and strong data protection laws.[25] Thus, being interdisciplinary, it creates a huge friction between the investigation methods and legal norms, which leads to a tension that still recurs throughout the comparative jurisdictions.

Therefore, Digital Forensics is far more than just being a technical pursuit instead, it is regulated legal mechanism that is central to the contemporary criminal justice. Thus it focuses on creating a balance between the investigation mechanism and legal propriety.

[19] V. Dahiya, 'Admissibility of Electronic Evidence in India' (2019) 61(2) *Journal of the Indian Law Institute* 278, 282.
[20] P. Duquenoy, 'Integrity of Digital Evidence' (2017) 33 *Computer Law & Security Review* 35.
[21] *Riley v. California*, 573 U.S. 373 (2014).
[22] R. Agarwal, 'Role of Digital Forensics in Cybercrime Investigation' (2020) 12(4) *Indian Journal of Law and Technology* 155, 159.
[23] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
[24] Anvar P.V v. P.K. Basheer & Ors (2014 10 SCC 473)
[25] A. Sharma, 'The Interdisciplinary Challenges of Digital Forensics' (2021) 8 *NUJS Law Review* 43.

3. LEGAL FRAMEWORK GOVERNING DIGITAL FORENSICS IN INDIA

The contemporary world is heavily dependent on the digital economy which unknowingly has become a vulnerability to numerous cyber crimes which involves data breaches, online frauds, cyber stalking, and hacking etc. And thus the investigation heavily depends upon the digital forensics, which serves as the milestone for the evidence collection in the cyber law domain. But the India's legal infrastructure is still fragmented as some of the statutes look after electronic evidences, but there is no single framework to govern collection, preservation, and admissibility of the digital evidences.

The legislation that govern digital forensics includes the Information Technology Act, 2000, Indian Evidence Act 1872 replaced by Bharatiya Sakshya Adhiniyam ,2023, Code of Criminal Procedure, 1973 replaced by Bharatiya Nagrik Suraksha Sanhita (BNSS),2023 and Indian Penal Code,1860 replaced by Bharatiya Nyaya Sanhita (BNS),2023. The judicial interpretation of these laws are seen to play as a very strong role in shaping the standards of the Digital Forensics uses in India.

3.1.The Information Technology Act, 2000

The Information Technology Act 2000 is the first cyber legislation enacted for India. It provides the base for the recognition of electronic records and digital signatures And also defines and states penalties for the cyber offences. It criminalises various forms of cyber crimes which include unauthorised access data tampering theft of identity and cyber frauds using computer systems, computer networks and computer resources.

The IT Act 2000 defines electronic records as "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche."[26]

This act also empowers the central government to notify the examiner of electronic evidence by stating "The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence."[27]

This provision was added by 2008 amendment to ensure digital evidence is examined only by the authorised people such as experts which would ultimately lead to enhancing the reliability and procedural transparency.

Even after these provisions, The IT act still does not provide any proper detailed guidelines on how to collect and preserve digital forensic instead it focuses on the criminal offences their liability and the procedural aspect to its connection with general law.

3.2.Bhartiya Sakshya Adhiniyam, 2023

Earlier the admissibility of electronic evidence was primarily governed by section 65 A and 65 b of Indian Evidence Act but now it is being Governed section 61 2 section 63 of BSA. Sec 61 states "Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63, have the same legal effect, validity and enforceability as other document."[28] Which means No evidence shall be denied just because it is in an electronic or digital form. Where as section 63 mentions:

1. Notwithstanding anything contained in this Adhiniyam, 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

[26] The Information Technology Act, 2000 (Act 21 of 2000), s. 2(1)(t)
[27] The Information Technology Act, 2000 (Act 21 of 2000), s. 79A
[28] The Bharatiya Sakshya Adhiniyam, 2023, s. 61

copied in any electronic form (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this 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.

2. The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:---

- the computer output containing the information was produced by the computer or communication device during the period over which the computer or Communication device 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;
- 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 or Communication device in the ordinary course of the said activities;
- 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
- the information contained in the electronic record reproduces or is derived from such information fed into the computer or Communication device in the ordinary course of the said activities.

3. Where over any period, the function of creating, storing or processing information for the purposes of any activity regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by means of one or more computers or communication device, whether--

- in standalone mode; or
- on a computer system; or
- on a computer network; or
- on a computer resource enabling information creation or providing information processing and storage; or
- through an intermediary,

all the computers or communication devices used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer or communication device; and references in this section to a computer or communication device shall be construed accordingly

4**.** In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely:--

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer or a communication device referred to in clauses (a) to (e) of sub-section (3);

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert shall be evidence of any matter stated in

the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule.
(5) For the purposes of this section,---
(a) information shall be taken to be supplied to a computer or communication device if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
(b) a computer output shall be taken to have been produced by a computer or communication device whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment or by other electronic means as referred to in clauses (a) to (e) of sub-section (3).”[29] Which Include manner outlines the admissibility of digital forensics in Indian courts. It also specifies the specific conditions for any digital/electronic record for being treated as valid legal documents. And that document can be directly used as the evidence in court without the need to present the actual original document.
The BSA focuses on substantive authenticity of the electronic evidence with the alignment of legal procedure also it has modernised India's evidentiary law bye eradicating unnecessary hurdles and preserving reliability and credibility of the digital forensic evidence during judicial proceedings.

3.3.Code of Criminal Procedure, 1973 replaced by Bharitiya Nagrik Suraksha Adhiniyam, 2023

The BNSS, 2023 works as the spine 4 investigation in cyber crime cases and supports India's criminal justice system. The BNSS is very similar to its predecessor but has introduced newer provisions which are more connected to rapid technological advancements. It has provisions like section 94, 95 100 and 185, which empower the executive and the judiciary to summon for documents issue search warrants, And seized property which includes computers digital media and various digital devices which can be relevant in an inquiry. Even after many updates the bss still fails that providing an exhaustive procedural legal framework to govern digital searches, data imaging, search and preservation of volatile electronic evidence or protection of clouds stored data. The Supreme Court of India in the case of Shafi Mohammad versus State of Himachal Pradesh[30] held that the certificates under the Evidence Act Should not defeat the main cause of justice where the electronic record is reliable and its authenticity is proved. This same view was later explained in Arjun Panditrao Khotkar versus Kailash Kushanrao Gorantyal.[31] The recent development in the techno legal field has led to reduction in rigidity of certification requirements but the absence of specialised procedure within the BNSS for collection handling imaging of digital data still leaves an incomplete bridge between the Indian investigation system and digital investigation framework.

4. COMPARATIVE ANALYSIS OF THE LEGAL FRAMEWORK FOR DIGITAL FORENSICS WITH RESPECT TO THE UNITED STATES, THE UNITED KINGDOM AND CHINA

Digital forensics functions with a broader perspective of animations techno legal and political environment the basic Principles are more or less same which are about data collection preservation and analysis across different jurisdictions in the world. The comparison of few of this frameworks can be understood ask follows:

4.1.The United States

The US is seem to have one off the best jurisdictions in the field off digital forensic. This field is guided by its constitutional principles, statutory provisions and a few judicial precedents. The US constitution

[29] The Bharatiya Sakshya Adhiniyam, 2023, s. 63
[30] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
[31] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

tense to protect its citizen against many unreasonable searches and seizures this notion was introduced by the 4th amendment. The same right it's also extended to the digital data by the case Riley v. California[32] Stating that that a warrant must be obtained to access for searching any kind of data on an arrested person's mobile phone. Also while protecting this amendment the court in the case of Carpenter v. United States held that any step towards accessing historical cell site location information without any warrant directly violates the 4th amendment of the constitution. This judicial recognition underlines the importance of privacy, showing that digital privacy deserves a very heightened protection.

The US is seen to have very intricate collection of statutes which regulate the digital forensics and cyber crime which includes the Computer Fraud and Abuse Act (CFAA) which provides provisions to criminalise unauthorised access to computer systems and networks.[33] It also covers the interception and disclosure of the digital communications under Electronic Communications Privacy Act.[34] For enhancing and giving an upper hand inservice alliance and procedural checks for data collection The US has enacted USA Patriot Act.[35] And the Federal Rules Of Evidence which includes rule 901 and 902(14) prescribe the standards To verify the authenticity of electronic evidence using hash values.[36] The federal agencies of USA which includes FBI and DHS play a major role in maintaining add fast digital forensic laboratories and it has an institute known as National Institute of justice that provides national standards for digital forensic evidence handling and preservation.[37] Even with so many legislations The US still finds it difficult to solve the conflicts between state and federal authorities regarding the encryption back doors which was seen in the case of Apple Inc. v. Federal Bureau of Investigation.[38]

4.2.The United Kingdom

The United Kingdom is one of the countries that has maintained highly regulated yet a very right conscious legal framework for the digital forensic investigations this is because it is deeply Inspired by the European Convention On Human Rights.[39] The UK too has sound legal framework for the procedural authority for search, seizure and examination of digital data As provided under the Police And Criminal Evidence Act.[40] This act empowers the authorities to seize electronic devices and conduct lawful search and seizure.[41] The unauthorised access and data interference are further criminalised by the Computer Misuse Act.[42] The Snooper's Charter is the nickname for the Investigatory Powers Act focuses on interception, retention, and acquisition of various digital communications while putting a mandate on judicial authorization for surveillance operations and making sure that there is proportionality between the two.[43]

The UK courts tend to interpret digital forensic investigations with proportionality to the right to privacy as stated in the R v. Chief Constable of South Wales Police[44]. In this case, it was held that the automated facial recognition technology must comply with Article 8 of the ECHR. This judgment showed the

[32] *Riley v. California*, 573 U.S. 373 (2014).
[33] Computer Fraud and Abuse Act, 18 U.S.C., 1030 (1986).
[34] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2523 (1986).
[35] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001).
[36] Federal Rules of Evidence, Rules 901(a), 902(14).
[37] National Institute of Justice, "Digital Evidence and Forensic Science Standards," U.S. Department of Justice, 2020.
[38] Apple Inc. v. Federal Bureau of Investigation, U.S. District Court, Central District of California (2016).
[39] European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.
[40] Police and Criminal Evidence Act, 1984, c. 60 (U.K.).
[41] Id S.19
[42] Computer Misuse Act, 1990, c. 18 (U.K.)
[43] Investigatory Powers Act, 2016, c. 25 (U.K.)
[44] *R (Bridges) v. Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

importance of judicial vigilance over the overriding effect of digital investigations. The UK is at a better stage with a holistically developed forensic accreditation system lab where the evidentiary reliability is rigorous in criminal trials.

4.3.China

China has a very strong and central controlled approach towards cyber governance and digital forensics its principle of "cyber sovereignty" makes it different from any other nation in the world. The Chinese government tends to have broader control over data networks, every other online activity.

The Chinese legal framework consists of China's Cyber Security Law[45], Data Security Law[46], and Personal Information Protection Law[47], which form a strong trio to govern the digital ecosystem. The Chinese laws put an effort to protect the national security public order and data localisation which simply means building a great firewall to protect all its citizen data within the boundaries of the nation. The cyber security law also compels the network operators to cooperate with the law enforcement agencies during the investigations by providing all the required data and letting the government to have a sweep access to their entire collected digital data.[48]

The supreme People's Court and the government issued joint guidelines which clarified the standards of digital forensic evidence, which also required technical verification by experts.[49] However the state control over data still remains a top priority rather than the individual privacy.

China is seen to follow an inquisitorial approach where the investigation authority judiciary and the government share sweep access to digital forensic evidence. It is also known for having centralised cyber forensic laboratories which are integrated with their strong intelligence units. This joint infrastructure ensures efficacy transparency and judicial independence. Though the frequent use of digital forensics in national security and censored prosecutions has raised the line between prevention of cyber crime and snoopy political surveillance.[50]

5. CHALLENGES AND GAPS IN INDIAN LEGAL SYSTEM

Digital forensic investigation is not just about being a technical process but is also a sensitive legal procedure that has to be governed by the basic principles a fairness reliability and admissibility. Due to the volatile nature of the digital data the procedure lapses lead to deterioration in the evidentiary value while the judicial proceedings. These procedural lapses which later on act as problems in cyber crime prosecutions are as follows:

- **Using the Chain of Custody:**

The chain of custody is the documented process where the search, custody, control, transfer, analysis, and the disposition of digital data is recorded With the sole purpose to prove that the evidence pink presented in the court is exactly the same which was collected from the scene that is it is untampered and untouched.

[45] Cybersecurity Law of the People's Republic of China adopted June 1, 2017, Order No. 53 of the President of the People's Republic of China.
[46] Data Security Law of the People's Republic of China adopted June 10, 2021, Order No. 84 of the President of the People's Republic of China.
[47] Personal Information Protection Law of the People's Republic of China adopted August 20, 2021, Order No. 91 of the President of the People's Republic of China.
[48] Cybersecurity Law of the People's Republic of China, 2017, art. 21.
[49] Supreme People's Court and Procuratorate, "Provisions on Evidence in Criminal Proceedings Involving Digital Information," 2019.
[50] Human Rights Watch, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App* (2019).

The conventional forensics maintained the chain of custody through physical scenes and signatures of the witness but in the case of digital forensics the authenticity is maintained by putting hash values which are nothing but unique alpha numeric codes generated by using different algorithm. Any kind of minor change in the data can meddle with the hash values making it visible that the evidence was being tampered. The High Court of Delhi stated that proper documentation verification and authentication of digital evidence is crucial to prove admissibility.[51]

- **Jurisdictional Complexities and the Transnational Data**

The nature of the cyber crimes are inherently transnational as they often involve numerous servers and perpetrators who are located in transnational jurisdictions. This leads further in complication during investigations data collection. Though under international law these kinds of cooperations are generally facilitated through frameworks like the Budapest Convention on Cyber Crime[52], to which India is not a signatory. India being non signatory has limited its axis to cross border digital evidence. This leads to delay hey obtaining the foreign server logs are the user data which ultimately collapses the case. Whereas on the other hand countries like USA chooses cloud Act Agreements which directly facilitate data from its trusted partners and expedites the retrieval of evidences. India lacking such a treaty is left behind in the race of digital forensic investigations.

- **Encryption and Decryption of Data putting privacy at stake**

The recent advancement in the use of end to end encryption in online communications has proved to be one of the toughest challenge for enforcement of cyber law. Where the encryption is used to protect individuals privacy the same acts as a major obstruction while investigating the data. India does not have a clear decryption compulsion over its citizens. Even if the section 69 of information technology act do empower government to decrypt the data when required in interest of national security but the procedural steps are to weak to be taken and RA direct subject to the discretion of executive.[53] The absence of a proper judicial oversight has led to raising the concerns about fundamental right of privacy that is article 21 which was recognised in the case of Puttaswamy v. Union Of India[54].

- **Preservation And Retention Of Data Under Digital Forensics**

The digital data is volatile and vast in nature which makes it difficult to preserve it for a longer time. The intermediary guidelines and digital media ethics code rules 2021 made it compulsory for all the intermediaries to retain the data for at least 180 days.[55] However it's not necessary back the period may be sufficient for complex or some delayed investigations.

Thus, cases with advanced jurisdictions need to be served with preservation orders which are issued by the judiciary that compels the service providers and then comedies to retain a specific data till the end of the investigation.

- **Lack of Awareness in the Judicial System**

Since the digital forensics is an amalgamation of science, technology and law, it's often difficult for the courts to interpret some authentic technical evidence. The judges generally lack training in evaluating metadata, encryption logs blockchain technologies and thus are inconsistent in providing better judgments.

[51] *State v. Mohd. Afzal*, 107 (2003) DLT 385.
[52] Council of Europe, *Convention on Cybercrime (Budapest Convention)*, ETS No. 185 (2001).
[53] Information Technology Act, 2000, s. 69.
[54] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[55] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(g).

The National Judicial Academy And Bureau Of Police Research And Development has taken initiative to provide capacity building programs but it's just a small initiative with very small number of participants.[56]

6. RECOMMENDATIONS AND CONCLUSION

RECOMMENDATIONS

- An organization should be created that will operate on a national level and will be responsible for monitoring or regulating all the activities that are related to forensic laboratories and digital investigation units, which will be called the National Digital Forensics Authority. And it will set certain standards for handling electronic evidence, certify experts, and issue updated guidelines, which will be based on international standards like ISO/IEC.
- It is very important to make sure that all the electronic evidence is handled carefully, as these are very critical for digital justice. Therefore, the Ministry of Home Affairs should collaborate with the Bureau of Police Research and Development (BPRD) for issuing binding procedural codes under the Bhartiya Nagarik Suraksha Sanhita, 2023. And it should state each stage, i.e., seizure, imaging (copying data), chain of custody, and forensic analysis.
- Nowadays, mishandling of evidence is becoming a problem in failing most of the cybercrime cases. That's why it is important to provide specialized training in data recovery, blockchain forensics, etc., which should be made compulsory for police officers, public prosecutors, and judicial magistrates. And this training can be provided in collaboration with institutes like the National Forensic Sciences University (NFSU), Gandhinagar, and the Central Forensic Science Laboratories (CFSLs).
- It is very important for the judges and prosecutors to be updated about the digital evidence, for which they need to study judicial training modules on digital evidence, which should be introduced in the National Judicial Academy and State Judicial Academies, which will help them to stay updated on all the new technological advances.
- As it is clear that cybercrime often involves the data that is stored abroad, it becomes more important for India to have agreements with other countries so that we can access this data quickly. This could involve agreements similar to the U.S. CLOUD Act or the Budapest Convention on Cybercrime.
- By using blockchain technology, we can make the evidence handling process forgery proof and transparent. And by using this technology, it will be easier to digitally record every step from when evidence is seized to when it's analysed.
- In current times, it is becoming very important for digital investigation that all law universities, IITs, and forensic institutes start joining their hands to develop necessary tools and frameworks for coping with the current situation.
- The Bhartiya Nyaya Sanhita,2023, and the Bhartiya Nagarik Suraksha Sanhita,2023, should be regularly updated to keep up with the new emerging cybercrimes like crypto scams, AI misinformation, etc.
- Internet intermediaries, telecom operators, and cloud service providers should be legally obliged to keep and share digital records when needed. They must cooperate during legal processes while ensuring data privacy.

[56] Bureau of Police Research and Development (BPRD), "Training Modules on Cyber Forensics," Ministry of Home Affairs, 2022.

- Educate the public on cyber-crimes, cyber security, and cyber hygiene through raising various campaigns by inculcating these in Digital India initiatives and educational curriculum.
- Each Indian should have at least 1 advanced cyber forensic lab, which will operate on the state level like NDFA. It should audit these labs annually to make sure that they are meeting their national standards regularly.
- India should adopt global benchmarks such as those which are developed by INTERPOL, etc., which will improve Indian digital forensics by making our reports credible internationally.

CONCLUSION

In today's contemporary world, digital forensics is at the heart of criminal justice by helping the investigation authorities to trace the crimes being shaped by technology and being committed by individuals sitting in any part of the world. India's shift from its criminal laws to the latest criminal acts shows the importance of modernization in the collection of evidence and putting it to use in this era of verification. These new laws are seem to be acknowledging that total forensics is not a supplementary subject but is often the core of the entire case. The passing of new laws is nothing but the very first step towards getting the nation to fight the digital crimes but it is also necessary to accept that the real challenge is in its implementation, which can only be done by putting investigating authorities under the right training, providing them better resources, teaching them about handling of digital evidence without tampering its integrity. Also lack of expertise, poor digital infrastructure and the absence of a proper law to regulate the cyber issues can still hinder progress.

India must learn from countries like the United States and the United Kingdom, How to get a robust cybercrime detection mechanism and how to balance the fundamental rights with cybercrime surveillance. India as a nation has a long way to go in accepting these reforms and putting them into everyday practice, as there has to be proper law enforcement training that ensures a strong cooperation between the different sectors of government, and it also requires laws that would bring fairness and diligence, along with handling the digital forensics transparently.