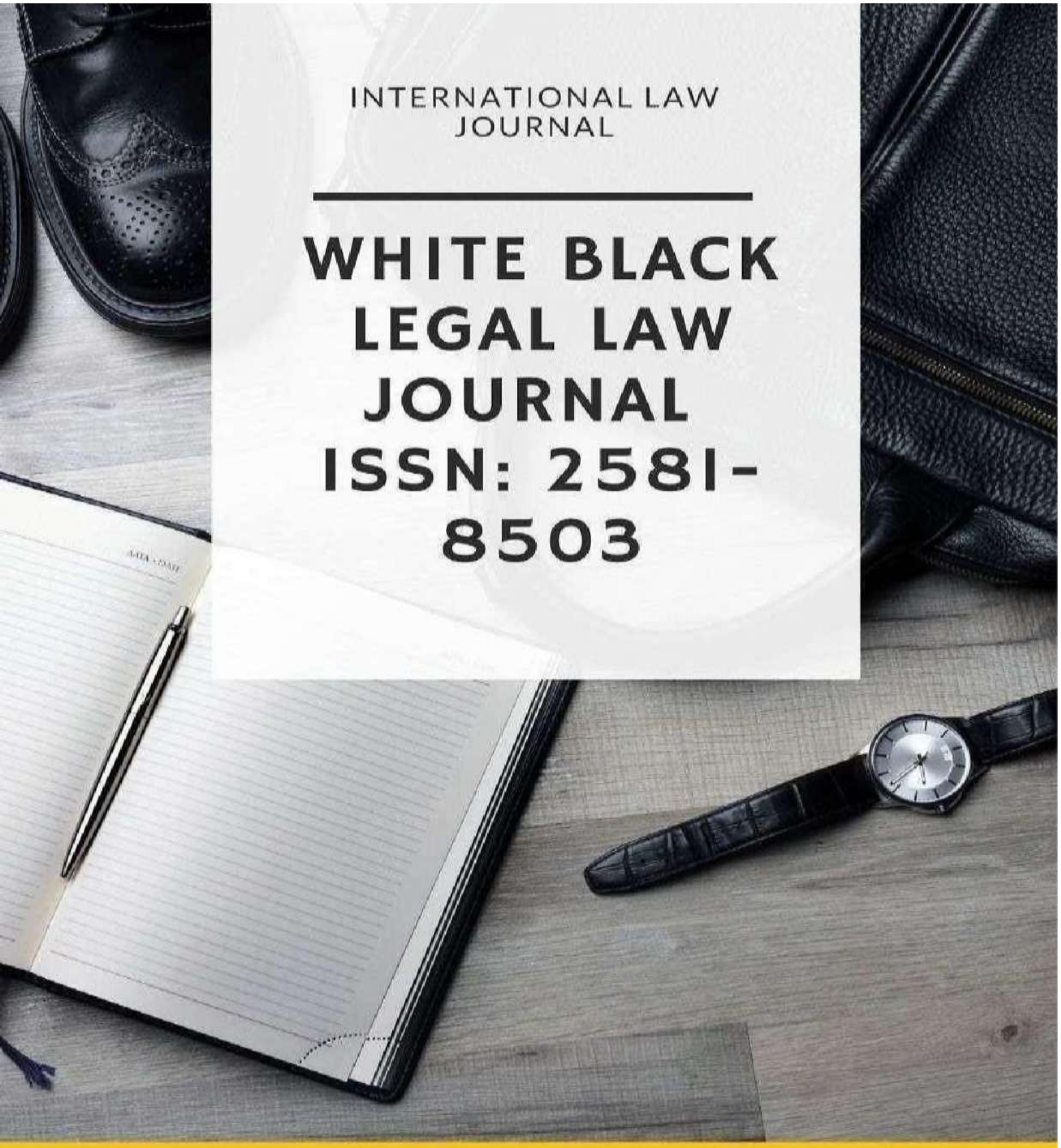

INTERNATIONAL LAW JOURNAL

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

ABOUT WHITE BLACK LEGAL

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

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

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

AIM & SCOPE

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

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

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

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

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

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

DIGITAL NAGARIK SAVDHAAN: NAVIGATING CYBER FORENSIC, CYBER SECURITY CHALLENGES IN INDIA'S DIGITAL HEALTHCARE ECOSYSTEM

AUTHORED BY - SAMRIDDHI RAI

ABSTRACT

The digitization of the healthcare ecosystem in India is referred to as a "watershed moment." The COVID-19 pandemic has significantly shifted the healthcare streamline and impacted overall well-being in India. While digital healthcare systems offer benefits such as accessibility, affordability, and efficiency, India is moving rapidly towards digitalization in the absence of a comprehensive legal framework. Though the DPDP Act, 2023 exists, it remains silent on essential aspects such as digital health, informed consent, biometrics, cyber forensic procedures, and AI. Globally, everything is fast-forward changing digitally, and digitalization is a ubiquitous or "indispensable element" of our lives. The healthcare system has gone digital in terms of collection, storage, and services, due to which cybercrime is rapidly increasing. However, India's latest past cyber records are not good in numbers. According to the DSCI-Seqrite India Cyber Threat Report 2025, key findings are triggering around 369.01 million malware detections were recorded in 2024. According to the study in this report, the healthcare system of India is considered a vulnerable center and the most cyber-targeted industry in India. This study aims to examine the core challenges at the intersection of cyber forensics and the digital healthcare system in India. It explores the gaps in legal frameworks, data collection practices, and cyber forensic investigation mechanisms, and proposes legal and policy-level safeguards. A systematic literature review was conducted using PRISMA 2020 guidelines. The doctrinal legal research method was adopted, focusing on peer-reviewed legal and policy research. The inclusion criteria encompassed studies discussing the legal framework of cyber laws related to cyber forensics in India's digital healthcare ecosystem. A qualitative synthesis was undertaken to identify recurring themes and critical gaps in the literature.

The review identified four thematic areas. First, there are critical challenges in cyber law particularly concerning cyber forensics within regulatory framework- CERT, NCIIPC, I4C, etc when applied to the healthcare ecosystem. Second, examining cyber forensic investigations procedural difficulties related to data identification, collection, examination, and judicial

admissibility within the DPDP Act, 2023, IT Act, 2000, the Evidence Act, and BNS when applied to the healthcare ecosystem. Third, privacy breaches frequently occur in the healthcare sector, exacerbated during forensic investigations. Lastly, the study finds a lack of regulatory clarity, digital literacy, rights-awareness among patients, and increasing vulnerabilities. The findings underscore the urgent need for a robust legal framework to address cyber forensic challenges in India's digital healthcare sector. The paper proposes a set of legal and technological solutions such as encryption strategies, legal reforms, admissibility protocols, and prioritization of privacy and cybersecurity to strengthen digital healthcare governance.

Keywords- Cyber Forensic; Digital Healthcare; Cyber Threats; Privacy; India.

Introduction

"Sarcasm: the last refuge of the chaste-souled individuals when their privacy is coarsely invaded"- **by Fyodor Dostoevsky from his book The Insulted and Humiliated**.

This also reminds us of the words of wisdom from Justice Subba Rao stated in the dissenting judgment in the Kharak Singh case: "*The right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life*." In this era of digitalization and rampant proliferation of technology, our privacy violations are at the cliff. Indeed, the healthcare industry is not immune from cyber-attacks and threats in India. According to the literature review and research conducted for this paper, it highlights the key alarming issues of privacy of patients in the healthcare industry, cyber-attacks, and cyber forensic investigation. AIIMS Delhi 2022 attack and Sun Pharmaceutical company data breach incidents are the highlights of cyber-attacks in India.

Another significant issue is cyber forensic investigation which takes place after a cyber-attack, and there are legal challenges associated with cyber forensic investigation, such as admissibility of digital evidence in the court, lack of privacy, and ethics in cyber forensic investigation in India. The digitalization in the health sector is the outcome of the Digital India initiative which is a "watershed moment"; however, it also exposed the huge amount of sensitive data of patients in the healthcare industry in the absence of a comprehensive legal framework of cybersecurity and privacy laws. The Digital Personal Data Protection Act, 2023 is a significant legislative achievement but there are gaps within the legal framework such as: digital health, digital literacy, sensitive data, and informed consent these terms are missing

from the DPDP Act 2023. There is also a lack of compliance between the DPDP Act, 2023 with cyber laws and the BNS.

The key findings of this paper suggest that though India has a legislative framework, challenges remain the same in terms of implementation and enforceability of laws, lack of awareness of digital literacy, and jurisdictional complexity in terms of cross-border issues. This paper delves around the role of cyber forensic experts in today's criminal investigation system and adds in the legislative framework of India as a significant step due to the expansion of digital devices especially in the healthcare industry, which is also highly vulnerable and the most targeted industry in cyber-crime attacks in India. The paper has attempted to examine the loopholes in the existing legal framework and propose a better framework for cyber forensic investigation with reference to the digital healthcare ecosystem of India. Currently, India is mostly governed by the IT Act, 2000 and BNS in terms of addressing cyber-related crimes, but with the rapid onset and amplification of cyber threats, India has to provide a comprehensive legal framework.

1. Critical Challenges in Cyber Security with Reference to Indian Digital Healthcare Ecosystem

Cybersecurity is nowadays a commonly used term by officials, laypersons, and professionals in the workplace. What is cybersecurity? In simple words, cybersecurity protects computer systems from all kinds of cyber threats that occur within the system[1]. The next logical question would be how? This question will be answered in this research paper through an analysis of India's current status quo in cyberspace and its regulatory framework. The main key aspect of cybersecurity is to protect digital data and to keep it intact[2]. One of the primary reasons why cyber threats are increasing is the lack of digital literacy[3]. In India, people are still not fully aware of their digital rights, and another associated issue is the digital divide, which is gendered in nature. Comparatively, women are less aware of their digital rights and digital literacy, especially in healthcare scenarios. For example, abortion services in clinics often require documentation (Aadhaar) for availing services. This data is stored in computer systems without

[1] Anjali Dixit, VB Malleswari and V Sai Medha, 'A Critical Study on Enhancing Cybersecurity in India's Healthcare Sector' (2024) 44(4) Library Progress International 193.
[2]Mthokozisi Hlatshwayo, 'Cybersecurity in The Digital Space' (2023) https://www.researchgate.net/publication/375115830_Cybersecurity_In_The_Digital_Space/citation/download accessed 6 July 2025.
[3] S Srivastava, 'International Literacy Day: Bridging India's Digital Divide' Bloomberg Quint (8 September 2020) https://www.bloombergquint.com/technology/international-literacy-day-bridging-indias-digital-divide accessed 6 July 2025.

taking patients' 'informed consent'. Another important finding relates to the accessibility and affordability of technology in the 21st century. Phones and the internet are easily available at cheaper prices, leading to a large number of users and an increasing dependency on the internet.

Undoubtedly, COVID-19 has been both a boon and a bane for the healthcare system in India. The digitalization of the healthcare system during pandemic has put patients' privacy at risk. According to a recent survey conducted by Check Point Software Technologies Ltd, approximately 6,935 cyber-attacks and threats were recorded each week over a six-month period in the Indian healthcare system. This number serves as a warning message for India's cybersecurity and healthcare systems[4]. In recent years, several major cyber threats have impacted the Indian healthcare sector. For example, AIIMS Delhi was severely affected by a cyberattack in 2022[5]. Similarly, ICMR experienced a significant cyberattack in 2023, during which passport and Aadhaar data were disclosed on the dark web[6]. This attack was identified by a U.S.-based firm, which reported that the leaked data was collected during the COVID-19 pandemic[7]. The important question arises: Is the digitalization of the healthcare system without a comprehensive framework sending a message to Indian citizens "Digital Nagarik, Savdhaan"?

Persistent challenges exist in the current cybersecurity framework concerning the healthcare system, such as: *1. Vulnerability in cyberspace*- The data breaches at ICMR, AIIMS, and other hospitals showcase the vulnerabilities in cybersecurity within the digital healthcare system. These gaps allow cyber hackers to exploit patients' data[8]. *2. Easy entry points*- There are numerous ways for hackers to enter computer systems due to the lack of digital safeguards in the healthcare system. For example, in 2024, a hospital located in Thiruvananthapuram was

[4] G Pariti, 'India's Healthcare Sector Battling 6,953 Weekly Cyberattacks: Report' India Technology News (28 June (2024) https://indiatechnologynews.in/indian-healthcare-sector-faces-6953-cyberattacks-weekly-outpacing-global-rates-check-point-threat-intelligence-report/ accessed 6 July 2025.
[5] B Sharma, 'Explained: What's Happening at AIIMS after Sensitive Ransomware Attack?' India Times (2 December 2022) https://www.indiatimes.com/explainers/technology/explainer-aiims-ransomware-attack-586542.html accessed 6 July 2025.
[6] Shubhdeep Kaur and Sukhchandan Randhawa, 'Dark Web: A Web of Crimes' (2020) 112 Wireless Personal Communications https://doi.org/10.1007/s11277-020-07143-2 accessed 6 July 2025.
[7] H Lohchab, 'Cyberattacks on Healthcare Sector Rising, 60% of Organisations Hit in a Year: Report' Economic Times (3 November 2023) https://economictimes.indiatimes.com/tech/technology/cyberattacks-on-healthcare-sector-rising-60-of-organisations-hit-in-a-year-report/articleshow/104917689.cms?from=mdr accessed 6 July 2025.
[8] 'An American Cybersecurity Company Has Said That the Personally Identifiable Information of Many Indian Citizens, Including Aadhaar Numbers and Passport Details, Were Being Sold on the Dark Web' The Hindu (7 November 2023) https://www.thehindu.com/sci-tech/technology/how-the-personal-data-of-815-million-indians-got-breached-explained/article67505760.ece accessed 6 July 2025.

affected by a ransomware attack that disrupted hospital operations for nearly five days. Computers and medical devices are interconnected through networks, which can easily become targets of such attacks[9]. *3. Poor defense mechanisms*- Cyber attackers are increasingly targeting India's healthcare sector because it is still undergoing digitalization without having adequate safeguards and robust mechanisms. It is important for the Indian healthcare ecosystem to strengthen defensive technology mechanisms to combat cyber threats. A notable example is the WannaCry ransomware[10] cyberattack in 2017, which exploited large amounts of digital data globally, including in parts of India. The key finding was that hackers used a flaw in Microsoft's system, and many other systems are still not trained or updated to fix such defects[11].

1.1. Role of Cyber Security Regulatory Frameworks in India:

A) Emergency Response Team- CERT is a key regulator in the Indian healthcare system. CERT is a mitigating tool which is essential and used by the healthcare system in order to combat cyber threats. Cyber Forensics plays an important role in understanding the cyber threat and digital evidence through cyber investigation. The CERT and Cyber Forensics come into the picture before and after the cyber-attack and breach has happened in the healthcare system at the same time. CERT provides the essential warning, guidance, defense strategy, and coordination with hospitals in order to prevent cyber-attacks. They are gatekeepers. It's more like an intelligence which works in the healthcare system. Cyber Forensics are key players for understanding and examining the cybercrime scene digitally in cyberspace, which requires technical skills and knowledge because of data's unique nature. As per the report of CERT, around 51% ransomware attacks happened in the Indian healthcare system in 2022[12].

[9] V George, 'Cyberattack Disrupted Functioning of RCC, but Patient Data Uncompromised' The Hindu (8 July 2024)https://www.thehindu.com/news/national/kerala/cyber-attack-disrupted-functioning-of-rcc-but-patient-data-uncompromised-veena/article68381750.ece accessed 6 July 2025.

[10] Maxat Akbanov and Vassilios Vassilakis, 'WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms' (2019) 1 Journal of Telecommunications and Information Technology 113 https://doi.org/10.26636/jtit.2019.130218 accessed 6 July 2025.

[11] Ibid.

[12]CERT-In, India Ransomware Report 2022 (2022) https://www.cert in.org.in/Pdf/Ransomware_Report_2022.pdf accessed 6 July 2025.

B) Indian Cyber Crime Coordination – I4C is an integral part of combating cyber threats in the healthcare system in India[13]. The primary work of I4C is to coordinate with hospitals and work as a responsive defense mitigating mechanism. I4C is a helpful tool used during cyber investigation and is helpful for Cyber Forensics during investigation, identification, examination, and it further provides support and strengthens the cyber security framework. It also helps the healthcare sector on how to overcome such data breaches and cyber-attacks.

C) National Critical Information Infrastructure Protection Center – NCIIPC is a center for identification of vulnerable check points within IT systems including the healthcare system. The center has been established with this intention to ensure resilient strategies and develop strong defensive mechanisms[14]. Further, NCIIPC also coordinates with the healthcare industry and is closely working on resolving the security issues related to electronic health records in order to detect and mitigate risks.

D) The Cyber Security Association of India – NCSAI works as a bridge between the cybersecurity world and the healthcare industry. The prime role is to spread cybersecurity awareness in the healthcare system and the best ways to adopt services for secure and uninterrupted services. NCSAI also helps healthcare professionals in order to conduct workshops and trainings.

Cybersecurity is crucial for the discussion in order to understand the cyber world. Digitalization of healthcare has brought cybersecurity and the legal framework into the limelight in the current times. The role of cyber forensics comes after the breach of data, cyber-attack, and any form of harm affected digitally. In order to understand the cyber forensics framework and challenges associated with cyber forensics, it's important to discuss firstly what we exactly mean by cybersecurity and what are the pressing issues the Indian digital healthcare system is dealing with. The next section of the paper is comprehensively focusing on the framework and challenges faced by Cyber Forensics in India.

[13] Indian Cybercrime Coordination Centre (I4C), Ministry of Home Affairs, Government of India, Official Website https://i4c.mha.gov.in/ accessed 6 July 2025.

[14] National Critical Information Infrastructure Protection Centre (NCIIPC), Official Website https://www.nciipc.gov.in/index.html accessed 6 July 2025.

2. Role of Cyber Forensics Investigations in Cybercrimes with specific reference to the Digital Healthcare Ecosystem in India.

The important question is: Why do we need a robust regulatory framework and cyber laws, especially concerning the role of cyber forensics in cybercrime investigation in India? There are several key points that address this question: Cyber forensic investigators are professionally equipped to conduct "cause analysis by looking at the digital misbehaviour[15]." In today's time, the cyber forensic field has become increasingly prominent in the realm of cyberspace. Cyber forensic investigators can detect and diagnose patterns and errors in systems, and through early detection, cybercrime can be prevented. According to the literature review, the research gap identified in this part lies in the inaccessibility of cyber forensic tools, the limited number of trained cyber forensic investigators, and the minimal participation of cyber forensic teams in cybercrime investigations. This is due to a lack of expertise and the small number of agencies in India currently engaged in cyber forensic investigations. Another reason is the "non-recognition" of cyber forensics by the legal fraternity. The judicial admissibility and authenticity of digital evidence in courts of law remains a pressing issue.

Cybercrime, especially in the healthcare industry in India, is prone to cross-border threats due to a vulnerable legal framework, and patients' sensitive data can easily be exploited by hackers. This part attempts to examine the role and process of cyber experts in cybercrime investigations and the challenges that currently exist in the legal framework. A cyber forensic expert plays a critical role in cybercrime investigation. Cyber forensics is a unique method because it deals with digital evidence not something tangible or physical, but data that requires technical expertise to interpret the cause of a crime. The role of cyber forensics does not end with the collection of data; rather, it begins there. Cyber forensic experts follow a structured process involving the identification, documentation, and interpretation of digital evidence found on computer systems, and present this digital evidence in a court of law to establish admissibility[16].

[15]M Varalakshmi and Sailaja Petikam, 'Role of Cyber Forensic Expert in Crime Investigation' (2022) 10(1) International Journal of Research in Management Sciences (IJRMS) 14 https://iaeme.com/Home/issue/IJRMS?Volume=10&Issue=1 accessed 6 July 2025.

[16] Arfid Ahmed, 'Have You Been Hacked? A Primer to Cyber Security and Cyber Forensics' (December 2005) The Chartered Accountant.

2.1. Cyber Forensic Analysis in Cybercrime Investigations: Cyber forensic investigation requires a comprehensive framework for the analysis of digital evidence[17]. It is therefore essential to follow all procedural steps to ensure proper and authentic analysis of such evidence. Cyber forensic investigations adhere to strict guidelines established by Interpol[18] and the international legal frameworks laid down by global organisations[19].

A) Identification of Preliminary Information[20]: This is the first step in a Cyber Forensic investigation, where cyber experts collect preliminary data, identify the parties involved, and understand the nature of the crime its place, date, and time. The difficulty lies in that if this identification phase is delayed, it may lead to degradation or loss of digital evidence. For example, digital evidence may be deleted, changed, or modified. In the healthcare industry, when cyberattacks or data breaches occur, sensitive data is often affected. This is because the nature of data stored or collected from patients is designated as "sensitive data". However, such data is not protected under the DPDP Act, 2023.

The cyber law landscape in India is vulnerable because it does not address breaches of sensitive data, particularly health data and other related cybercrimes. If such data is leaked or breached by hackers, the identification process of the data and its admissibility under cyber laws and in courts becomes difficult. Unlike other countries European nations under the GDPR[21] and California under the California Consumer Privacy Act[22] (CCPA). India does not explicitly protect sensitive health data.

B) Preservation of Digital Evidence for Analysis[23]: This stage is essential in cyber forensic investigations. It requires maintaining the integrity of digital evidence, and a record of the chain of custody for further scrutiny. In a court of law, the evidence

[17]US National Institute of Justice, Digital Evidence and Forensics https://nij.ojp.gov/digital-evidence-and-forensics accessed 6 July 2025.
[18]Interpol, Guidelines for Digital Forensics First Responders (March 2021) https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf accessed 6 July 2025.
[19]International Organization for Standardization (ISO), ISO/IEC 27037:2012: Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence (2012, confirmed 2018) https://www.iso.org/standard/44381.html accessed 6 July 2025
[20] Morgan Heavener, Paul Wright and Darren Mullins, 'Cyber Forensic Analysis: Strengthening Digital Evidence for Legal Proceedings' (July 2023) Accuracy https://www.accuracy.com accessed 6 July 2025.
[21]European Council, The General Data Protection Regulation (September 2022) https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation accessed 6 July 2025.
[22]State of California Department of Justice, California Consumer Privacy Act (CCPA) (May 2023) https://oag.ca.gov/privacy/ccpa accessed 6 July 2025
[23] Heavener, Wright and Mullins (n 6).

must be intact to be accepted in legal proceedings. India is still in the process of establishing dedicated cyber forensic centres. As of now, there are nearly seven Central Forensic Science Laboratories (CFSLs), and the National Cyber Forensic Laboratory (NCFL) is located in New Delhi.

C) **Examination of Digital Evidence[24]:** This step requires the technical expertise of Cyber Forensic professionals to interpret digital data. The interpretation of digital evidence plays a crucial role in cybercrime investigations. The final report should be precise, inclusive, cite proper findings and documents, and include a brief explanation for the admissibility of digital evidence in a court of law.

2.1.1. Legal Challenges in Cyber Forensic Investigation and Judicial Trends

The scope of digital evidence has expanded significantly over time. Cyber Forensic investigations have challenged traditional notions of admissible evidence in courts[25]. India is still progressing in its battle against cybercrimes, digital evidence management, and judicial admissibility. This section attempts to examine the challenges and gaps in the legal framework. Previously, the Indian Evidence Act, 1872, did not define what constitutes digital evidence, placing considerable pressure on the judiciary to interpret digital evidence and determine its admissibility. The newly enacted Bhartiya Sakshya Adhiniyam, *2023*, attempts to address these issues. However, this Act is silent on the procedures for using digital evidence in Cyber Forensic investigations. To some extent, the Information Technology Act, 2000, has tried to bridge the gap by defining electronic records and setting out conditions for admissibility[26]. However, the definition remains incomplete and narrow, leaving room for judicial interpretation. There is a landmark judgment by the Supreme Court in **Anvar P V v P K Basheer[27]**, which recognised the admissibility of digital evidence but only with proper authentication. Another significant case is **Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal[28]**, where the Court reaffirmed the requirement of a certificate under Section 65B (4) for the authenticity of electronic evidence. However, the Court did not clarify the definition of digital evidence.

[24] Ibid.
[25] Srinivas Katkuri, 'Legal Challenges and Lacunas in the Digital Forensics Jurisprudence in India' (2024) 10(3) International Journal of Law 23.
[26] Information Technology Act 2000, s 65B.
[27] Anvar P V v P K Basheer (2014) 10 SCC 473.
[28] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal AIR 2020 SC 4908.

This becomes problematic in scenarios involving the Indian digital healthcare ecosystem. Consider the following: The DPDP Act, 2023, is silent on digital health and "sensitive data." The IT Act, 2000, only covers "electronic records." These lacunae in the legal framework provide loopholes for cyber hackers to escape penalties. Further, the judicial admissibility of digital evidence remains unclear: What constitutes digital evidence? What is digital health? If patient data is breached, does it constitute "sensitive data"? What are the penalties and remedies for aggrieved patients? The DPDP Act, 2023, is not in compliance with other legal frameworks. It does not define "sensitive personal data" nor does it categorise "health data". This Act lowers the protection of patients' data, and since such data qualifies as sensitive, it should be safeguarded through a Data Protection Impact Assessment (DPIA) which is missing. This gap grants unrestrained power to data fiduciaries to misuse patient data[29].

Currently, the Bhartiya Nyaya Sanhita, 2023 (BNS) has reformed criminal law in alignment with cybercrime developments. It covers electronic fraud, possession, preservation, and tampering with digital evidence during criminal investigations[30]. Digital evidence and Cyber Forensic investigation are now a crucial part of new enactments. The focus must now shift to Cyber Forensics and digital-centric laws that address upcoming challenges in criminal investigations. However, challenges persist. The lack of compliance and legal coherence across various laws has created multiple avenues for judicial interpretation. These need to be resolved to strengthen India's legal system. The next part of the paper will discuss the critical issue of privacy especially relating to patients' data and the challenges within the legal framework for safeguarding the privacy of citizens during cyber forensic investigations and cyberattacks.

3. Analysis of Privacy Right of Digital Nagarik

This part is dealing with privacy issues associated with the cyber-attack and challenges concerning cyber forensic investigation. History is a good place to start. The Supreme Court, in the landmark case **of KS Puttuswamy (Retd.) & Anr. v Union of India[31]**, declared the right to privacy a fundamental right under Article 21 of the Indian Constitution. However, this judgment in reality has had little effect on the legislative framework. To understand the

[29] Paarth Naithani, 'Protecting Healthcare Privacy: Analysis of Data Protection Developments in India' (2024) 9(2) Indian Journal of Medical Ethics New Series 149.
[30] Deepali and Radhika Dev Verma, 'Role of Digital Forensics and Criminal Investigation in India' (2024) 5(11) International Journal of Research Publication and Reviews 87 http://www.ijrpr.com accessed 6 July 2025.
[31] KS Puttuswamy (Retd.) & Anr. v Union of India (2017) 10 SCC 1

problem of privacy in the cyberspace world and the challenges concerning digital data of patients are pressing issues. Let us discuss the scenario where a pregnant woman goes for an abortion. For abortion services, she has to submit and complete the documentation process. For abortion services, Aadhaar is required for identification. Aadhaar is linked with other documents (bank account, ration card, PAN card, etc.). The Aadhaar details along with her medical data are collected and stored in the computer system in the form of digital data. Afterwards, the hospital receives cyber threats or data is leaked. According to the KS Puttuswamy judgment, the right to privacy, which is guaranteed under Article 21 of the Indian Constitution, has been breached. However, Aadhaar cannot be used unnecessarily for abortion services or for any other medical services. TB patients are required to submit their Aadhaar for the continuation of medical services in hospitals[32]. The privacy has been breached because of surveillance due to lacunae in the legal framework. The pregnant woman's data, which is breached because of a cyber threat, is a case of privacy violation. The loopholes are attached to such scenarios.

The *first issue* is under the DPDP Act, 2023, digital health, sensitive data, and informed consent are missing. If the aggrieved pregnant woman seeks remedies, she has to prove her stance, but because the law is absent, the accused person can easily escape. The *second issue* is related to cyber forensic experts. There is a lack of compliance between the IT Act, 2000, DPDP Act, 2023, and BNS in relation to cyber forensics, digital evidence, sensitive data (e.g., health data), digital health, and informed consent. These terms are missing, and there is no interlinkage within these legal frameworks, and the framework is overlapping in nature. The *third issue* is that we do not have separate laws dealing with privacy, digital health, and cyber forensic investigation, which gives a lot of room for open interpretation. What are the standards and parameters that cyber forensic experts are following while collecting digital evidence? And what if sensitive data has been misplaced what are the remedies? Is there any grievance redressal? Privacy is sensitive in nature. There are major ethical issues attached to Cyber Forensic investigations. It creates policing on privacy issues. What if a cyber forensic expert stumbles on sensitive personal data which has nothing to do with the investigation but uses that information? It's a clear violation of Article 21 of the Indian Constitution[33].

[32] Anoo Bhuyan, 'And Now, Aadhaar Is Mandatory for TB Patients Seeking Government Cash Benefits' The Wire (21 June 2017) https://cms.thewire.in/149709/aadhaar-manadatory-tb-cash-benefits/ accessed 8 July 2025.
[33] Deepali and Verma (n 30)

There was a pilot study conducted and published by Springer as a chapter[34].The findings of the survey show that "privacy of an individual is at risk during a digital forensic investigation and that there is an urgent need to incorporate data privacy measures in the investigative process[35]." A key observation made by the researchers in their survey which is relevant is that there is no uniformity or balance between the protection of the privacy of individuals and the completion of investigation. The key reason observed was a lack of awareness about the importance of data privacy and digital literacy. Researchers have suggested the use of cryptographic mechanisms for the protection of digital evidence during investigation. Another technique proposed by the researchers is the "compartmentalization of data into layers."

Currently, the laws are not solution-centric but rather procedural-centric focusing on how to conduct investigation and analysis. The major frameworks which are indirectly dealing with cyber forensic investigation have no integration with privacy protections. The persistent issues arising from cyber forensic investigations are: Unnecessary digital data collection and storage, which raises privacy concerns, including third-party privacy breaches. Cyber forensic experts, while investigating cybercrimes, collect information from personal devices without taking informed consent. Sometimes, digital data needed to be collected by cyber forensic experts is physically stored on computer servers located in different countries, which raises jurisdictional issues, different privacy laws, and cross-border challenges in healthcare. For example, there is a patient whose data is stored on a cloud server in multiple locations, and a cyber breach happens. In such scenarios, privacy is of utmost concern while locating the data and proving the admissibility of digital data in the court of law.

Conclusion

Cyber Forensic is still in a nascent stage and finding its place in the Indian legislative framework and investigation space. Not only technology has changed but the crime patterns have also changed over the period of time. In the 21st century, we are mostly dealing now with digital evidence, and cyber forensic is essential for a robust mechanism to combat cyber-attacks in the Indian legislative framework, especially in the healthcare sector of India. The Indian judiciary has somewhat shown the pathway through legal interpretation but enforcement

[34] Robin Verma, Jayaprakash Govindaraj and Gaurav Gupta, 'Data Privacy Perceptions About Digital Forensic Investigations in India' in Gilbert Peterson and Sujeet Shenoi (eds), Advances in Digital Forensics XII (Springer 2016) 25.
[35]Ibid.

agencies have to actively bring forward the changes, and implementation has to be efficient. The Indian approach towards cyber law still remains a dismal picture and for achieving the broader goals for cyber forensic investigation, there are a few key suggestions for enhancement of cyber forensic investigation, such as: *1. Robust legislative engagement*- The DPDP Act 2023 is a welcoming step, but the law is not fulfilling the purpose. The existing current data protection law needs to be incorporated as per international norms and make amendments related to biometric data, digital health, digital literacy, informed consent, sensitive data, data portability, and explicitly define its admissibility in the court of law. *2. Efficient engagement of enforcement agencies*- There is a lack of skilled staff in CERTs, the Data Protection Board of India, cyber cells, and other establishments. There is a lack of coordination among enforcement agencies, police, judiciary, government, and cyber unit cells. They must come together for effective implementation. *3. Tech-centric legal approach*- Bridging the gap between technology, law, and judiciary for better accessibility. Usage of AI, automated redressal mechanisms, blockchain, and creating a multilingual database for inclusive justice.

"Science & technology have freed humanity from many burdens & given us this new perspective & great power. This power can be used for the good of all. If wisdom governs our actions, but if the world is mad or foolish, it can destroy itself just when great advances & triumphs are almost without its grasp". By- Jawaharlal Nehru