Page 1038 - 1052 **DOI:** *https://doij.org/10.10000/IJLMH.118109*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 4

2024

Cyber Crime and the Challenges of Prosecution and Prevention

JAY KUMAR GUPTA[1] AND URJA LUNIA[2]

ABSTRACT

The swift increase in internet access and electronic transactions in India has raised worries about cybersecurity, which makes it more difficult to prosecute cybercrimes. This essay examines the difficulties associated with prosecuting cyber crimes in India, emphasising important problems such inadequate laws, a lack of knowledge, jurisdictional difficulties, and the quick speed at which technology is developing. Important obstacles include a lack of knowledge about cybersecurity between people and organisations, a manpower deficit, and jurisdictional problems brought on by the international reach of cybercrimes. Also, many of the regulations in place today—such as the Information Technology Act of 2000—are out of date, which means that new laws must be passed on a regular basis to deal with new dangers. Inadequate coordination among diverse law enforcement organisations frequently impedes the success of prosecutions. Insufficient reporting and poor conviction rates are also caused by businesses' unwillingness to disclose cybercrimes for fear of harming their reputation. Cybercrime cases need very complicated investigation, which includes identifying, preserving, collecting, analysing, and presenting digital evidence. Major hurdles include jurisdictional issues, the volatility and ease of change of digital evidence, and the use of encryption and anonymity by hackers. The study emphasises the need for enhanced technology capabilities, strong regulations, and specialised training for legal and law enforcement personnel. The enhancement of cybercrime investigation and prosecution necessitates the investment in contemporary forensic tools, international coordination, and public-private cooperation. Resolving these issues is essential to fostering confidence and trust in India's digital environment, which is critical for the growth of e-commerce and e-governance initiatives.

Keywords*: cybercrime, cyber security, prosecution, technology, enforcement.*

I. INTRODUCTION

India is facing a significant and growing challenge with cybercrime. The number of reported cases is continuing to rise; hence it requires a multi-faceted approach to effectively prosecuting

[1] Author is a student at School of Law, Narsee Monjee Institute of Management Studies, Bengaluru, India.
[2] Author is a student at School of Law, Narsee Monjee Institute of Management Studies, Bengaluru, India.

 [ISSN 2581-5369]

and preventing these crimes.[3] One major hurdle is the lack of cybersecurity awareness[4] among both individuals and businesses which leaves them susceptible to phishing scams, data breaches, and ransomware attacks. Further complicating matters is the ever-evolving nature of cybercrime. Criminals develop new tactics faster than law enforcement can adapt, with emerging threats like deepfakes and cyberterrorism adding to the complexity.

Jurisdictional issues create additional roadblocks. Cybercrime often transcends borders, making investigations and prosecutions difficult due to differing legal systems and the need for international cooperation. Furthermore, the Indian legal framework is considered outdated. The Information Technology Act, the primary legal tool for addressing cybercrime, needs a comprehensive review and update to address the evolving landscape.

To effectively combat cybercrime, India requires a holistic approach. Public and business awareness campaigns are essential to educate people about online threats and preventive measures. Law enforcement and the judiciary need training and capacity building to stay ahead of cybercriminals. The legal framework must be modernized, and international cooperation strengthened to harmonize laws and improve global efforts. Finally, establishing dedicated cybercrime investigation units and digital forensic labs will be crucial for effective investigations and prosecutions. Only through a comprehensive and coordinated effort can India hope to effectively prevent and prosecute cybercrime.

II. ROLE OF E -GOVERNANCE IN CRIMINAL JUSTICE SYSTEM

The widespread availability of affordable computers, mobile phones, and internet access has revolutionized communication and daily life. However, this same technology has created opportunities for criminals and terrorists to exploit it for illegal activities. Cybercrime, encompassing forgery, fraud, hacking, and identity theft, is on the rise, often fueled by a sense of anonymity in the virtual world.[5] While India has implemented the National e-Governance Plan to modernize government operations, there has been less focus on computer forensics and the legal implications of electronic evidence.[6] As e-governance initiatives mature, disputes involving electronic evidence will become more common in both civil and criminal cases. To ensure a robust criminal justice system and a thriving IT industry, India must address the

[3] Growing Cyber Crimes in India: Reasons, Challenges, and Way Forward, OnlyIAS by PhysicsWallah(Accessed on: 30th June, 2024) Available at: https://pwonlyias.com/current-affairs/cyber-crime-in-india/

[4] Cyber Security in India: Challenges and Measures, geeksforgeeks.org (04 Nov, 2022) Available at: https://www.geeksforgeeks.org/cyber-security-in-india-challenges-and-measures/

[5] Rameesh Kailasam, India stares at a steep cybercrime challenge. Is it prepared?, The Indian Express (May 27, 2024) Available at: https://indianexpress.com/article/opinion/columns/india-cyber-crime-challenge-9351602/

[6] CYBER CRIME AWARENESS, Ministry of Home Affairs, PIB Delhi(19 DEC 2023) Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1988265

 [ISSN 2581-5369]

importance of computer forensics and equip law enforcement with the ability to handle electronic evidence effectively. This needs to be balanced with protecting citizens from undue restrictions on their use of technology.[7]

III. COMPUTER FORENSICS AS A TOOL TO COMBAT CYBER CRIMES IN INDIA

Electronic devices are central to cybercrime, either as targets, tools or evidence. Most cybercrimes mirror traditional crimes, but the evidence is electronic or the crime is committed through ICT tools. Even traditional crimes increasingly involve some form of electronic evidence, such as phone records or emails. In India, most cybercrimes are prosecuted under the Indian Penal Code and economic offense laws, with limited use of the Information Technology Act, which allows electronic evidence in court. Cybercrime transcends borders and information warfare is a recognized national security threat. International cooperation, including recognition of foreign computer forensics, is crucial to combat cybercrime. Businesses are often reluctant to report cyberattacks due to fear of bad publicity, lengthy investigations and potential loss of control over their systems.[8] However, this silence emboldens criminals.[9] The rise of cybercrime necessitates reevaluating the criminal justice system to address the impact of technology on crime. Computer forensics, a new field analyzing electronic devices for evidence, is essential in both minor and major crimes. It examines data on devices, networks and storage media to gather evidence for court.[10] This includes examining live and recorded data, identifying speakers, tracing emails, and recovering deleted files. With terabytes of server memory now common, forensics rely on server and router logs, requiring cooperation from network administrators who may be located anywhere in the world. Computer forensics has become a crucial discipline in investigating cybercrime. Unlike traditional crime scenes, cybercrime investigations lack standardized procedures and manuals. Investigators must possess specialized skills to collect and preserve electronic evidence without damaging or altering it. Improper data collection can render evidence inadmissible in court, and investigators risk legal repercussions for unlawful surveillance techniques.[11] The evolving nature of technology further complicates matters, as many investigative tools lack formal validation.

[7] Gupta AK, Gupta MK. E-governance initiative in cyber law making. International Archive of Applied Sciences and Technology. 2012 Jun; 3(2):97-101

[8] Rastogi A. Cyber Law, Law of Information Technology and Internet. 1st ed. Lexis Nexis; 2014. p. 1-17

[9] Legal gaps and concerns abound as cybercrime rises unabated in India, The Economic Times(Jan 1, 2024) Available at: https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/legal-gaps-and-concerns-abound-as-cybercrime-rises-unabated-in-india/106434980

[10] Ashley Brinson, Abigail Robinson, Marcus Rogers, a cyber-forensics ontology: Creating a new approach to studying cyber forensics, Digital Instigation, Elsevier, 2006

[11] Barkha, Mohan UR. Cyber law and crimes. IT Act 2000 and Computer Crime Analysis. 3rd ed. 2011. p. 1-8

 [ISSN 2581-5369]

Cybercriminals, often highly skilled and tech-savvy,[12] actively employ anti-forensic measures to avoid detection. Encryption and other security features create additional hurdles for investigators.[13]

IV. TECHNOLOGICAL DEFICIT IN CYBER CRIME INVESTIGATIONS AND PROSECUTIONS

Securing convictions in cybercrime cases presents unique challenges for the criminal justice system. Unlike traditional crimes, evidence in cybercrime may solely exist electronically, lacking physical proof or eyewitnesses. The burden falls on the computer forensics examiner to ensure the admissibility, authenticity, and reliability of this electronic evidence in court. While India has established computer forensic units, these are often under-resourced, placing a heavy strain on central forensic laboratories. The surge in cybercrimes creates a backlog of cases, further complicated by the need for examiners to appear in court and prepare reports. Delayed forensic examinations can jeopardize prosecutions. To effectively handle cybercrime, a significant expansion of computer forensic labs is necessary. This includes increasing staff, updating equipment, and addressing resource limitations. Without this expansion, prosecuting cybercrime will become increasingly difficult.[14]

The surge in cybercrime cases is threatening to overwhelm the central forensic laboratories in India. To address this growing challenge, a multi-pronged approach is necessary. Firstly, it's crucial for state governments to develop their own cybercrime investigation expertise. This can be achieved by establishing dedicated Computer Forensics Cells at both the district and state levels. These cells would be equipped to handle the initial stages of digital evidence collection and analysis. Secondly, the central forensic laboratories can play a vital role in standardizing the tools and techniques used for digital forensics across the country. This would include standardizing equipment, toolkits, software, and most importantly, the actual forensic examination procedures. This standardization would ensure consistency and reliability of digital evidence collected throughout India. Thirdly, the central laboratories can offer regular certification programs for state government technicians.[15] This certification would equip them with the necessary expertise to conduct digital forensic investigations and ensure their findings

[12] Policing cyber crimes: Need for National Cyber Crime Coordination Centre. 2016. Available from: http://www. orfonline.org/expert-speaks/policing-cyber-crimes-needfor-national-cyber-crime-coordination-centre
[13] Cyber Security in India: Challenges and Measures, geeksforgeeks.org (04 Nov, 2022) Available at: https://www.geeksforgeeks.org/cyber-security-in-india-challenges-and-measures/
[14] Benjamin Turnbull, Jill Slay, Wireless Forensic Analysis Tools for use in the Electronic Evidence Collection, IEEE Proceedings of the 40th Annual Hawaii International Conference on System Sciences-2007 (HICSS'07)
[15] Juneed I. Bilal M. 2017. Cyber crime in India: Trends and Challenges. International Journal of Innovations & Advancement in Computer Science, 6(12): 2347 – 8616

 [ISSN 2581-5369]

are admissible in court. Fourthly, legal amendments are needed to streamline the process of collecting and presenting digital evidence. Law enforcement officers need a wider range of authorized personnel under Section 80 of the IT Act to effectively investigate cybercrime. This would expedite investigations and improve conviction rates. Finally, considering the rapid pace of technological advancement, a Public-Private Partnership (PPP) model could be highly beneficial. The private sector is often better positioned to adapt and integrate new technologies. A PPP could leverage private sector expertise for equipment upgrades, software development, and training programs for law enforcement personnel. This collaborative approach would ensure that India's cybercrime investigation capabilities remain at the forefront of technological advancements. By implementing these measures, India can create a robust and decentralized system for handling cybercrime investigations. This will not only reduce the burden on central forensic laboratories but also expedite investigations, strengthen the legal framework for handling digital evidence, and ultimately lead to a higher rate of successful prosecutions in cybercrime cases.[16]

V. STATUTORY FRAMEWORK OF CYBER CRIMES IN INDIA

The Information Technology Act, enacted in 2000 (IT Act)[17], serves as the cornerstone of India's legal response to cybercrime. This act outlines a range of offenses and corresponding penalties. Section 43[18] specifically addresses damage to computer systems, ensuring accountability for those who disrupt or destroy critical digital infrastructure. Furthermore, Sections 66B[19] to 66D[20] tackle a growing concern – data theft and hacking. These sections encompass identity theft, data breaches, and privacy violations, aiming to protect individuals and businesses from the misuse of their information. Recognizing the potential for cybercrime to threaten national security, the IT Act also includes Section 66F[21].

This section penalizes activities that leverage computer resources to engage in cyberterrorism. Additionally, Section 67[22] prohibits the dissemination of obscene content online, safeguarding users from exposure to inappropriate material. Perhaps most concerning is the proliferation of child sexual abuse content. Section 67B[23] specifically tackles this issue, criminalizing the

[16] Ibrahim M. Baggily, Richard Mislan, Marcus Rogers, Mobile Phone Forensics Tool Testing: A Database Driven Approach, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2
[17] The Information Technology,,Act ,21 OF 2000, Act of Parliament [9th June, 2000.][india]
[18] The Information Technology Act ,S. 43, 21 OF 2000, Act of Parliament [9th June, 2000.][india]
[19] The Information Technology Act ,S. 66B, 21 OF 2000, Act of Parliament [9th June, 2000.][india]
[20] The Information Technology Act ,S.66D, 21 OF 2000, Act of Parliament [9th June, 2000.][india]
[21] The Information Technology Act ,S. 66F, 21 OF 2000, Act of Parliament [9th June, 2000.][india]
[22] The Information Technology Act ,S. 67, 21 OF 2000, Act of Parliament [9th June, 2000.][india]
[23] The Information Technology Act ,S. 66B, 21 OF 2000, Act of Parliament [9th June, 2000.][india]

 [ISSN 2581-5369]

possession and distribution of child pornography. The IT Act, however, is not the only legal framework in place to combat cybercrime. The Indian Penal Code (IPC), a longstanding set of laws, also applies to certain cybercrimes. Sections 292 to 294[24] of the IPC address the distribution of obscene material, mirroring the concerns addressed in the IT Act's Section 67. [25]

Furthermore, Section 354D[26] criminalizes cyberstalking, acknowledging the psychological harm inflicted through electronic harassment. Financial crimes are not exempt from legal repercussions in the digital age. Section 420[27] of the IPC covers online frauds and cheating, ensuring that cybercriminals who exploit others financially face consequences. The IPC also addresses issues like email spoofing (Section 463[28]), defamation through email (Section 499[29]), and various forms of online harassment and intimidation (Sections 503 to 507[30]). This combined approach, utilizing both the IT Act and the IPC, demonstrates India's commitment to a comprehensive legal response to cybercrime. By outlining specific offenses and their corresponding penalties, this framework provides a strong foundation for investigating, prosecuting, and deterring cybercrime, ultimately protecting individuals and businesses in the digital landscape.

VI. CYBER JURISDICTION- NATIONAL, TRANSNATIONAL OR INTERNATIONAL

National jurisdiction applies to cybercrimes when the domestic laws of a country grant its courts the authority to hear the case. This includes defining what constitutes a crime, who is responsible for prosecution, and how punishment is carried out. For instance, offenses under India's Information Technology Act (IT Act) fall under national jurisdiction, with Indian courts empowered to handle them. Cybercrime often transcends national borders, becoming transnational. Imagine a hacker in the USA hacking into a computer located in London and stealing data. In such cases, the crime involves more than one country. International cybercrime also exists, though the distinction between transnational and international crime can be blurry. Critically, cybercrime is not classified as an "International Crime" under the Rome Statute of the International Criminal Court. Several factors contribute to jurisdictional challenges in cybercrime: * Material posted online can be accessed globally. * Websites can be easily relocated from one territory to another. * A website's hosting location might differ from where it targets users. * Different parts of a website can be hosted in separate locations. * Determining

[24] Indian Penal Code, Section 292-294
[25]The Information Technology Act ,S. 67, 21 OF 2000, Act of Parliament [9th June, 2000.][india]
[26] Indian Penal Code, Section 354D
[27] Indian Penal Code, Section 420
[28] Indian Penal Code, Section 463
[29] Indian Penal Code, Section 499
[30] Indian Penal Code, Section 503-507

 [ISSN 2581-5369]

the location of a website or user can be difficult.

(A) Transnational Jurisdiction of Cybercrime

With the globalised world in effect, cybercrime has become internationalised and thus the existing legal frameworks and jurisdictions are facing severe difficulties. We are studying how complex transnational jurisdiction can be where cybercrimes are involved with specific reference to a situation where a person from America hacks a mobile phone belonging to someone from another nation, steals money or personal information. Jurisdiction lines for cybercrimes are blurred at best; thus, any attempt to enforce justice must consider how things stand now and what structures might work better. Legal authorities are authorised to hear cases and carry out legal duties. Because cybercrime has no geographical boundaries and criminals, victims, and affected systems can be located anywhere, jurisdiction issues arise. Because of this, conventional concepts like territoriality, nationality, and the protective principle are unable to adequately handle the complexities associated with cybercrimes.

(B) Current Scenario

There isn't yet a structure for multinational jurisdiction over cybercrime that is widely acknowledged. It is the goal of several international accords as well as national regulations, however they are typically dispersed and uneven. The Budapest Convention on Cybercrime was created by the Council of Europe and it is a major global convention on cyber-crime. It seeks to unify legislation, enhance investigations and encourage collaboration between countries. Nevertheless, its jurisdictional provisions place more emphasis on facilitating cooperation rather than dealing with jurisdictional matters. The Mutual Legal Assistance Treaties (MLATs) makes it easier for nations to work together to gather evidence and enforce international law. Though helpful, MLATs are frequently challenging and sluggish, which makes it difficult to respond quickly in cybercrime instances when time is of the essence. Cybercrime is governed by national laws, however these vary immensely. For example, the United States offers broad jurisdictional claims for cybercrimes involving US people or companies under the Computer Fraud and Abuse Act (CFAA). Different standards and processes may apply in other nations when claiming jurisdiction, though. Judges evaluate whether the CFAA applies extraterritorially to prosecute foreign offenders targeting the United States based on jurisdictional principles (territoriality, nationality, passive personality, universality, or the protective principle) and legislative intent. Computer abuse is an intangible crime that can be started anywhere in the world. For both reasons, the CFAA may be applicable. A Connecticut

 [ISSN 2581-5369]

district court found jurisdiction against a Russian national in United States v. Ivanov[31] because the legislation' intended extraterritorial application was intended by Congress and the negative consequences took place in the United States. The Patriot Act may confer such jurisdiction even if the legislative purpose of the 1996 amendments and the norms of international jurisdictional law do not support the application of the CFAA extraterritorially.[32]

The basic law regulating cyberspace jurisdiction in India is the Information Technology Act of 2000. The legal foundation for governing digital signatures, electronic transactions, and the security and integrity of data throughout the nation is provided by this historic statute. This legislation guarantees that the law applies to acts committed through digital means by giving Indian authorities the authority to look into and prosecute cybercrimes that occur inside its borders. However, because the act's authority is restricted to India, difficulties emerge when handling cybercrimes that cross international borders. The extraterritorial applicability of the act has been explored in order to allay these worries, particularly in situations where Indian people are impacted by cybercrimes committed outside of their nation.[33] In China, International jurisdiction disputes and substantive law are involved in transnational computer criminal jurisdiction.

The fundamental foundations of criminal jurisdiction are challenged by cybercrime's virtual and global character. The goal of Chinese criminal law is to defend China's and its citizens' rights and interests. It is founded on territorial, personal, protective, and worldwide jurisdiction. However, further research is needed to determine how jurisdiction applies to international cybercrime. Cybercrime involving computers falls within the ordinary criminal law jurisdiction. Crimes that occur on Chinese territory, including aboard ships, planes, and embassy premises, are covered by Article 6 of the Chinese Criminal Law. Articles 7, 8, and 9 give jurisdiction over cybercrimes committed overseas by Chinese nationals. This implies that China has jurisdiction over cybercrimes perpetrated by Chinese nationals living overseas, cybercrimes committed by foreigners against Chinese nationals or the state, and cybercrimes covered by international treaties to which China is a party.[34]

[31] United States v. Ivanov, 175 F. Supp. 2d 367, 370 (D. Conn. 2001)
[32] WILLIAM KANE & MELISSA MIKAIL, Extraterritorial Application of the Computer Fraud and Abuse Act, ipwatchdog.com (Accessed on: 03-07-2024) Available at: https://ipwatchdog.com/2020/05/27/extraterritorial-application-computer-fraud-abuse-act-2/id=121826/
[33] Kirtika Sarangi, Issues And Concerns Of Cyberspace Jurisdiction In India,Linkedin(Accessed on: 30-06-2024) Available at: https://www.linkedin.com/pulse/issues-concerns-cyberspace-jurisdiction-india-kirtika-sarangi-vk6qc/
[34] Xiaobing Li , Yongfeng Qin , Research on Criminal Jurisdiction of Computer cybercrime, Elsevier (Accessed on: 30-06-2024) Available at: https://www.sciencedirect.com/science/article/pii/S1877050918306434?ref=pdf_download&fr=RR-2&rr=89d43c9c58c53bbc

 [ISSN 2581-5369]

VII. Case analysis

(A) Hacking from the USA

Imagine if someone in the USA broke into a phone in another nation and took cash or personal data. There are other considerations to consider while determining whether a court or body has jurisdiction. Conventionally, jurisdiction would be claimed by the nation where the crime is committed (i.e., where the phone is hacked). However, since the victim and the criminal are often located in separate places, pinpointing the exact site of a crime can be difficult. Based on the idea that crimes against its citizens, no matter where they are committed, are subject to national jurisdiction, the nation of the victim may assert jurisdiction. The perpetrator's country may claim jurisdiction to defend its national interests if the cybercrime presents a serious harm to that country's security or interests.

VIII. Challenges and proposals

Different laws in different countries can cause problems and complexities in dealing with cybercrimes that happen across borders. Criminals sometimes run away to other countries or use new identities. It's hard to decide who has the right to deal with crimes that you can't touch, like cybercrimes. For example, in the case of United States v. Ivanov, it was tough to decide if a Russian person could be prosecuted for cybercrimes done from another country under the CFAA law. Getting countries to agree on cybercrime laws could help with these problems. It's hard to find out who did a cybercrime and to gather proof from other countries. They need to work together and come up with rules for sharing proof. Making the process for sharing proof faster could really help in dealing with cybercrimes that cross borders. Making special courts for cybercrimes that work internationally could make it easier to deal with cases that cross borders, make it less likely to argue about who has the right to judge, and make sure there's fairness in the law. The ways that are used now to deal with cybercrimes that cross borders aren't always good enough. To really deal with cybercrime all over the world, countries have to work together to make their laws the same, speed up how they work together, and even make special courts for cybercrimes that work internationally. No matter where cybercriminals are or who their victims are, the world can come up with a better and more fair way to deal with them by solving these problems.

(A) Challenges of Prosecuting Cyber Crimes in India

The emergence of the digital age has brought about a substantial change in the criminal scene, leading to the emergence of intricate and advanced cyber crimes. The rapid increase in internet

 [ISSN 2581-5369]

usage and digital transactions in India has made cybersecurity a crucial concern. However, because cyber crimes are so complex, prosecuting them comes with special difficulties, such as insufficient legislation, lack of experience, jurisdictional problems, and technical improvements. Through an analysis of these obstacles, we seek to underscore the necessity of strong regulatory frameworks and improved technological capacities in order to successfully tackle cyber crime in India. There is a lot of debate on the advantages and disadvantages of cybercrime. We face several obstacles in our battle regarding cybercrime. We go over a few of them below.

1. Insufficient knowledge and understanding of cyber security, both personally and within organisations.

2. Inadequately skilled and trained workforce to carry out the actions.

3. Since cybercrimes frequently cross national borders, deciding which jurisdiction is best for prosecution can be challenging. Differing national guidelines and standards add to the complexity of legal processes.

4. Current legislation, such the Information Technology Act of 2000, could not fully address every facet of contemporary cybercrimes. To handle new cyberthreats, the regulatory framework must be updated on a regular basis.

5. Efficient prosecution is hampered by an absence of communication and cooperation between various law enforcement organisations and cybercrime units. Ineffectiveness and delays are frequently caused by overlapping jurisdictions and duties.

6. Compared to other crimes, the state spends little on security, particularly on educating law enforcement, security officers, and investigators in ICT.

7. The baseline requirements for joining the police force do not include any understanding of computers, making applicants virtually ignorant when it comes to cybercrime.[35]

8. Companies that have been the victims of cybercrime, in particular, might feel hesitant to report instances for fear of losing customers' faith and damaging their brand. A smaller percentage of cybercrimes are punished as a consequence of under-reporting.

(B) Evidence Gathering Issues

When it comes to cybercrime, the crime scene isn't just the actual place where electronic gadgets that were intended for targeting or employed in the crime are located. The digital devices that

[35] Gobinda Bhattacharjee, Issues and Challenges of Cyber Crime in India: An Ethical Perspective (Accessed on: 30-06-2024) Available at: https://philarchive.org/archive/BHAIAC.

 [ISSN 2581-5369]

could contain digital evidence are also included in the cybercrime crime scene, which consists of several digital devices, systems, and servers.[36]

Proof collection in the context of cybercrime is a difficult procedure that entails obtaining digital information from a variety of sources like computers, mobile devices, servers. Emails, logs, databases, files, and even social network activities can all include this data. Generally, the procedure goes like this:

1. Identification: Identifying possible digital evidence resources.
2. Preservation: Preserving the evidence means making sure it doesn't get changed or erased. Making a forensic picture of the data is frequently required for this.
3. Collection: Acquiring the information while preserving its integrity. This might entail gathering network activity, file extraction, and data recovery from deletion.
4. Analysis: Looking through the gathered data to locate pertinent details. This may entail metadata analysis, file decryption, and password recovery.
5. Presentation: Arranging the proof for the legal system. To do this, studies and testimony from specialists explaining the technical details to a non-technical audience are created.[37]

In these situations, it is critical to ensure the legitimacy of evidence, which calls for painstaking recording and verification procedures. The chain of custody is essential because it records each action taken with the evidence to ensure that it wasn't tampered with. To ensure the integrity of data over time, hashing uses cryptographic hash functions to create a distinct fingerprint for every piece of data.[38] Furthermore, for digital evidence to remain relevant and in context during the course of the investigation and judicial procedures, precise and trustworthy time stamps are crucial.[39] The existing method for processing digital evidence in cybercrime cases has a number of flaws and difficulties despite strict processes.

The swift advancement of technology frequently surpasses the current legal and procedural structures, resulting in deficiencies in the management of evidence. The integrity of digital evidence can be compromised by its extreme volatility and ease of alteration or deletion—sometimes even accidentally. Due to the frequent cross-border nature of cybercrimes,

[36] Handling of digital evidence, UNODC (Accessed on: 30-06-2024)Available at: https://www.unodc.org/e4j/zh/cybercrime/module-6/key-issues/handling-of-digital-evidence.html
[37] Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.
[38] Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to Computer Forensics and Investigations. Cengage Learning
[39] Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional

 [ISSN 2581-5369]

jurisdictional problems provide logistical and legal difficulties. Furthermore, it is challenging to obtain and attribute data because cybercriminals utilise encryption and anonymity techniques. A lot of lawyers also lack the technical know-how needed to comprehend digital evidence completely and use it appropriately. It is possible to provide a number of helpful recommendations to solve these problems. It is essential to standardise protocols for managing digital evidence across countries through international collaboration.

Judges, attorneys, and law enforcement officials must have specialised training in digital forensics. Keeping up with technological changes may be facilitated by investing in modern forensic tools and methods, such as artificial intelligence and machine learning. It is imperative that legal frameworks be updated with more precise standards regarding the admission and management of digital evidence. Capabilities for investigating cybercrimes can be improved through public-private collaborations. Finally, lowering the frequency of cybercrimes can decrease the amount of digital evidence that has to be processed. This can be achieved by increasing cyber security awareness and education.1[40]

IX. LANDMARK CASE LAWS

(A) Yahoo!, Inc. v. La Ligue Contre Le Racisme[41]

Yahoo!, an American internet company, sued two French anti-racism groups in a US federal court. The dispute arose from interim orders issued by a French court against Yahoo! and its French subsidiary. These orders required Yahoo! to remove content related to Nazi memorabilia from its auction site, accessible to users worldwide. The central question was whether US law allows a foreign nation to regulate speech originating in the US, simply because it can be accessed by internet users in that foreign nation. The court ruled against the French orders, reasoning that principles of international cooperation (comity) don't compel the US to enforce foreign regulations that violate its own constitution. While US courts generally recognize foreign judgments, enforcement cannot happen if it contradicts US interests. In this case, enforcing the French order would infringe upon Yahoo!'s First Amendment rights, protecting freedom of speech. The court acknowledged the validity of the French order under French law and the potential for retroactive penalties. Furthermore, the ongoing threat of enforcement in the US was deemed to have a chilling effect on Yahoo!'s First Amendment rights. With a real and immediate threat established, the court ruled in favor of Yahoo!, declaring the French orders

[40] Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. Computers & Security, 23(1), 12-16

[41] Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme, 433 F.3d 1199 (9th Cir. 2006)

unenforceable in the US.

(B) Microsoft Ireland Case [Microsoft Corp. v. United States][42]

This case centered on drug trafficking evidence stored in the cloud. A US magistrate judge issued a warrant to Microsoft, demanding all emails and information linked to a specific user account. The twist? This user, though a US resident, registered their account in Ireland, and according to company policy, emails were stored on an Irish server. Microsoft complied with the warrant for account information but refused to hand over emails, arguing a US judge lacked authority over data stored abroad. The magistrate judge disagreed and ordered Microsoft to produce the emails. Microsoft appealed, and the case reached the Supreme Court. Adding another layer of complexity, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was passed while the case was ongoing. This act amended a previous law (Stored Communications Act of 1986) and empowered US law enforcement to compel American tech companies, via warrant or subpoena, to disclose user data stored on servers anywhere in the world.

Extra-territorial Jurisdiction – Cybercrimes

India has established a legal framework to determine which courts have jurisdiction over cybercrimes. Two main statutes govern this: the Indian Penal Code (IPC) and the Information Technology Act (IT Act). The IPC's Section 4[43] outlines its extraterritorial application for specific offenses. These include crimes committed by Indian citizens anywhere globally, offenses on Indian registered vessels, and crimes committed outside India that target a computer resource located within India. The IT Act, however, has a wider reach. Section 1(2) extends its application to offenses committed by any person outside India, while Section 75 clarifies jurisdiction for such cases. This section applies if the act involves a computer, computer system, or network located in India, regardless of whether it was specifically targeted. This broader scope stands in contrast to the IPC's focus on targeting a specific Indian computer resource. The Criminal Procedure Code (CrPC) adds another layer by specifying locations for trying specific crimes. Section 179[44] defines jurisdiction based on where the act itself or the resulting consequence occurred. Section 182[45] deals with cheating offenses committed through communication or by fraudulently obtaining property. In these cases, the trial can be held in the jurisdiction where the communication occurred or the property was delivered/received. In

[42] United States v. Microsoft Corp., 584 U.S. ___ (2018)
[43] The Indian Penal Code, Section 4
[44] The Criminal Procedure Code (CrPC), Section 179
[45] The Criminal Procedure Code (CrPC), Section 182

 [ISSN 2581-5369]

conclusion, India's legal framework combines the broader reach of the IT Act with the specific jurisdictional details of the CrPC to ensure effective prosecution of cybercrimes, regardless of where they originate or how they impact Indian computer systems.

Ajay Agarwal v. Union of India (1993)[46] and **Lee Kun Hee & Ors. v. State Of U.P. (2012)**[47], illustrate the concept of jurisdiction in Indian courts for criminal activity involving foreigners. In Ajay Agarwal, an Indian businessman based in Dubai (NRI) conspired with others to cheat a bank in Chandigarh. The Supreme Court ruled that despite the crime being planned abroad, Indian courts had jurisdiction because the consequence, the financial loss, occurred in India. This decision hinged on Sections 179 and 182 of the Criminal Procedure Code (CrPC) which allow trials to be held where the act or its consequence takes place. The Lee Kun Hee case involved a foreign company failing to honor a bill of exchange after an Indian seller delivered goods to an intermediary. Here too, the Supreme Court asserted Indian court jurisdiction based on Section 179 of the CrPC[48]. The court interpreted this section broadly, stating that jurisdiction applies not just to the final act of the crime but also to any actions taken in furtherance of it. In this case, the agreement itself was considered an action furthering the crime of non-payment. This interpretation allows Indian courts to hear cases under Section 4(3) of the IPC[49] (offenses by a person outside India targeting an Indian computer resource) and Section 75 of the IT Act[50] (offenses outside India involving an Indian computer system) The CrPC also has Section 188[51], granting jurisdiction for crimes committed outside India by Indian citizens or on Indian registered vessels. This provision, however, doesn't apply to Section 4(3) of the IPC or Section 75 of the IT Act unless the offender is an Indian citizen. In essence, these cases highlight the interplay between different sections of the CrPC and the broader reach of the IT Act in determining where cybercrimes involving foreign nationals can be tried in India.

X. CONCLUSION

The ICT revolution has undeniably reshaped our social and economic landscape, and the criminal justice system is no exception. As cybercrime becomes increasingly pervasive, a proactive approach is essential to ensure our justice system is adequately prepared. The current state of computer forensics laboratories is a cause for concern. These critical facilities are understaffed and lack the resources necessary to keep pace with the rising tide of cybercrime.

[46] Ajay Agarwal vs Union Of India And Ors 1993 AIR 1637, 1993 SCR (3) 543, AIR 1993 SUPREME COURT 1637
[47] Lee Kun Hee & Ors vs State Of U.P.& Ors AIR 2012 SUPREME COURT 1007
[48] The Criminal Procedure Code (CrPC), Section 179
[49] The Indian Penal Code, Section 4(3)
[50] The Criminal Procedure Code (CrPC), Section 188
[51] The Information Technology Act ,S. 75, 21 OF 2000, Act of Parliament [9th June, 2000.][india]

 [ISSN 2581-5369]

A complete overhaul is urgently needed. Investing in human capital is paramount. Staffing computer forensics labs with highly trained experts is essential. These professionals should possess a deep understanding of digital forensics techniques, data recovery, and electronic evidence analysis. Furthermore, staying abreast of the latest cybercrime trends and advancements in digital technology is crucial. Equipping these labs with cutting-edge technology and software is equally important. State-of-the-art hardware and specialized software tools are vital for efficient and accurate digital evidence collection, analysis, and presentation. The need for modernization extends beyond forensics labs. Law enforcement personnel must also undergo comprehensive training in cybercrime investigation techniques. Understanding digital footprints, online investigative methods, and legal considerations related to electronic evidence is crucial for effective cybercrime prosecution. Public prosecutors also require specialized training. They need the skills to effectively present complex electronic evidence in court and build compelling arguments in cybercrime cases. The ability to translate technical details into clear and understandable terms for judges and juries is paramount. Combating cybercrime isn't just about safeguarding individuals and businesses; it's about fostering the nation's technological development. Failure to effectively address cybercrime will stifle the growth of e-commerce and e-governance initiatives. A robust criminal justice system equipped to handle cybercrime is essential for building trust and confidence in the digital landscape. By prioritizing investment in human capital, cutting-edge technology, and comprehensive training for law enforcement and legal professionals, we can fortify our criminal justice system against the evolving threat of cybercrime. This will not only protect our citizens and businesses but also pave the way for a thriving digital future.

*****

 [ISSN 2581-5369]