LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 2 | Issue 1

2024

CYBERSECURITY AND DIGITAL FORENSICS: LEGAL ASPECTS OF INVESTIGATING CYBERCRIMES

Muskan Jaiswal[1]

I. ABSTRACT

The rapid development of cyberspace has resulted in an increase in cybercrimes, posing substantial obstacles for global legal systems and law enforcement agencies. With a focus on cybersecurity and digital forensics, this research paper examines the legal aspects of cybercrime investigation. It looks at jurisdictional concerns, legislative obstacles, international cooperation, and the current legal framework pertaining to cybercrimes. The paper also explores digital forensics, which includes the gathering, storing, and admissibility of electronic evidence in court, along with the integrity of that evidence. Advanced technologies such as blockchain and encryption and their effects on digital forensic practices are discussed, along with ethical and privacy considerations in cybercrime investigations. Case studies and precedents are used to show how cybercrime investigations are carried out in different legal frameworks around the world and to suggest ways to improve investigations while maintaining due process. This essay seeks to shed light on the intricacies of cybercrime investigations and make suggestions for enhancing their efficacy while abiding by the law.

II. KEYWORDS

Cybersecurity, Digital Forensic, Cybercrimes, Investigation, Regulatory Guidelines, The Indian Evidence Act, Information Technology Act, Data privacy

III. INTRODUCTION

Digital forensics and cybersecurity are essential tools in the fight against cybercrime in the modern era. This essay explores the significance of these fields from a legal perspective, delving into their intersection. It specifically looks at the different legal

[1] BBA LLB 3rd Year Student, New Law College, Bharati Vidyapeeth (Deemed to be University), Pune

frameworks that influence how cybercrimes are investigated in court, such as evidence law, contract law, property law, criminal procedure, and cybercrime legislation. The significance of legal search authority in the digital forensic process is emphasized by the strict criteria that must be followed for the admission of digital evidence. It is crucial to understand, though, that constitutional amendment violations during digital forensic investigations may result in legal consequences. The purpose of this paper is to clarify the dynamics of case law and the changing regulatory environment that shapes the field of digital forensics.

IV. WHAT IS CYBERCRIME?

Any criminal act that uses digital technology such as computers, the internet, or networked devices is classified as a form of cybercrime. It includes a variety of illegal practices, including fraud, identity theft, data breaches, computer viruses and all kinds of scams. Cybercriminals may be motivated by profit or ill intent toward people, corporations, or any public entities.[2]

There are several types of cybercrime, including:

- **Hacking:** Unauthorized login to a computer system or an account, often to cause more harm to the victim.
- **Phishing:** pretending to be genuine companies or individuals to lure users into disclosing confidential details.
- **Malware:** The introduction and dissemination of infectious programs such as viruses, worms, Trojans, and ransomware in a device or network.
- **Identity theft:** What is known as identity theft is the stealing of personal information like names, addresses, and social security numbers to impersonate another individual.[3]

[2] https://www.techtarget.com/searchsecurity/definition/cybercrime , last visited 29 Jan 2024
[3] Interpol , last visited 20 March 2024

V. WHAT IS CYBERSECURITY?

The process of safeguarding networks, data, computers, servers, mobile devices, and other electronic systems against illegal or hacker activity is known as cybersecurity.[4] By security, we mean preventing unauthorized users from accessing or using systems, networks, or technologies. Numerous techniques, such as network security, endpoint security, application security, data security, real-time malware detection, and others, can be used to accomplish this. Cybersecurity is essential to both personal and business operations because it protects against data breaches, monetary losses, and reputational harm. To keep up with the volume and complexity of cyber threats, a proactive and adaptable response is needed. On the other hand, cybersecurity management entails putting in place the appropriate security measures, conducting regular risk assessments, and creating a robust cybersecurity culture in an organization.

VI. WHAT IS DIGITAL FORENSIC?

The field of digital forensics belongs to the sphere of forensic science and is concerned with tracing, preservation, analysis, and presentation of electronic data which may be of value in the investigation. It includes digital information from mobile devices, smart appliances, computers, and car navigation systems. The gathering, examination, and preservation of evidence is the goal of digital forensics. Identification, preservation, analysis, documentation, and presentation are among the steps. In order to read the data from the device without causing any damage, digital forensic tools are highly helpful. Both private investigations and criminal law frequently use digital forensics.[5]

VII. IMPORTANCE OF INVESTIGATING CYBERCRIMES

Cybercrime investigation is essential because of the worldwide threat that cybercrime poses to individuals, organizations, and governments. The investigation's primary

[4] "NIST Computer Security Resource Center | CSRC." https://csrc.nist.gov/. Last visited 20 March 2024

[5] "Digital Forensics | NIST - National Institute of Standards and Technology." https://www.nist.gov/programs-projects/digital-forensics. Last visited 20 march 2024

objectives are, to find the crime scene, gather a tone of evidence, and present it in a way that will allow cybercriminals to be fairly charged in court[6]. To protect future cyber threats and give justice to the victims of cybercrime, this process is essential. Since cybercrime is a very sophisticated crime, law enforcement agencies, for-profit companies, and organizations that specialize in cybercrime must secure evidence that is shared to successfully prosecute any cybercriminals[7]. Anticipated expenditures of $10.5 trillion by 2025[8], equivalent to $32,000 per person in the United States, underscore the importance of cybercrime investigation concerning the defense and preservation of both individuals and organizations. Forensic data related to hacking incidents, data breaches, phishing attacks, and online fraud is retrieved and examined as part of the investigative process. Cybercrime investigations must adhere to standard investigative procedures and confer with prosecutors due to the global reach of the Internet.

VIII. LEGAL FRAMEWORK FOR CYBERCRIME INVESTIGATION

The legal framework governing the conduct of cybercrime investigations, evidence gathering, and international collaboration constitutes the investigative framework. Robust legislation targeting cybercrime not only forbids specific forms of cybercrime but also establishes acceptable usage guidelines for digital devices and the Internet. There are also limitations aimed at lessening the harm that cybercrime causes.

A. INTERNATIONAL LAWS AND TREATIES

International collaboration, harmonization of national legal frameworks, and improved cybercrime investigation techniques are the goals of cybercrime treaties and laws. This is demonstrated by the 2001 Council of Europe Convention on Cybercrime, which

[6] "Cybercrime Investigation Tools and Techniques You Must Know! - CyberTalents." https://cybertalents.com/blog/cyber-crime-investigation. last visited 29 Jan 2024.
[7] "Cybercrime Module 5 Key Issues: Who Conducts Cybercrime Investigations?." https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/who-conducts-cybercrime-investigations.html. last visited 29 Jan 2024.
[8] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/. Last visited 20 March 2024.

mandates that all member nations make offences like hacking, the production, sale, or distribution of hacking tools, as well as intellectual property infringement, punishable by law. Each party to the treaty shall also provide its law enforcement agencies with enhanced capabilities for search and seizure. These authorities include the ability to compel an ISP to maintain a customer's connection and to track a customer's online activities in real time. Bilateral, regional, and international cybercrime treaties are examples of formal frameworks for international cooperation. Since May 2021, the member states of the UN have been working on a draft international convention on cybercrime. This treaty may grow to be a significant body of international law that unites efforts to prosecute criminals everywhere.[9]

One well-known international agreement that deals with cybercrime is the Budapest Convention on Cybercrime. The Council of Europe established this agreement in 2001 with the goals of enhancing global cooperation in the battle against cybercrime, enhancing investigative techniques, and harmonizing state laws. It mandates that member states engage in illicit activities such as the development or distribution of hacking tools, hacking, and intellectual property infringement. It also necessitates providing law enforcement agencies with equipment for electronic evidence gathering, search and seizure, and real-time Internet service provider (ISP) activity monitoring.[10] Another significant development in the area of international cybercrime law is the ongoing efforts of United Nations member states to create a treaty against cybercrime. Commencing in May 2021, the objective of this agreement is to establish a comprehensive legal.

B. NATIONAL LEGISLATION AND REGULATIONS

[9] "Cybercrime Module 7 Key Issues: Formal International Cooperation Mechanisms." https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html. Last visited 29 Jan 2024

[10] "Budapest Convention: What is it and How is it Being Updated?." 02 Jul. 2020, https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/. Last visited 20 March 2024

In India, the legal, regulatory, and institutional framework for cybersecurity is controlled by a number of statutes, applicable regulations, and industry-specific regulatory frameworks that define cybercrimes, encourage adherence to security standards, and mandate incident reporting. Data security, cybercrime, and cybersecurity are primarily governed by the Information Technology (IT) Act, 2000[11]. The IT Act defines the components of cybersecurity, and among the laws that address cybersecurity is the Indian Penal Code 1860. The Digital Personal Data Protection Act, 2023[12] is a strict privacy law that governs the digital processing of personal data. Violating it carries a maximum penalty of INR $31 million. As of June 2024, the law will be in effect. The code requires all holders of telecom licenses to set up monitoring systems to keep an eye out for any fraudulent activity, hacking attempts, or attacks on the technical infrastructure. They must also notify the Department of Telecommunication of any such incidents. Cybercrime includes theft,[13] fraud[14], forgery [15], defamation [16], mischief [17], and all other offences covered by the Indian Penal Code of 1860. In addition, bilateral, regional, and multilateral cybercrime treaties—formal processes for international cooperation—are part of India's legal framework for cyber defense.[18]

C. LANDMARK CASES RELATED TO CYBERCRIMES INVESTIGATION

[11] "Information Technology Act 2000 | Ministry of Electronics and ...." https://www.meity.gov.in/content/information-technology-act-2000-0
[12] "Digital Personal Data Protection Act 2023 | Ministry of Electronics and ...." 12 Aug. 2023, https://www.meity.gov.in/content/digital-personal-data-protection-act-2023. Last visited 29 jan 2024.
[13] "Section 378 in The Indian Penal Code, 1860 - Indian Kanoon." https://indiankanoon.org/doc/1280620/. Last visited 29 jan 2024
[14] "Section 25 IPC: Understanding the Offense of "Fraudulently"." 03 Mar. 2024, https://capitalvakalat.com/blog/section-25-ipc/.
[15] "IPC Section 463 - Forgery - Punishment and bail - LawRato." https://lawrato.com/indian-kanoon/ipc/section-463. Last visited 29 jan 2024
[16]"Section 499 in The Indian Penal Code, 1860 - Indian Kanoon." https://indiankanoon.org/doc/1041742/. Last visited 29 jan 2024
[17] "Section 425 in The Indian Penal Code, 1860 - Indian Kanoon." https://indiankanoon.org/doc/441951/. Last visited 29 jan 2024
[18] "A comparison of cybersecurity regulations: India - PwC." https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html. Last visited 29 jan 2024

India has very few landmark cases in terms of cybercrime investigations. However, some important cases have set legal precedents:

1. **State of Maharashtra v. Vijay Mukhi (2003)[19]:** This was the first conviction in India, under the Information Technology Act, 2000. The defendant was convicted of breaking into a website and changing the content on it.
2. **Anvar PK v/s P K Basheer[20]:** This is a notable case concerning electronic evidence. The court demonstrated that electronic evidence should be authenticated similarly to ordinary evidence.
3. **Shreya Singhal v. UOI[21]:** This is another landmark case that has looked into the problems of the freedom of speech on the Internet. In this case, section 66A of the Information Technology Act, 2000, which criminalized sending messages through communication services, was struck down.
4. **Syed Asif-ud-din and Ors. v. State of Andhra Pradesh and Anr.[22]:** This is another significant case on the cyberstalking matter. The case set out that cyberstalking is a criminal offense in accordance with Indian Penal Code.

These cases established landmark legal precedents and established a solid legal framework governing cybercrime investigation in India.

IX. LEGAL ASPECTS OF DIGITAL FORENSIC

The Indian constitutional laws governing the legal connotations of digital forensics are designed and compiled from various statutes, rules and legal principles. According to the Indian Constitution, the following are some significant legal facets of digital forensics:

1. **Constitutional Rights:** The Indian Constitution's Article 21 guarantees the right to privacy, while Article 20 protects the right to self-incrimination. Digital

[19] "The State Of Maharashtra vs Vijay Mohan Jadhav @ Nanu And Ors on 25 ...." https://indiankanoon.org/doc/132764905/.
[20] Anvar P.V vs P.K.Basheer & Ors on 18 September, 2014 - Indian Kanoon, last visited 29 Jan 2024
[21] Shreya Singhal v. Union Of India AIR 2015 SC 1523 - Legal Service India , last visited 29 Jan 2024
[22] Syed Asifuddin And Ors. vs The State Of Andhra Pradesh And Anr. on 29 ... , last visited 29 Jan 2024

evidence collection and utilization in criminal investigations is greatly influenced by these rights.

2. **Information Technology Act, 2000[23]:** Digital signatures, digital evidence, and electronic transactions are all recognized by the Information Technology Act of 2000 and its later amendments. We also cover the topic of cybercrimes and whether or not electronic documents can be used as evidence in court.

3. **The Indian Evidence Act,1872:** Under the Indian Evidence Act, evidence admissibility in Indian courts is governed. Section 65B [24] provides detailed guidance on the use of electronic documents, subject to certification by a responsible official regarding the operation of the relevant information system.

4. **The Code of Criminal Procedure, 1973:** The Code of Criminal Procedure (CrPC) provides for the process of investigations and prosecution of various criminal offences. The CrPC formulates the legal discipline for admissibility of electronic evidence in criminal cases. Section 91 and 165 provide power to obtain summons for production of e-records and seizure of electronic devices, respectively. The term 'Section 172' is used to describe the investigative proceedings log. These acts are associated with the gathering and evidential scrutiny of electronic evidence that has been utilized in criminal procedures.

5. **Right to Privacy:**[25] Among the many cases related to the right to privacy, the case of ***K.S. Puttaswamy (Retd.) and Anr. v. Union of India*** [26] was brought up to acknowledge the right to privacy as a fundamental right under the Indian Constitution. This also has significant implications for the collection and usage of digital evidence, particularly in privacy-related matters.

[23] "Information Technology Act 2000 | Ministry of Electronics and ...."
https://www.meity.gov.in/content/information-technology-act-2000-0. Last visited 20 march 2024
[24] Section 65 in The Indian Evidence Act, 1872 - Indian Kanoon , last visited 29 Jan 2024
[25] Right to Privacy: Constitutional Rights & Privacy Laws , last visited 20 March 2024
[26] Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018

6. **Jurisdictional Consideration:** In the field of digital forensics, cross-border components are often added, and these elements bring challenges of jurisdiction. Therefore, concepts of treaty and international law are very useful in addressing these issues especially in cases where transnational forms of cybercrimes are implicated.

In order to guarantee that investigations in cases involving digital evidence are carried out based on legal provisions and their constitutional rights, all these legal considerations should be handled by legal professionals, law enforcement agencies, and digital forensic experts in accordance with Indian constitutional law. Furthermore, as technology advances, the Indian legal system will need to adapt to new developments in digital forensics and engage in ongoing legal research.

X. REGULATORY GUIDELINES FOR COLLECTING DIGITAL EVIDENCE

There are several legal regulations governing the acquisition of digital evidence in India. These standards are governed by numerous statutory laws, regulations, and legal precepts. The following significant legal requirements must be met in India when collecting digital evidence:

1. **Search Warrants:** One of the common procedures for protecting electronic devices in order to collect digital evidence is this one. Law enforcement must obtain a search warrant from a judicial magistrate or another authorized officer before beginning a search and seizure operation.
2. **Chain of Custody[27]:** For the digital evidence, an appropriate chain of custody had to be established. In order to maintain information integrity standards and the admissibility of the evidence in accordance with legal requirements, this also entails documenting the handling, storing, and transferring of the digital evidence.

[27] Chain of Custody - StatPearls - NCBI Bookshelf , last visited 29 Jan 2024

3. **Admissibility**: The digital evidence should have to fulfill criteria regarding standards of admissibility as mentioned in the Indian Evidence Act 1872. The Section 65B in the Act stipulates the conditions under which evidence in the form of electronic records is admissible in court and the evidence must contain an authentication certificate.

4. **Data Privacy and Consent:** Adherence to data privacy regulations and obtaining consent for the access or collection of personal data are required in cases where digital evidence contains communications or personal data. Confidential personal data protection is outlined in the Information Technology (Responsible Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[28]

5. **Evidence Preservation:** Proper preservation of digital evidence should help prevent manipulation or change. It is a matter of making notes of actions taken, ensuring the integrity of original evidence, as well as taking forensic photos of electronic devices.

6. **Legal expertise:** Digital forensics in most cases, one man's experience and specialized knowledge are needed to help with the digital evidence collection process. To guarantee the acquisition of evidence under more lawful circumstances, law enforcement officials and legal specialists involved in the process should either collaborate with digital forensic professionals or possess the necessary technical knowledge.

7. **Compliance with Procedural requirements:** The Code of Criminal Procedure, 1973 is the statute that establishes standards for conducting investigations and obtaining evidence in criminal cases. It also outlines the procedural requirements that must be met when gathering digital evidence.

[28] "IT Reasonable Security Practices and Procedures and Sensitive Personal ...." https://cis-india.org/internet-governance/files/it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.pdf. Last visited 20 March 2024.

8. **International Considerations:** In order to ensure that evidence from foreign jurisdictions is admissible in Indian courts in cross-border cases involving digital evidence, it may be necessary to adhere to international laws, treaties, and agreements for mutual legal assistance.

The significance of digital evidence collection that conforms with privacy laws, constitutional rights, and evidentiary standards is underscored by these legal demands. Ensuring the validity and admissibility of digital evidence in Indian judicial proceedings requires strict adherence to regulatory criteria.

XI. LEGAL ISSUE IN DIGITAL FORENSIC

Digital forensics professionals must consider a wide range of intricate legal issues in order to gather, examine, and present digital evidence in a way that is both morally and legally sound:

1. **Digital evidence admissibility:** Ensuring that digital evidence is gathered and stored adhering to the proper chain of custody and authentication procedures, as well as legal standards for admissibility in court[29].
2. **Respecting privacy and data protection laws:** Adherence to privacy and security regulations and personal data protection is of paramount importance whenever sensitive or confidential material is at stake, including in the context of digital forensic examinations.[30]
3. **Laws pertaining to searches and seizures:** Preserving the protections provided by the Constitution against unlawful search and seizure by obtaining warrants based on a reasonable suspicion in order to retrieve data or electronic equipment.[31]

[29] "Chain of Custody - StatPearls - NCBI Bookshelf." 13 Feb. 2023, https://www.ncbi.nlm.nih.gov/books/NBK551677/.
[30] Data Privacy Rights and Protection in Digital Forensics ... - LinkedIn , last visited 21 March 2024
[31] Digital Search Warrants - Law Enforcement Cyber Center , last visited 21 March 2024

4. **Laws pertaining to computer crimes:** Understand and abide by the laws pertaining to computer crimes, such as those pertaining to hacking, unauthorized access, data theft, and cyberstalking, when examining digital evidence[32].
5. **Intellectual property rights**:[33] When using digital evidence that may contain proprietary or copyright-protected content, it is crucial to make sure that intellectual property rights and copyright are upheld.
6. **Electronic Communications Privacy Act:** That adheres to ECPA's rules regarding electronically stored communications, such as emails and other electronic messages, and electronic communication interceptions.
7. **Jurisdictional issues:** Handling the legal challenges brought on by jurisdictional concerns during digital forensic operations involving data stored across national borders or legal jurisdictions.
8. **Legal challenges to forensic methods:** The contentious issues surrounding the reliability and validity of the forensic techniques and instruments used to gather and examine digital evidence will be covered in this section.
9. **Legal requirements in corporate settings:** Comprehending the responsibilities and constraints imposed by employment laws, digital preservation guidelines, and employee privacy when performing digital forensics in commercial settings.
10. **Expert witness testimony**: By ensuring that the necessary number of digital forensics specialists are available to testify in court and that their qualifications and reliability are up to par with the law.

These legal concerns highlight how crucial it is to review pertinent laws and rules and consult with legal counsel in order to guarantee compliance and moral conduct during digital forensics investigations.

[32] The 10 Most Common Internet Crimes | Complex , last visited 21 March 2024
[33] Intellectual property , last visited 22 March 2024

XII. FUTURE TRENDS AND SUGGESTIONS FOR ADVANCEMENT

Future directions and recommendations for cybercrime investigations include finding solutions to novel legal problems, suggesting policies to support legislative frameworks, and outlining moral standards for digital forensics professionals.

a. Emerging Legal Issues in Cybercrime Investigations

Ongoing criminal activity and technological advancements, however, will continue to create new legal challenges in cybercrime investigations for as long as they are conducted. The topics covered include safeguarding privacy rights in digital forensics, cyberspace jurisdictional concerns, and the admissibility of digital evidence. Legal systems will need to be updated frequently in order to combat cyber threats and uphold the rule of law.

b. Policy Recommendations for Improving Legal Frameworks

Legislators are expected to take into account updating current legal frameworks to accommodate the novel viruses. This could entail rerouting funds for cybercrime prevention and investigation to law enforcement organizations, as well as modifying international cooperation-related laws and treaties. With the goal of making sure that new forms of cybercrime are appropriately dealt with by the legal system and that people's rights and privacy are safeguarded.

c. Ethical Guidelines for Digital Forensic Practitioners

The one of the most important things to create ethical guidelines or guidelines for practitioners, which doesn't just give a notion of professional behavior, but also the accountability, to the field of digital forensics. Under such policies the areas to be covered are like upholding the integrity of the evidence collection, the security of the privacy individual, the declaration of any possible conflict of interest, and the standards and practices that govern digital forensics. Ethical norms are the way of ensuring that the duties of digital forensic professionals are done within the standards of integrity and ethics.

XIII. CONCLUSION

As it has been summarized above, cleaning up cybercrimes and ensuring that quality evidence is sustained highly rests on the legal aspects of cybersecurity and the digital forensics. As we have seen in the discussion, we have been discussing the definition of digital forensics and cybersecurity in relation to the investigation of cybercrimes illustrating the importance of these two concepts in the digital world. With the thought for the complicated environment in which these regions operate and also with the appropriate intention of revealing the legal and ethical considerations that stand behind them, we have as well operated under the problem. Goals- A review of the legal commentary for cybercrime investigations, based on the case of former court rulings, national legislation, and international treaties. On top of these, we italicized the obstacles law enforcement faces in enforcing cybercrime, including jurisdictional issues, evidence gathering, and chain of custody.

A comprehensive legal Implication within innovative technology, field is digital forensics, criminal procedure, evidence law, constitutional law and ethical obligations were completely analyzed. Topical legislative matters were discussed, and we emphasized the need to follow the law when collecting digital evidence. We also talked about the legal and moral concerns surrounding the handling of digital evidence, going over the chain of custody protocols, the method for allowing electronic evidence into court, and the moral implications of forensic investigators' work.

The fields of digital forensics and cybersecurity will always be shaped by new legal concerns that are frequently brought up during cybercrime investigations. Consequently, we make the case for the necessity of developing moral standards for those working in digital forensics as well as the necessity of amending laws to make them stronger. We can make sure that the legal components of cyber security and digital forensics are up to par to meet the demands of an incredibly complex world by putting such a policy into place.

 (ISSN: 2583-7753)