The Investigative Procedure for Cybercrime Cases

Authors: Krishna CV Grandhi, Chandra Lekha

I. Registration of FIR and Zero FIR in Cyber Offences

Under Section 173(1) of the BNSS, it is mandatory for police to register an FIR upon receipt of information regarding a cognizable offence. This applies equally to cyber offences such as hacking (BNS Section 109), identity theft (Section 112), and cyber terrorism (Section 113).

The concept of Zero FIR has now been formally codified under BNSS, allowing victims of cybercrime to file complaints at *any* police station regardless of jurisdiction. This is crucial given the borderless nature of cybercrimes.

Further, e-FIRs are permitted, allowing electronic submission of complaints. However, the informant's signature must be obtained within three days for formal registration.

II. Preliminary Enquiry in Cyber Offences

Section 173(3) of BNSS introduces a 14-day preliminary enquiry period for offences punishable with more than 3 but less than 7 years of imprisonment. Several cyber offences, such as doxxing, online impersonation, and fraud, may fall within this band.

A preliminary enquiry may be initiated to determine if a prima facie case exists, but only with prior approval of an officer not below the rank of DSP. Delay in FIR registration due to such enquiry can be addressed under Section 175(3) by seeking Magistrate intervention.

III. Commencement and Supervision of Investigation

Once a cognizable cybercrime is reported, the investigating officer (IO) may proceed with investigation under Section 175**.** Alternatively, a Magistrate may direct investigation under Section 210 BNSS.

Given the technical nature of cybercrimes, state cybercrime units or specialized technical cells often assist or lead such investigations. Offences under Section 109 (unauthorised access)**,** Section 112 (identity theft), and Section 113 (cyber terrorism) demand technical expertise, including forensic imaging and IP address tracking.

IV. Search and Seizure of Digital Evidence

Searches in cybercrime investigations are covered under Section 185 of BNSS, which allows search without a warrant if delay might cause destruction or concealment of digital evidence. This is particularly relevant for crimes involving encrypted data or volatile memory.

A seizure memo or panchnama must be prepared under Section 188, before by two witnesses. Electronic devices, storage media, cloud credentials, routers, etc., may be seized and sent for forensic examination.

Cyber investigators also rely on powers under the Information Technology Act, 2000 and Bharatiya Suraksha Adhiniyam (BSA), particularly in matters relating to digital surveillance and telecom data.

V. Collection and Preservation of Digital Evidence

Under Section 105 of BNSS, all searches and seizures must be recorded via audio-video means, and such recordings must be submitted to a Magistrate. This ensures integrity and authenticity of digital evidence.

The Investigating Officer may collect:

- IP logs from service providers
- Email trails and cloud records
- Mobile tower dumps and geolocation data
- System memory, browser history, deleted files, and registry logs

Witness statements under Section 180 of BNSS and forensic expert reports (hash values, metadata, etc.) become key elements of cybercrime trials. The BSA allows real-time interception or tracking of electronic communication under strict judicial and executive supervision, particularly in matters related to national security or cyber terrorism.

VI. Role of Forensics and Electronic Means

The BNSS and BSA stress the use of technology in investigation. Section 105 mandates audio-visual recording of searches. Section 308 also allows for examination of the accused via video conferencing.

Further, Section 349 (read with former CrPC Section 311A) permits collection of:

- Voice samples, handwriting, digital signatures, and
- Biometric data, even from third parties, if relevant to the offence.

VII. Arrest in Cyber Offences

The police may arrest an accused for cognizable cyber offences without a warrant under Section 35 and 36 of BNSS.

However, in offences punishable with less than 3 years and if the accused is above 60 years or infirm, prior DSP approval is required before arrest (Section 35 BNSS). Following such arrest, the arrest persons must be presented before the Magistrate within 24 hours.

VIII. Filing of Chargesheet in Cyber Offences

Upon completing investigation, a chargesheet under Section 193 of BNSS must be filed. For serious cyber offences (e.g., sexual cyber exploitation, child pornography under POCSO), the investigation must be completed within 2 months, extendable to 90 days.

The report should include:

1. Offence description and applicable sections (BNS + IT Act)
2. Evidence collected—digital, documentary, forensic
3. Details of accused and whether bail/custody was sought
4. Seized devices and preservation reports
5. Victim/informant updates on case status

In certain cases, portions of the report can be kept confidential if their disclosure is against public interest (e.g., cybersecurity vulnerabilities, informant identity).

Jurisdiction in Cyber Offences – BNS vs IT Act

BNS:
Section 1(5), Bharatiya Nyaya Sanhita (BNS), 2023
Applies to offences committed:

- By Indian citizens outside India
- On Indian ships or aircrafts
- Outside India, by any person targeting a computer resource in India
- "Offence" includes any act committed abroad that would be punishable if committed in India

IT Act:
Section 75, Information Technology Act, 2000
Applies to any person, regardless of nationality, if the offence:

- Is committed outside India.
- Involves a computer system, network, or resource located in India.
- Wider scope than BNS: Focuses on computer systems involved, not just the location of the target.

Comparative Analysis – BNS vs IT Act

Criteria	**BNS, 2023**	**IT Act, 2000**
Jurisdiction Basis	Targeting of Indian computer resources	Involvement of Indian computer systems

Applicability	Limited to offence targeting Indian resources	Any offence involving Indian IT infrastructure
Scope	Slightly narrower	Broader and more inclusive
Nationality-based enforcement	Yes (Indian citizens abroad)	No nationality restriction

The investigation of cybercrimes in India is primarily conducted by the State Police Cyber Cells and Specialised Units of Central agencies such as the CBI, depending on the nature and gravity of the offence. These powers are exercised in coordination with agencies like CERT-In, the National Cybercrime Reporting Portal (MHA), and the Indian Computer Emergency Response Team. Approval from senior officers or magistrates is often required for actions like arrests, searches, and surveillance, ensuring a check on arbitrariness.

Standard Operating Procedure for Cybercrime Investigation

According to the Judicial Academy and OSCE guidelines, a comprehensive cybercrime investigation typically involves the following stages:

1. Registration of FIR and Jurisdiction
   - Crimes can be registered where the offence occurred, its effects were felt, or in the location of either the victim or accused.
   - In complex or multi-location crimes (e.g., phishing across cities), FIRs may be registered in any relevant jurisdiction.
2. Immediate Response
   - Freeze victim and suspect accounts via bank notifications
   - Notify nodal officers of digital wallets under Section 91 CrPC
3. Evidence Collection and Digital Forensics
   - Devices must be secured like physical evidence (fingerprints, DNA)
   - Forensic imaging, metadata analysis, email header tracing, browser history examination, and OSINT are employed
   - Digital traces: avoidable (e.g., browsing history) and unavoidable (e.g., system logs)
4. Communication Data Acquisition
   - Includes IP addresses, IMEI, traffic logs, subscriber info, and message records.
   - Requests made under national legislation and MLATs for foreign data sources
5. OSINT and Covert Monitoring
   - Involves careful research of public data sources (social media, forums)
   - Should follow proportionality standards to avoid privacy violations.

Statutory Provisions under the IT Act, 2000 Supplementing An Investigation

Section 78 – Investigation Authority

- Only a Police Officer of Inspector rank or above is empowered to investigate offences under the IT Act, 2000

- Ensures a minimum standard of authority and expertise in cybercrime investigations

Section 80 – Powers of Entry, Search, and Arrest

- Any Inspector-rank officer or above may:
- Enter any public place
- Search premises
- Arrest without warrant if a person is reasonably suspected of:
- Having committed
- Being about to commit
- Or committing an offence under the IT Act

Digital Evidence – Procedure

Collection of digital evidence

During an investigation, one of the most crucial steps is to collect evidence. As per Jharkhand Police Manual, it stipulates the procedure for gathering evidence from switched off systems and switched on systems, as mentioned hereunder:

A) Procedure for gathering evidence from switched – off systems

• Secure and take control of scene of crime both physically (sending all persons away from scene of crime) and electronically (disabling all the network connections.)
• Make sure the computer is switched off, remove the battery from laptop.
• Never switch ON the computers in any circumstances.
• Label and photograph/video of all components of the system.
• Take out storage device (Hard Disk) carefully and record all unique identifiers like model and serial numbers.
• Signature of accused and witness on Hard Disk with a permanent marker.
• After Hard Disk is removed, switch on the system and go to BIOS, also keeping a note of date and time as shown in BIOS.
• Prepare detailed notes giving "when, where, what, why & who" and overall actions taken in relation to the computer equipment.
• Connect the suspected hard drive to the investigator computer through write – block device for forensically previewing/ copying/ printing or for duplication.
NEVER CONNECT DIRECTLY WITHOUT THE BLOCKER DEVICE.

B) Procedure for gathering evidence from switched – off systems

• Secure the area containing the equipment.
• Move people away from computer and power supply.
• Disconnect the modem if attached.
• If the computer is believed to be networked, seek advice from the technically trained officer, in-house forensic analyst or external specialist.
• Label and photograph/video of all components of the system.

Remove all other connection cables leading from the computer to other wall or floor sockets or devices.
• Carefully remove the equipment and record the unique identifiers – the main unit, screen, keyboards and other equipment.
• All items must have signed exhibit labels attached to them.
• The equipment should be cooled down before removal.
• Check if there are any passwords, and those must be recorded.
• Detailed notes of all actions taken in relation to computer equipment.
• Keep a note of the content of screen.
• Forensic assistance to be taken for the removal of information present in temporary memory such as RAM.
• If no specialist available then remove the power supply without closing any programs. The power supply cable which is attached at the end of the computer should be removed and not the one attached to the socket.

C) Procedure for gathering evidence from Mobile Phones.
• If the device is "Off", do not turn "ON".
• If device is On, leave ON. Powering down device could enable password, thus preventing access to evidence.
• Photograph device and screen display.
• Keep the device charged.
• Label and collect all cables (including power supply) and transport with device.
• Seize additional storage media
• If device cannot be kept charged, analysis by an expert must be completed prior to battery discharge or data may be lost.
• Document all steps involved in seizure of devices and components.

www.csail.org