FROM FIR TO FORENSIC ANALYSIS IN THE DIGITAL AGE: LEGAL POWERS, INVESTIGATIVE MODELS, AND JUDICIAL OVERSIGHT OF CYBERCRIME POLICING IN INDIA

Bandu B. Meshram[1*], Dr. Manish Kumar Singh[2]

[1]Research Scholar, NIMS, School of Law, NIMS University Rajasthan, Jaipur, (India).*
Email: bbmeshram.jes@gmail.com
[2]Head Of Law Department, NIMS, School of Law. NIMS University Rajasthan, Jaipur, (India),
Email: manishsinghlaw@gmail.com

Corresponding Author:

Abstract

This paper explores the comprehensive cybercrime investigation forensic model employed by Indian police, from FIR registration to forensic analysis of digital evidence. It examines the collection, preservation, and analysis of digital evidence in line with key legislative frameworks such as the IPC, BNS 2023, the Cr.PC, the BNSS 2023,The IEA with the BSA 2023 and the IT Act. This study delineates the empowered role of cybercrime police in executing digital searches, seizures, and offender prosecution under defined legal mandates. Judicial oversight ensures territorial jurisdiction and safeguards the integrity of digital evidence. The paper underscores the integrated nexus between statutory authority, forensic protocols, and judicial scrutiny—forming a resilient legal architecture for cybercrime adjudication. The investigative framework now spans FIR initiation, digital forensics, and court-monitored due process, ensuring lawful, effective, and rights-oriented resolution of digital offenses in India's evolving cyber jurisprudence.

1. INTRODUCTION

The evolution of criminal justice in India has undergone a profound transformation from its colonial origins to its current engagement with the digital age. Rooted in foundational texts such as the Indian Penal Code of 1860 and the Code of Criminal Procedure, first enacted in 1898 and later revised in 1973, the early Indian legal system was tailored to address conventional crimes—those involving physical evidence, eyewitness testimonies, and confessions. These frameworks, developed under British rule, were inherently ill-equipped to confront crimes that transcend physical space and manifest in digital domains.

The rapid expansion of digital infrastructure, the rise of internet-based financial systems, and the ubiquity of smartphones have ushered in complex cyber threats—ranging from hacking and data breaches to online fraud, identity theft, and cyberstalking. Recognizing these emergent dangers, India took its first legislative step into cyberspace with the enactment of the Information Technology Act, 2000. However, as technology evolved and cybercriminals grew more sophisticated, it became clear that isolated statutory responses were inadequate. There was a pressing need for comprehensive reform in both substantive and procedural laws governing cybercrime investigation and prosecution.

In response, India has introduced a new triad of legislation: the Bharatiya Nyaya Sanhita (2023), Bharatiya Nagarik Suraksha Sanhita (2023), and the Bharatiya Sakshya Adhiniyam (2023). These statutes replace their colonial predecessors with a vision aligned to contemporary challenges, including digital evidence handling and cyber forensic investigation. These legal reforms not only redefine criminal conduct and procedural rights but also enhance the state's capacity to detect, prevent, and prosecute cyber offences with technological precision.

Today, cybercrime investigations are anchored in specialized forensic models implemented by cyber cells within the police force. This model begins with the registration of a First Information Report, followed by the collection, preservation, and forensic analysis of digital evidence, and culminates in the identification and prosecution of offenders under judicial scrutiny. Offences are now classified under the Indian Penal Code and the Bharatiya Nyaya Sanhita, while procedures for investigation and trial are regulated by the Code of Criminal Procedure and the Bharatiya Nagarik Suraksha Sanhita. The Information Technology Act remains the backbone of India's cyber jurisprudence, and the Bharatiya Sakshya Adhiniyam governs the admissibility and integrity of electronic evidence.

Digital forensics now serves as the fulcrum of evidence-based cyber policing. Devices, servers, and logs are treated as crime scenes, requiring meticulous examination by trained personnel. At every stage, judicial authorities exercise vital oversight, ensuring territorial jurisdiction, legal compliance, and protection of fundamental rights. Together, these advancements illustrate a dynamic shift in India's legal and forensic landscape—one that integrates historical legal wisdom with cutting-edge technology to uphold justice in the digital era.

2. THE CYBER CRIME INVESTIGATION FORENSIC MODEL USED BY POLICE

The specific sections and laws involved in the cybercrime Police administration & investigation process[1], may differ based on the type of cybercrime or the particular cyber offense involved and the jurisdiction in which the investigation takes place (location) and any recent changes in relevant laws or regulations.

[1] The Police Act 1861

2.1 Cyber Crime FIR and Police Investigation

As per Section 78 of the ITA, 2000, as amended in 2008, any offense under this Act shall be investigated by a police officer not below the rank of Inspector. However the authority under Cr.PC (BNSS 2023)such as a constable or any police officer in charge will have a power to arrest.

The activities performed by the cyber police during the investigation of cybercrimes, from the registration of the FIR to the preparation of the charge sheet, involve several steps[2,3]

Registration of First Information Report (FIR): The police will register an FIR based on the complaint[4]. The FIR is a formal document that initiates the investigation and includes details such as the nature of the cybercrime, the identity of the injured party, and a brief description of the incident.

(Cr.PC - Section 154 and BNSS, -Section 173) **:**The cybercrime investigation starts with the registration of an FIR at the concerned police station or Cyber Crime Investigation Cell (CCIC) or Cyber Crime Unit (CCU). If an initial inquiry indicates a cognizable cybercrime, the police register an FIR under Section 154 of the CrPC and Section 66 of the IT Act.". The FIR includes details of the offense and parties involved, initiating the formal investigation. Complainants must highlight both provisions when reporting cybercrimes.

(iii)Initial Examination and Collection of Evidence: The investigating officer will conduct an initial examination to determine the nature and scope of the cybercrime. Evidence related to the offense, such as log files, digital devices, online communications, and other relevant data, will be collected and preserved following the proper chain of custody. The police conduct a preliminary inquiry, interview the complainant, gathering evidence, and assessing the offense's severity. For cognizable offenses, they apply Section 2 and 154 of the CrPC (Section 173 BNSS 2023)for collection of information in oral or in written from informant in cognizable cases. "As per Section 78 of the ITA 2000, only officers holding the rank of Inspector or higher are authorized to conduct investigations in such cases." Preliminary Investigation is done under Cr.PC - Section 156: After the FIR is registered, the investigating police officer has a power to starts the preliminary investigation; investigate cognizable offenses of the cybercrime. They may collect preliminary information and evidence related to the case[5].

(iv)Expert Involvement for Tracing online Activity and Identifying the Perpetrator: Cybercrime investigations often require specialized technical expertise. Forensic experts and cyber security professionals may be involved in analysing digital evidence, tracing IP addresses, and recovering data from digital devices. The investigating team will work to trace and identify the perpetrator(s) behind the cybercrime. This may involve obtaining information from service providers and conducting online surveillance. Police track offenders' online activity such as digital footprints, including IPs, emails, and social media, using electronic evidence under Section 3 of the Evidence Act(Section 2 of Bharatiya Sakshya Adhiniyam 2023(BSA 2023) .The police officer (IT Act -. Sec 78) may collaborate with Internet Service Providers (ISPs), cyber forensic experts or other agencies to gather this information(The evidence Act -Sec 45, 45A & 46 which are parallel to section39(1), 39(2) & 40 of BSA 2023. In the context of cybercrime investigations under Section 91 of the Cr.PC[6], the police may approach ISPs to obtain subscriber information, IP logs, access logs, or communication records, or any other relevant data that can assist in identifying and apprehending cyber criminals. Under Section 69B,IT Act[7], authorized agencies & forensic laboratories by Indian government, including the police, can seek cooperation from ISPs to intercept, monitor, or decrypt information generated, transmitted, received, or stored in any computer resource related to cybercrimes.

(v) Examination of Witnesses: Witnesses, victims, and suspects may be interviewed to gather additional information and evidence related to the cybercrime. As per–Cr.PC - Section 160(BNSS Sec179,), Section 161(BNSS Sec180,), The investigating officer may examine witnesses who have information about the cybercrime or are victims of the offense. Section 160: This section allows the police officer to summon witnesses for attendance of witnesses during the examination for investigation. Section 161: This section deals with the questioning of witnesses and examination of witnesses by the investigating officer during the investigation.

(vi)Suspect Identification and Arrest: Based on the evidence gathered, the police identify and locate the suspects involved in the cybercrime. They follow legal procedures to effect arrests, if required, and present the suspects before the appropriate judicial authority. The identification and arrest of a cyber criminal in India is primarily governed by the provisions of the CrPC- Section 41 of the CrPC(Section-35BNSS) and Section 75 of the IT Act, 2000.

(vii)Charge Sheet Submission: Once the investigation is complete, and the police have gathered sufficient evidence, a charge sheet (also known as a final report or police report) is prepared. The charge sheet includes a detailed account of the investigation, the evidence collected, and the sections of the law under which the accused should be charged. The preparation of Charge Sheet is done as per Section 173(2) Cr.PC(Section-193 BNSS) which state that Once the investigation is complete, and the police have gathered sufficient evidence, a charge sheet (final report) is prepared.. The charge sheet includes a detailed account of the investigation, the evidence collected, and the sections of the laws (IPC and IT Act) under which the accused should be charged.

---

[2] Ratanlal and Dhirajlal, The Code Of Criminal Procedure, Eastern Book Company , 15th edition 2018.

[3] S C Sarkar, P C Sarkar, Sudipto Sarkar ,The Code of Criminal Procedure (In 2 Volumes) , 12th Edition, 2018, LexisNexis

[4] Dr. Gupta and Agrwal , Cyber Laws, Premier Publishing Company, 2023

[5] Gerard Johansen , Digital Forensics and Incident Response, Birmingham - Mumbai Copyright © 2017 Packt Publishing

[6] Criminal Procedure code 1973, Bare Act, 2019: Section 91 in The Code of Criminal Procedure, 1973: https://indiankanoon.org/doc/788840/

[7] Section 69B in The Information Technology Act, 2000: https://indiankanoon.org/doc/100506284/

(viii) **Case Documentation & Submission of Charge Sheet to the Court :** The police prepare a charge sheet based on a comprehensive investigation report that includes evidence, witness statements, and forensic analysis. As per Section 173 Cr.PC (Section 193 BNSS)**,** this final report is submitted to the Magistrate. Under Section 207 Cr.PC (Section 230 BNSS**)**, copies of all relevant documents and statements must be provided to the accused. The charge sheet forms the basis for trial proceedings by presenting a detailed summary of the investigation.

(ix) Judicial Proceedings: **Judicial Proceedings**: Upon submission of the charge sheet, the court initiates trial, examining evidence and hearing arguments. It applies relevant laws including the IT Act, DPDP Act, BSA 2023, BNS 2023, the Specific Relief Act, and other applicable statutes before delivering a verdict[8].

2.2 Collection Of Digital Evidence (Search & Seizure)

Depending on the nature of the cybercrime, the investigating officer may collect digital evidence[9] such as log files, emails, chat records, IP addresses, website data, social media posts, and any other relevant electronic data. The specific sections of the Cr.PC (BNSS-2023), IPC(BNS-2023) and the IT Act that are relevant for collecting digital evidence are as below: (i)Criminal Procedure Code (Cr.PC) : The Cr.PC lays down the procedure for search and seizure under section 91 to 103[10]. Key CrPC Sections for Search & Seizure of Digital Evidence are (i)Section 91 Cr.PC (Section 94 BNSS): Enables police or court to compel any person, service provider, or entity to produce electronic records or digital devices relevant to an investigation.**(ii)**Section 92 Cr.PC (Section 95 BNSS) Allows authorized access to telecom or postal records, such as emails and call logs, through a Magistrate or higher authority's order.(iii)Section 100 Cr.PC (Section 103 BNSS): Permits lawful entry, search, and seizure of digital devices like mobiles and computers under a warrant, especially in cybercrime cases.(iv)Section 165 Cr.PC(Section 185 BNSS) – Empowers police to conduct immediate searches and seize digital evidence without a warrant when delay may hinder investigation.

However procedure under Cr.PC is inadequate in respect of computer cybercrimes for search and seizure of devices, volatility of computer files or digital evidence. In effective investigation and evidence collection, When the court issues summons or a search warrant under Section 93 Cr.PC(*Section 96 BNSS 2023*)) or when the investigating officer directs by a written order, section 91 CrPC directs "duty to surrender sizable objects "which obligates a person having the document or any such matter to surrender it while "the duty to testify for active cooperation" under section 100(1) CrPC(Section 103 BNSS 2023) confers a duty upon a person in charge of a place where the investigation is carried out to provide access to such place and to help officers in all manner.

Section 93 of the Cr.PC.(Section 96 BNSS 2023) states that the warrant issued may authorize the seizure of computer devices or parts thereof, followed by a comprehensive forensic analysis of all records and data stored on the device. However, this may infringe upon the right to privacy; as such devices may contain data related to trade secrets, records of other economic activities, or personal information, including videos and images.

Section 99 of the CrPC (Section 102 BNSS 2023) : Directions Regarding Search Warrants**:** Section 99 of the CrPC states that search warrants issued under Sections 93, 94, 95, and 97(ie . Section 96, 97,98, and 100 of BNSS 2023 respectively) must adhere to the provisions outlined in Sections 38, 70, 72, 74, 77, 78, and 79, (ie Section 32,72,74,79, 81 of BNSS 2023 respectively) wherever applicable. These provisions ensure that search warrants are legally valid, properly executed, and conducted within the framework of procedural law. In the context of cybercrime investigations, these sections play a crucial role in governing how search operations involving digital evidence, online data, and electronic devices are carried out.

Section 38 CrPC – Forms(Section 32 BNSS 2023 **) :**This Section prescribes the standardized forms that should be used in various legal proceedings, including search warrants. This section ensures that official documents follow a consistent structure, preventing ambiguities and procedural errors.

In cybercrime cases, this provision ensures that search warrants for electronic devices, cloud storage, and digital records are correctly documented, reducing the risk of legal challenges due to improper formatting or missing details.

Section 70 CrPC – Form and Contents of Warrant of Arrest (Section 72 BNSS 2023) **:** Section 70 lays d o wn the essential elements that must be included in an arrest warrant, such as the suspect's identity, the specific offense, and authorization by a competent court. This section ensures that the warrant is legally binding and properly structured. In cybercrime cases, where offenders operate anonymously or across multiple locations, having a clear and detailed arrest warrant is critical to ensuring lawful apprehension of hackers, cyber fraudsters, and other digital criminals.

Section 72 CrPC Warrants to Whom Directed (Section 74 BNSS 2023) **:** Section 72 specifies the individuals or authorities responsible for executing a warrant, including law enforcement officers or designated officials. It clarifies the chain of command in enforcing judicial directives.

Given the technical nature of cyber investigations, this section ensures that search warrants are executed by trained cyber police officers, digital forensic experts, or specialized agencies, thereby maintaining the integrity of electronic evidence.

Section 74 CrPC Warrant Directed to Police Officer (Section 76 BNSS 2023) **:** Section 74 mandates that a search or arrest warrant should typically be directed to a police officer unless specified otherwise by. the court. In digital crime

[8] Pavan Duggal, Cyberlaw: The Indian Perspective, *4th ed., Saakshar Law Publications, 2021, Chapter on Cybercrime Investigation and Judicial Proceedings*.

[9] Bandu B. Meshram , Manish Kumar Singh, Cyber Crime Detection Methodology & Tools: An Experimentation Research, 3rd International Conference on Advances in Science, Engineering & Management

[10] S.N. Mishra*: Criminal Procedure Code*, Central Law Agency, Year: 2020, section 91 to 103

investigations, this provision ensures that only officers with the requisite cyber expertise handle the execution of warrants, ensuring proper seizure and handling of digital devices without compromising forensic evidence.

Section 77 CrPC Warrant May Be Directed to Any Person (Section 79 BNSS 2023) **:**This Section allows a warrant to be executed not just by police officers but also by other authorized individuals when necessary. This flexibility is particularly useful in complex investigations requiring specialized intervention. Cybercrime cases often require collaboration with IT professionals, cyber security experts, and forensic specialists. This section enables courts to direct search warrants to qualified experts who can assist law enforcement in tracking digital footprints, decrypting data, or retrieving deleted files.

Section 78 CrPC : Warrant Forwarded for Execution Outside Jurisdiction (Section 80 BNSS 2023)**:** This Section permits a search warrant to be executed in another jurisdiction by forwarding it to the relevant law enforcement authority in that area. This provision is essential in handling crimes that extend beyond a single region. Given the borderless nature of cybercrimes, offenders often operate from different cities, states, or even countries. This section facilitates cross-jurisdictional cooperation, ensuring that cybercriminals can be investigated and apprehended even if they operate outside the investigating agency's geographical limits.

Section 79 CrPC Warrant Directed to Multiple Persons (Section 81 BNSS 2023)**:** Section 79 allows a warrant to be executed by multiple officers or authorities simultaneously when the situation demands. Cybercrime investigations often involve multiple suspects, data servers in different locations, or large-scale financial frauds. This provision enables coordinated raids and searches across multiple locations, ensuring efficient evidence collection in cases like hacking, online scams, and digital money laundering.

Search Warrants in Cybercrime Investigations : Sections 93, 94, 95, and 97 of CrPC(Section 96 , 97, 98, 100 of BNSS 2023respectively)

Section 93 CrPC When Search Warrant May Be Issued(Section 96 BNSS**) :**Section 93 empowers a court to issue a search warrant when it believes that specific documents, records, or electronic evidence are relevant to an on going investigation. The search can be conducted at any place where such evidence is suspected to be stored. This section is frequently used in cyber investigations to obtain search warrants for electronic devices, cloud servers, social media accounts, and encrypted databases. Law enforcement agencies rely on this provision to access crucial digital evidence in hacking cases, ransom ware attacks, and data breaches.

Section 94 CrPC Search of a Place Suspected to Contain Stolen Property or Forged Documents(Section 97, BNSS **):** Section 94 permits law enforcement to search premises that are suspected of storing stolen or counterfeit materials, including forged documents.

This provision is particularly significant in cases of identity theft, fake digital certificates, and fraudulent financial transactions. Cybercriminals often store stolen personal data, credit card details, or counterfeit digital identities, making this section vital in cyber fraud investigations.

Section 95 CrPC : Power to Declare Certain Publications Forfeited (Section 98 BNSS) **:** Section 95 grants the government the authority to seize, prohibit, or forfeit any objectionable publication that poses a threat to public order. This section is applied in cases involving online hate speech, fake news propagation, child pornography, deep fake content, and other illegal digital publications. It enables authorities to take down harmful online content and block access to malicious websites.

Section 97 CrPC – Search for a Person Wrongfully Confined(Section 100 BNSS)**:** This Section empowers a court to issue a search warrant to rescue an individual who is believed to be unlawfully confined in any location. This section is applicable in cases involving cyber trafficking, online blackmail leading to physical confinement, and instances where individuals are lured into captivity through digital deception, such as honey trapping or sextortion.

Section 99 of the CrPC ensures that search warrants in cybercrime cases are executed with proper legal safeguards, preventing unauthorized searches and ensuring electronic evidence is collected lawfully. The referenced sections provide a robust legal framework that enables law enforcement to investigate, track, and prosecute cybercriminals effectively while adhering to due process. By integrating these procedural laws into digital forensics and cyber investigations, authorities can enhance their ability to combat cyber threats, maintain legal integrity, and strengthen cyber security governance.

According to Section 100 of the Criminal Procedure Code (Cr.P.C.), individuals in charge of a closed location must permit the officer or person executing the warrant to enter freely and provide reasonable facilities for conducting a search. If such individuals refuse or neglect, without reasonable cause, to attend and witness the search, they shall be considered to have committed an offence under Section 187 of the IPC. .Section 101 of the Cr.P.C. addresses the disposal of items discovered during a search that falls beyond jurisdiction. Section 102 empowers police officers to seize certain properties, while Section 103 allows a magistrate to order that a search be conducted in their presence.

(ii)Indian Penal Code (IPC) In Investigation And Evidence Collection: In the context of cybercrimes, Sections 91, 102, of the Indian Penal Code (IPC) (ie Sections 29,40 of BNS 2023) play a crucial role in investigation and evidence collection[11], [12].

Section 91 IPC – Summons for Documents & Evidence (Sections 29, BNS 2023)**:** Section 91 IPC allows the police to issue a summons to any person in possession of documentation or materials or any other evidence or any other aspects critical for the investigation. This provision allows law enforcement to summon individuals or entities in possession of

[11] The Indian Penal Code, Bare Act 2018

[12] Suresh T Viswanathan , Bharat's The Indian Cyber Law with The Information Technology Act 2000 , Aggarwal Law House E-Solutions, Delhi- 110002 Edition 2022.

crucial documents, electronic records, or other materials necessary for an investigation. In cybercrime cases, this can be used to compel internet service providers (ISPs), financial institutions, social media companies, or cloud service providers to provide logs, transaction details, chat records, emails, or other digital evidence that may be critical in identifying cybercriminals and their activities.

Section 102 IPC – Seizure of Property (Section 40 of BNS 2023**):** Section 102 of the IPC grants authority to law enforcement officers to confiscate any asset that is either linked to a criminal act or has the potential to be utilized in the commission of a crime. Law enforcement agencies can use this provision to seize digital assets linked to cyber offenses, such as hacked computers, unauthorized databases, crypto currency wallets used for fraud, malicious software, and other electronic devices involved in cybercrimes. For example, if a suspect is involved in a hacking or financial fraud case, police can confiscate their hard drives, mobile phones, or servers to retrieve evidence.

(iii) IT Act, 2000 : ITA provide Judicial recognition for electronic data interchange and electronic communication transactions and main act about digital signature recognition, hacking, cybercrime punishment and regulations[13],[14]. Section 69 grants the government the authority to intercept, oversee, or decrypt any data produced, transmitted, received, or stored within any computer resource for the purpose of enhancing cyber security. Cybercrime cooperation extends across intra-state, inter-state, and international levels. Under Section 69B of the ITA 2008, the Central Government can authorize agencies to monitor and collect traffic data from computer resources to enhance cyber security and prevent unauthorized intrusions or malware threats. Section 79A requires intermediaries, such as internet service providers (ISPs), to provide assistance and cooperation to government agencies in the investigation of cyber offenses. Section 79B mandates intermediaries to preserve and retain necessary information as per the rules and regulations for the purpose of investigation. Section 80: This section grants powers to police officers to enter any community area or civic location and conduct searches and arrests without a warrant in certain circumstances.

2.3 Identification And Prosecution Of Cybercrime Offenders

Depending on the specific offenses committed, relevant sections of the CrPC(BNSS 2023), IPC (BNS 2023) and IT Act are used to identify and charge the accused.

(i)For Identifying And Prosecuting Cybercrime**: Cr.PC (BNSS 2023)** Each relevant section of the CrPC in the context of identifying and prosecuting cybercrime offenders in India:

(i) Section 154 CrPC-(Section 173 BNSS 2023):Information in Cognizable Cases: requires law enforcement to formally document a First Information Report (FIR) upon receiving details of a cognizable cyber offense. Upon receiving a complaint, such as one involving phishing or unauthorized online transactions, the police are required to document the details and initiate an investigation without delay.

(ii)Section 155 CrPC (Section 174-BNSS 2023**)**- Information in Non-Cognizable Cases: In cases where the cybercrime is classified as non-cognizable, law enforcement officials are required to secure a warrant from the judicial authority before proceeding with any arrest, the information is recorded in the general diary, and the police must seek permission from a Magistrate to investigate further. For example, in cases like online defamation or minor cyber offenses, the police would need judicial approval to proceed with an investigation.

(iii) Section 156 CrPC (Section 175-BNSS 2023) :(Police Officer's Power to Investigate Cognizable Cases) authorizes law enforcement to probe cognizable cyber offenses without prior approval from a Magistrate. In cases of hacking or unauthorized system access, officers can promptly initiate investigations, gather digital evidence like access logs, and analyze system activity records.

(iv) Investigation Procedure**:** Section 157 CrPC (Section 176-BNSS 2023): Once the FIR is lodged, the police are obligated to initiate the inquiry by inspecting the location of the offense, questioning potential witnesses, and gathering relevant evidence. In a cybercrime scenario, this might involve retrieving and analyzing digital data from computers, servers, or mobile devices linked to the crime.

(v)Section 165 CrPC (Section 185-BNSS 2023) - Search by Police Officer: This section authorizes the police to conduct searches in locations where they believe evidence related to a cybercrime might be found. For instance, if the police suspect that incriminating data is stored on a suspect's personal computer or a remote server, they can conduct a search to seize the necessary evidence.

(vi) Procedure for Delayed Investigation : Section 167 CrPC (Section 187 of BNSS 2023)**:** If the inquiry remains incomplete within 24 hours, law enforcement must obtain judicial authorization to prolong the suspect's custody. If the police cannot complete the investigation within the mandated 24 hours, they must produce the suspect before a Magistrate who can authorize further detention. In cybercrime cases, having encrypted data or international elements, the investigation may require extended time for the police to gather and analyse evidence.

(vii) Police Officer's Report: Section 173 CrPC (Section 193-BNSS 2023) **:-** Upon concluding the investigation, the police must file a conclusive report commonly known as a charge sheet, to the Magistrate under this section. This report details the findings of the investigation, including all collected evidence and the charges being brought against the accused, such as in a case of cyber fraud.

(ix) Section 207 CrPC (Section 230-BNSS 2023): **Furnishing of Police Report and Other Documents to the Accused**: The accused has the right to receive copies of the charge sheet, FIR, and other documents collected during the investigation

[13] The Information Technology Act of 2000/2008

[14] Surendra Malik , Sudeep Malik, Supreme Court On Information Technology Act Internet And Cyber Laws And Aadhaar 1950 To 2019, Eastern Book Company, January 2020

under this section. In a cybercrime case, the accused would be provided with access to the digital evidence the prosecution plans to use, such as emails, transaction records, or logs.

(ii) Offences under IPC (BNS 2023) : Some common IPC sections or BNS 2023 used in cybercrime investigations to charge the accused include :Cheating and fraudulently inducing someone to transfer property under Section 420 **IPC (**Section 318(4) BNS 2023) is punishable. Similarly, breach of entrusted property falls under Section 406 IPC **(**Section 316(2) BNS 2023)**.** Any act of forgery or creating false documents to deceive, under Section 463 and Section 464 IPC respectively **(**Section 336(1) BNS 2023 **&** Section 335 BNS 2023 respectively), is criminalized, and penalties are outlined in Section 465 IPC(Section 336(2) BNS 2023). When forgery is committed for the purpose of cheating, it is addressed under Section 468 IPC (Section 336(3) BNS 2023), while forgery aimed at tarnishing someone's reputation falls under Section 469 IPC **(**Section336(4) BNS 2023)**.** Using a falsified document as genuine is prohibited by Section 471 IPC (Section 340(2) BNS 2023)**.** Threatening someone with criminal intimidation is addressed by Section 503 IPC (Section 351(1) BNS 2023), and any words, gestures, or actions meant to offend a woman's dignity fall under Section 509 IPC **(**Section 79 of BNS 2023). Lastly, defamation, whether in spoken or written form, is punishable under **Sections 499** IPC (**Section 356(1)** BNS 2023) and defamation is punished under 500 **IPC (**Section 356(2) BNS 2023) and Section 506 IPC (**Section 351(2)(3)** BNS 2023) deals with punishment for Criminal intimidation.

Punishments under IPC or BNS for cybercrimes : The list the cybercrimes and punishment for it is recognized by different sections of IPC as given below[15],[16]:

(i) Section 292 IPC(Section 294 BNS): Punishment for the sale, distribution, or public display of obscene material, including sexually explicit content.

(ii)Section 294 IPC(Section 296 BNS): Punishment for obscene acts or songs in public places, including online platforms.

(iii)Section 354D(Section 78 BNS)): Punishment for stalking a person through electronic communication, such as sending threatening messages or engaging in unwanted surveillance.

(iii) Section 383 IPC(Section 3078(1) BNS): Punishment for Online Extortion and Blackmail, including threatening to harm the reputation of an individual or cause damage to their property using online communication.

(iv) Section 416 IPC(Section 319(1) BNS): Punishment for impersonation with fraudulent intent, including pretending to be another person online to commit fraud.

(v) Section 419 IPC(Section 319(2) BNS): Punishment for cheating by personation, including the identity theft & fraudulent impersonation of another person with the intent to deceive and cheat. In the context of cybercrimes, this applies to cases involving identity theft, phishing, fake social media profiles, and deepfake frauds, where offenders impersonate individuals to commit financial or social deception

(vi) **Section 420** IPC(Section 318(4) BNS): Penalty for deceit and dishonestly obtaining property via the internet, digital platforms, or electronic fraud which extends to online frauds, e-commerce scams digital payment frauds, crypto scams, and phishing attacks.

(vii)Section 499 IPC(Section 356(1) BNS): Defamation or Online Harassment and Section 500 IPC: Punishment for defamation, including making false statements to harm the reputation of an individual or entity through online means. and Section 500 IPC (Section 356(2) BNS) decides punishment for defamation.

(viii) Section 509 IPC **(Section 79 BNS)** addresses actions that are intended to insult or online harassment and insults or harm the modesty of a woman through online means electronic communication.

These sections, among others, empower law enforcement agencies to investigate and prosecute cyber criminals effectively.

(iii) Offences under ITA 2000

The ITA 2000 provides statutory validity to online dealings and electronic authentication with digital signature, while defining cyber offenses and penalties to regulate, investigate, and prevent cybercrimes, ensuring digital data protection and privacy. Key sections address cybercrime investigations.

(i) Section 43 imposes penalties for unauthorized access to computer systems, while Section 43A provides for compensation/ restitution in cases of failure to adequately Safeguard Information.(ii) Section 65 addresses the offense of manipulating digital records.

(iii) Section 66 outlines penalties for Online criminal activities, including hacking, unauthorized access to computer systems, data tampering, and the introduction of viruses or malware.(iv) The Supreme Court of India held that prosecution under Section 66A of the IT Act, 2000, is impermissible, as the provision was struck down as unconstitutional in the landmark Shreya Singhal judgment (2015)**.**

(v) Section 66B prescribes penalties for knowingly possessing or dealing in stolen digital assets, computer resources, or communication devices with dishonest intent.

(vi) Section 66C penalizes the fraudulent acquisition and misuse of digital credentials, personal data, or authentication information, including unauthorized access to financial records, stolen credentials, software piracy, SIM swap fraud, database breaches, and other cyber offenses involving the illicit use of digital identities and computer resources.

.(vii) Section 66D outlines penalties for "fraudulent identity misuse" refers to offenses like phishing, identity theft, deepfake scams, and account takeovers**,** where criminals impersonate individuals to deceive victims, steal data, or commit financial fraud. (viii)Section 66E addresses the offense of violating an individual's privacy.(ix) Section 66F defines the crime of cyber terrorism.(x) Sections 67 and 67A impose penalties for publishing or transmitting sexually explicit content, including child pornography, through electronic means.(xi) Section 67B prescribes penalties for creating, sharing, or

[15] Ratanlal & Dhirajlal ,The Indian Penal Code 36th Edition, Lexis Nexis July 2019

[16] Sharma RK. Legal framework against cybercrime in India. Indian J Criminol. 2023;51(1):45-59.

distributing digital content featuring minors in sexually exploitative acts, including possession, transmission, or circulation of child sexual abuse material (CSAM) in electronic form.
(xii) Section 70 addresses the destruction or incapacitation of critical information infrastructure.(xiii) Section 72 prescribes penalties for unauthorized disclosure, misuse, or compromise of confidential information and personal data, violating privacy rights and data protection norms.
(xiv)Section 72A establishes punishment for the unauthorized disclosure of information in violation of lawful contracts.(xv) Section 73 outlines penalties for publishing false particulars in electronic signature certificates.(xvi) Section 74 addresses penalties for publications made for fraudulent purposes.

2.4 Preservation of Digital Evidence

The preservation of digital evidence is typically carried out using
(i)Section 102 Cr.PC(Section 106 BNSS & Section 94 BNSS – Power to seize certain property): Authority of a police officer to confiscate specific property, applicable for the seizure and safeguarding of digital evidence. This includes digital devices (e.g., mobile phones, hard disks) if suspected to contain evidence
(ii) Under Section 69, 69A, 69B**, and** Section 76**,** digital evidence can be seized, intercepted, or confiscated as per lawful procedure. Section 84A ITA: The Central Government shall establish guidelines or techniques for cryptography to ensure secure usage of digital communication system and to enhance digital governance and online commerce.
(iii)Section 39 of the Indian Evidence Act (Section 33 BSA 2023) grants the police the authority to seize documents and preservation of electronic evidence or electronic records during the investigation.
However, standard investigative procedures, chain of custody protocols, data authorization and authentication, hashing techniques, and specialized forensic tools used by experts are not explicitly defined or mandated under existing cyber laws.

2.5 Forensic Analysis and Examination(FAE) Of Digital Evidence

During the forensic analysis, the forensic expert follows proper chain of custody protocols to preserve the digital evidence to ensure its authenticity, integrity, credibility, admissibility and relevance of electronic evidence in court. The forensic analysis depends on the specific cyber offenses being investigated.
(i)FAE using Cr.PC - Section 293:(i) Section 293 Cr.PC (Section 329 BNSS): Use of Government scientific/digital forensic expert reports in court proceedings. The forensic expert is called upon to analyse the digital evidence collected during the cybercrime investigation.
(ii) **FAE using ITA 2000:**(i) As per Section 2(t) of the IT Act, 2000, an "electronic record" encompasses any digitally stored, processed, or transmitted data, including multimedia content such as audio, images, and video, as well as microfilm and computer-generated microfiche. (ii)Section 6. IT Act 2000 Use of electronic records and electronic signatures for authenticity in Government and its agencies. (iii) Section 79A of the IT Act empowers the Government of India to appoint any institution, body, or agency under the Central or State Government as an Authorized Examiner of Digital Evidence for submission before a judicial body or competent authority.(iv) Section 79 IT Act 2000: providing immunity to intermediaries, but they do not specifically cover the detailed process of analysis and interpretation of digital evidence.
(iii) FAE using IEA 1872 Vs. BSA 2023 : In cybercrime investigations, expert opinion becomes crucial in interpreting complex digital evidence.(i) Section 45A of the IEA(39(2) BSA) allows for the opinion of examiner of electronics evidence/consultant's recommendation / expert testimony to be admitted as evidence on matters related to electronic records. Courts may solicit expert testimony from certified specialists to evaluate the technical complexities of cybercrimes, digital forensics, and the integrity and admissibility of electronic evidence during legal proceedings[17]. (ii) Section 65A IEA(Section 62 BSA) sets the foundation for the admissibility of electronic evidence, requiring compliance with prescribed conditions under section 65 B IEA(Section 63 BSA) instead of traditional document evidence rules and (iii) Section 65B IEA lays down mandatory conditions for the admissibility of electronic records in legal proceedings. such as computer outputs, as secondary evidence. Section 65A mandates that electronic evidence be substantiated by a digitally authenticated certificate in the legally prescribed format, duly signed by an authorized officer holding a position of accountability within the relevant authority, to ensure its authenticity, integrity, and evidentiary admissibility in cybercrime prosecutions. (vi) Section 60 IEA's((Section 55 BSA)) hearsay rule for oral evidence, generally disallows the admission of hearsay evidence, i.e., statements made by individuals who are not available for cross-examination. However, Section 65B(4) IEA's(Section 63 BSA) carves out an exception to the hearsay rule for admissibility of electronic records. Electronic records containing statements of a person who is unavailable to testify is permissible as evidence provided the criteria established in Section 65B(2) and (3) are satisfied. This exception recognizes the challenges of obtaining direct testimony in cybercrime cases and allows for the introduction of electronic statements that meet the prescribed conditions. (vii) Section 65B(2) outlines the conditions for the permissibility of digital evidence, highlight or stress the importance of a particular requirement to establish that the information was produced by a computer during the regular course of its operation, and that the computer-generated data and electronic evidence is authenticated , untampered accurate(Integrity) and reliable. Courts often rely on digital forensics experts to verify the chain of custody and ensure that electronic evidence is reliable.
(iv)identify the perpetrator(s) : The cyber police work to trace and identify the perpetrator(s) behind the cybercrime and may use various techniques such as IP address tracing, the Geolocation of cyber attacker online surveillance, and data analysis.

[17] Indian Evidence Act of 1872, Kamal Publishers, New Delhi

(i)The CrPC provides guidelines for the *arrest and custody* of suspects involved in cybercrimes. Section 41 details the conditions under which arrests can be made, while Section 57 addresses the duration of detention. Section 41 and Section 57 protect the rights of peoples suspected of cybercrimes and facilitate the effective investigation and prevention of further offenses.

(ii) Section 46(2) CrPC empowers a Investigating police officer *to arrest* the perpetrator *without a warrant* when an offense is committed in real-time in his or her presence.

To identify and prosecute the perpetrator of a cybercrime, the police typically rely on various provisions from both the IPC and the ITA 2000, depending on the nature of the cyber offense. They may also collaborate with forensic experts, cybersecurity specialists, and other agencies to gather digital evidence and identify the individuals or groups responsible for the cyber offense.

3. The Judiciary's Pivotal Role and Police Collaboration in Cybercrime Investigations

In cybercrime investigations, the judiciary, particularly Magistrates, ensure that formal legal processes and rules governing actions like filing lawsuits, conducting trials, presenting evidence, and making legal arguments are followed by the Police and the rights of individuals are protected. Several sections of the CrPC are involved in this process, and various case laws illustrate the application of these sections in the context of cybercrime.

3.1 Police Report and Action

In cybercrime investigations, the role of the judiciary begins prominently after the submission of the police report under Section 173 of the Cr.PC.

(i) Section 173 Cr.PC / Section 193 BNSS – Police Report**:** Upon completion of investigation, the officer-in-charge submits a final police report to the Magistrate, enabling judicial scrutiny of evidence and determination of further proceedings. **(ii)** Section 190 CrPC / Section 210 BNSS – Cognizance of Offences**:** The Magistrate takes cognizance of offences based on police reports, complaints, or information, initiating judicial proceedings in cybercrime matters.(iii) Section 200 Cr.PC / Section 223 BNSS Examination of Complainant: In complaint cases, the Magistrate records sworn statements of the complainant and witnesses to verify the veracity of allegations.(iv) Section 202 CrPC / Section 225 BNSS. Postponement of issue of Process: The Magistrate may defer issuance of process and direct police inquiry or further investigation to evaluate digital or electronic evidence.

(v) Section 204 Cr.PC / Section 227 BNSS Issue of Process**:** If prima facie grounds exist, the Magistrate may issue summons or warrants to secure the appearance of the accused before the court. (vi) Section 207 CrPC / Section 230 BNSS – Supply of Documents**:** The accused must be provided with all relevant documents, including digital records and expert reports relied upon by the prosecution by Magistrate. (vii**)** Section 293 CrPC / Section 329 BNSS **–** Reports of digital forensic Experts: The court may rely on certified forensic reports from government scientific experts, treating them as valid evidence unless otherwise challenged. (viii) Section 309 CrPC / Section 346 BNSS – Postpone or Adjournment of Proceedings: The court controls trial progress, allowing postponement or adjournments proceedings only when necessary for effective justice, including pending expert analysis.(ix) Section 313 Cr.PC / Section 351 BNSS – Examination of Accused**:** The court examine /questions the accused on incriminating evidence, including digital material, providing an opportunity for explanation.(x) Section 320 CrPC / Section 359 BNSS - Compounding of Offences**:** The court may allow compounding of compoundable cyber offences with voluntary consent of parties, ensuring compliance with legal standards.

3.2 Judgment Pronouncement Across Courts under CrPC and BNSS

Court Type	**CrPC Section / BNSS Section**	**Purpose of Section**
All Criminal Courts	CrPC: Section 353 BNSS: Section 392	Pronouncement of judgment in open court by presiding officer.
	CrPC: Section 354 BNSS: Section 393	Specifies language & contents of the judgment – points for determination, decision, reasons.
Sessions Court	CrPC: Section 235 BNSS: Section 258	Judgment after trial and hearing the accused in a Sessions case for acquittal or conviction
Magistrate (Warrant Case)	CrPC: Section 248 BNSS: Section 271	Judgment by Magistrate in warrant cases instituted on police report for acquittal or conviction.
Magistrate (Summons Case)	CrPC: Section 255 BNSS: Section 278	Judgment in summons cases after hearing evidence and arguments for acquittal or conviction.
Appeal / Revision (Any Court)	CrPC: Section 386, 387 BNSS: Section 427, 428	Powers of appellate courts **(** Section 386) in disposing appeals **(** Section 387)—confirm, reverse, modify, etc.
High Court (all criminal courts**,** including Magistrate Courts, Sessions Courts**,** and High Courts)	CrPC: 353, 386 BNSS: 392, 427	Pronouncement of judgments (Sec.**353)** in appeals/revisions**,** and powers of appellate Court(Sec.386) maintaining open court principle.
Supreme Court	Governed by Article 132–136, (appellate jurisdiction) & Article 145 of Constitution (follows CrPC- Sec 374(2)/BNSS 415 Sec principles)	CrPC Sec 374(2) allows appeals from convictions to Supreme Court; judgment delivered under Constitution Articles 132–136, not under Cr.PC. Article 145: Supreme Court may make procedural rules with Presidential approval, subject to Parliament's laws.

Through its judicial discretion and adherence to procedural safeguards, the court ensures that the digital evidence collected during police investigations is scrutinized, validated, and fairly used in trial, maintaining the balance between justice delivery and individual right

3.3 Judicial Territorial Jurisdiction

(i)Section 80 of the Cr.PC provides for the issue of a summons or warrant to persons located outside the territorial jurisdiction of the court including the cases of cross-border cybercrimes. As per Section 179 of the Cr.PC, when cybercrime offense is committed partly within one jurisdiction and partly within another, any of the courts within those jurisdictions have jurisdiction to try the offense even beyond geographical boundaries.
(ii) To tackle the challenges posed by cross-border cybercrimes and promote effective international cooperation, India has entered into Mutual Legal Assistance Treaties (MLATs) with 42 nations, including the Russian Federation, the Islamic Republic of Iran, Ukraine, Turkey, and others. These MLATs enable the Ministry of Home Affairs for seeking, sharing of information, collection of evidence, and provision of support during investigations and prosecutions of transnational cyber offenses and provide mutual legal assistance in criminal law matters.
(iii) Apart from MLATs, interpol and other international law enforcement agencies play a crucial role in facilitating collaboration, cooperation and coordination among different countries to combat cross-border cybercrimes effectively.

4. Key CrPC Sections and Landmark Case Laws

(i) Section 156 Authority of Police Officers to Investigate Cognizable Offenses: Magistrates have the authority to monitor police investigations in cognizable offenses, including cybercrimes. They can order the police to register an FIR and investigate if the police are reluctant.
In *Lalita Kumari v. Govt. of U.P. & Ors., (2014) 2 SCC 1***,** the Supreme Court of India ruled that filing a First Information Report (FIR) is compulsory under Section 154 if the details indicate a serious/ cognizable offense. This ensures that the police act promptly in cybercrime cases, and the Magistrate plays a crucial role in overseeing the investigation.
(ii). Section 157 - Procedure for Investigation: Under this section, the Magistrate ensures that the police follow the proper procedure during the investigation, including collecting evidence and examining witnesses in cybercrime cases.
T.T. Antony v. State of Kerala, (2001) 6 SCC 181: This case highlighted the importance of proper investigation procedures. The SC emphasized that an investigation must be fair, and the Magistrate has the responsibility to ensure that the procedures under Section 157 are followed diligently.
(iii) Section 159 - Power to Hold Preliminary Inquiry: A Magistrate may conduct a preliminary inquiry to determine whether there is sufficient ground to proceed with a cybercrime investigation.
State of Haryana v. Bhajan Lal, 1992 Supp (1) SCC 335: The Supreme Court laid down guidelines for the exercise of powers under Section 159, including the circumstances in which a Magistrate can order a preliminary inquiry, particularly in cases involving complex cybercrimes.
(iv) Section 167 - When the procedure of Investigation cannot be completed in 24 Hours,: the magistrates can authorize the detention of the accused beyond 24 hours if the investigation is incomplete, ensuring that the rights of the accused are balanced with the needs of the investigation.
CBI v. Anupam J. Kulkarni, (1992) 3 SCC 141: In this case, the Supreme Court clarified the scope of judicial custody under Section 167, reinforcing the Magistrate's role in safeguarding the legal rights of individuals during prolonged cybercrime investigations.
(v) Section 173 - Report of the Police Officer: The final police report (charge sheet) must be submitted to the Magistrate, who reviews it to determine if the evidence is sufficient to proceed to trial in a cybercrime case.
Bhagwant Singh v. Commissioner of Police, (1985) 2 SCC 537: The Supreme Court ruled that the Magistrate must carefully review the police report submitted under Section 173, ensuring that all relevant evidence, including digital evidence in cybercrime cases, has been considered before proceeding to trial.
(vi) Section 202 - Postponement of Issue of Process: Magistrates can postpone the issuance of summons or warrants to the accused until further investigation is conducted, ensuring that there is sufficient evidence before proceeding against the accused in cybercrime cases.
National Bank of Oman v. Barakara Abdul Aziz, (2013) 2 SCC 488: The Supreme Court emphasized the need for a cautious approach by the Magistrate under Section 202, especially in complex cases, including cybercrimes, where additional investigation may be necessary to establish the accused's involvement.
(vii) Section 207: The Magistrate ensures that the accused is provided with copies of Police Report and all relevant documents, including digital evidence, to prepare a defense.
State of Punjab v. Sukhdev Singh, (1998) 3 SCC 198: The Supreme Court underscored the importance of supplying all relevant documents to the accused under Section 207, which is crucial for ensuring a fair trial, particularly in cybercrime cases where digital evidence is key.
(viii) Section 313 - Power to Examine the Accused: During the trial, the Magistrate examines the accused to clarify any points of evidence, including digital evidence in cybercrime cases, ensuring that the accused has an opportunity to explain any incriminating circumstances.
Bachan Singh v. State of Punjab, (1980) 2 SCC 684: This case established the importance of the accused's examination under Section 313 as a crucial step in ensuring justice, allowing the accused to address the evidence against them in cybercrime trials.
These sections of the CrPC, along with the cited case laws, illustrate how the judiciary, particularly Magistrates, play a pivotal role in ensuring that cybercrime investigations are conducted fairly and legally, safeguarding the rights of both the accused and the victims.
While the IPC does not have specific sections dealing with jurisdiction and cross-border crimes, the legal framework for handling such cases involves a combination of provisions from the CrPC , international agreements, and cooperation mechanisms.

5. CONCLUSION

The integration of forensic science into cybercrime investigation has transformed the landscape of criminal justice in India. Today, the legal system does not merely rely on eyewitness testimony or physical evidence, but also on the intricate analysis of digital trails that cybercriminals leave behind. The Indian Penal Code and its successor, the Bharatiya Nyaya Sanhita, define a wide range of offences that are now extended to cover acts committed through digital means.

The procedural backbone of cybercrime investigations is strengthened through the Code of Criminal Procedure and its modern counterpart, the Bharatiya Nagarik Suraksha Sanhita. These statutes regulate how investigations are initiated, evidence is collected, and cases are brought before the courts. The powers granted to cybercrime police officers, such as the authority to conduct searches of digital devices, intercept communications, and preserve digital logs, are rooted in these legal provisions.

Equally important is the evidentiary framework provided by the Indian Evidence Act and the Bharatiya Sakshya Adhiniyam. These laws ensure the authenticity, reliability, and admissibility of digital evidence—essential in an age where data manipulation and deepfakes pose real threats to justice.

Moreover, the judiciary plays a supervisory role in ensuring that the rights of both the victims and the accused are protected throughout the investigation and trial. Courts assess whether digital evidence has been handled according to legally established forensic models and whether territorial jurisdiction is rightly invoked in cyberspace-related offences.

Thus, the journey from FIR to forensic analysis in cybercrime cases is no longer linear but multifaceted, involving a delicate balance between police efficiency, technological accuracy, and judicial integrity. The collaborative approach adopted under India's updated legal framework represents a significant step toward a cyber-resilient and justice-oriented criminal justice system.