DegreeLive

BBA | Semester I | UK1DSCMGT103

E-Commerce and Cyber Law

Course Code: UK1DSCMGT103 • Module 5 Notes

Module V: Cyber Regulations, Information Technology Act and Digital Forensics

1. The Information Technology Act, 2000: Historical Context, Scope, and Objectives

In response to the rapid proliferation of computer networks, the explosive growth of electronic commerce, and the international adoption of the UNCITRAL Model Law on Electronic Commerce (1996), the Parliament of India enacted the **Information Technology Act, 2000 (IT Act 2000)**, which came into legal force on October 17, 2000. It stands as India's primary legislation governing information technology, electronic communications, digital commerce, electronic governance, and cyber crimes.

A. Core Legislative Objectives of the IT Act, 2000

- To grant legal recognition for transactions carried out by means of electronic data interchange (EDI) and other means of electronic commerce, in substitution of paper-based methods of communication and storage of information.
- To facilitate the electronic filing of documents with government departments, statutory bodies, and licensing authorities, inaugurating formal Electronic Governance (E-Governance).
- To facilitate the electronic transfer of funds between commercial banking and financial institutions.
- To grant legal recognition for the retention of books of account and electronic records by bankers and commercial corporations.
- To establish a regulatory regime for Certifying Authorities and public-key digital signatures.
- To define cyber crimes, establish statutory penalties and compensatory remedies, and amend consequential Indian statutes, including the Indian Penal Code (IPC 1860), the Indian Evidence Act (1872), the Bankers' Books Evidence Act (1891), and the Reserve Bank of India Act (1934).

B. Extraterritorial Jurisdiction of the IT Act (Section 75)

Recognizing the borderless nature of cyberspace, Section 75 of the IT Act establishes explicit **Extraterritorial Jurisdiction**. The statute mandates that the Act applies to any offense or contravention committed outside the physical territory of India by any person—irrespective of their nationality, citizenship, or physical geographic location—provided that the act or conduct constituting the offense involves a **computer, computer system, or computer network located physically within India**. If a cyber criminal sitting in Eastern Europe hacks into an e-commerce server located in Bengaluru, Indian cyber courts possess full legal jurisdiction to try the offense.

C. The Information Technology (Amendment) Act, 2008

The 2008 amending statute enacted comprehensive structural reforms: (1) Replaced narrow "digital signatures" with the broader, technologically neutral concept of **Electronic Signatures**; (2) Introduced dedicated cyber crime sections addressing identity theft (66C), cheating by personation (66D), privacy violations (66E), cyber terrorism (66F), and child pornography (67B); (3) Formally

Degreelive

established the **Indian Computer Emergency Response Team (CERT-In)** as the national nodal agency for incident response under Section 70B; (4) Overhauled Section 79 to establish a modern "Safe Harbor" framework for internet intermediaries; and (5) Created the statutory architecture for protecting *Critical Information Infrastructure (CII)* under Section 70 via the National Critical Information Infrastructure Protection Centre (NCIIPC).

2. Legal Recognition of Electronic Records, Electronic Signatures, and E-Governance

Sections 4 to 10A of the IT Act codify the legal functional equivalence between traditional paper records and modern electronic messages:

- **Section 4 (Legal Recognition of Electronic Records):** Where any statutory law mandates that information or matter shall be in writing, typewritten, or printed form, such requirement is deemed satisfied if the information is rendered or made available in an electronic form and accessible so as to be usable for subsequent reference.
- **Section 5 (Legal Recognition of Electronic Signatures):** Where any law requires that any information or document shall be authenticated by affixing a signature, such requirement is deemed satisfied if authenticated by an electronic signature affixed in such manner as prescribed by the Central Government.
- **Section 6 (Use of Electronic Records in Government Agencies):** Authorizes the electronic filing of applications, statutory forms, and returns, the issuance of government licenses and permits in digital format, and the electronic receipt and disbursement of public fees.
- **Section 7 (Retention of Electronic Records):** Where any law mandates the retention of documents, records, or information for a specified period, that requirement is satisfied if retained in an electronic form, provided the format remains accessible, the original message metadata (origin, destination, date, and time of generation) is preserved, and the integrity of the data remains intact.
- **Section 10A (Validity of Contracts Formed Electronically):** Explicitly affirms that in contract formation, the communication of proposals, acceptance of proposals, and revocation of proposals may be expressed in electronic form or by means of electronic records, and shall not be deemed unenforceable solely on the ground that electronic records were used.

3. Formation, Attribution, and Dispatch of Online Electronic Contracts

Sections 11 to 13 of the IT Act establish precise procedural rules governing the mechanics of contract formation in cyberspace:

- **Section 11 (Attribution of Electronic Records):** An electronic record is legally attributed to the originator if it was sent by the originator personally, or by a person authorized to act on behalf of the originator, or by an automated information system programmed by or on behalf of the originator to operate autonomously.
- **Section 12 (Acknowledgment of Receipt):** Where the originator has not agreed with the addressee on a specific form of acknowledgment, receipt may be proven by any communication

(automated or manual) by the addressee, or any conduct sufficient to indicate to the originator that the electronic record was received. If the originator specifies that the record is conditional on receiving an acknowledgment, the record is treated as never sent until acknowledgment arrives.

- **Section 13 (Time and Place of Dispatch and Receipt):**
  - *Time of Dispatch:* The dispatch of an electronic record occurs at the exact chronological moment when it enters a computer resource outside the control of the originator.
  - *Time of Receipt:* If the addressee has designated a specific computer resource (designated email address): receipt occurs when the electronic record enters the designated computer resource. If sent to a non-designated computer resource, receipt occurs when the addressee actually retrieves the record.
  - *Place of Dispatch and Receipt:* An electronic record is deemed to be dispatched from the originator's **principal place of business**, and deemed received at the addressee's principal place of business, regardless of where the physical cloud server or mobile device is physically located.

4. Cyber Crimes, Statutory Penalties, and Judicial Landmark Rulings

The IT Act bifurcates cyber wrongdoing into civil contraventions (attracting financial compensation and penalties under Chapter IX) and criminal offenses (attracting imprisonment and criminal fines under Chapter XI):

Statutory Section	Prohibited Conduct and Elements	Maximum Statutory Penalty / Punishment	Real-World Context
Section 43	Unauthorized access, downloading, copying, or extracting of data; introducing computer viruses/contaminants; disrupting system performance; denying access to authorized users.	Civil compensation to affected victims (originally capped at INR 1 Crore; 2008 amendment removed ceiling, granting Adjudicating Officers power to award unlimited actual damages).	Corporate data theft, ex-employee stealing customer proprietary databases.
Section 65	Knowingly or intentionally concealing, destroying, or altering computer source code when required to be maintained by law.	Imprisonment up to 3 years and/or fine up to INR 2 Lakhs.	Maliciously modifying accounting software source code to conceal corporate embezzlement.
Section 66	Hacking: Doing any act referred to in Section 43 dishonestly or fraudulently.	Imprisonment up to 3 years and/or fine up to INR 5 Lakhs.	Defacing an e-commerce website, exploiting database injection flaws to steal passwords.
Section 66C	Identity Theft: Fraudulent or dishonest use of another person's	Imprisonment up to 3 years and fine up to INR 1 Lakh.	Phishing bank passwords, unauthorized

Statutory Section	Prohibited Conduct and Elements	Maximum Statutory Penalty / Punishment	Real-World Context
	electronic signature, password, or unique identification feature.		use of a director's digital signature token.
Section 66D	Cheating by Personation: Cheating by personating another person using any computer resource or communication device.	Imprisonment up to 3 years and fine up to INR 1 Lakh.	Creating fake executive social media profiles, lottery prize advance-fee fraud.
Section 66E	Privacy Violation: Intentionally capturing, publishing, or transmitting the image of a private area of any person without consent.	Imprisonment up to 3 years and/or fine up to INR 2 Lakhs.	Installing hidden spy cameras in retail changing rooms or hotel restrooms.
Section 66F	Cyber Terrorism: Accessing computer systems to threaten national unity, integrity, sovereignty, or striking terror using malware to cause death or disruption of critical infrastructure.	**Imprisonment for Life** (the harshest criminal penalty in the IT Act).	Launching cyber warfare attacks against nuclear grid controllers, military defense networks.
Section 67 / 67A / 67B	Publishing or transmitting obscene material (67), sexually explicit acts (67A), or child sexual abuse material - CSAM (67B) in electronic form.	Imprisonment up to 5 years (1st offense) or 7-10 years (subsequent), with fines up to INR 10 Lakhs.	Non-consensual image distribution, hosting child sexual abuse content online.

The Historic Landmark Ruling: Shreya Singhal v. Union of India (2015)

Section 66A of the IT Act had criminalized sending any electronic message that was "grossly offensive" or had "menacing character." Law enforcement authorities routinely abused this ambiguous section to arrest innocent citizens and political satirists for legitimate political commentary on social media. In a historic constitutional victory for civil liberties, the Supreme Court of India in **Shreya Singhal v. Union of India (2015)** struck down Section 66A in its entirety as **unconstitutional, void, and a direct violation of Article 19(1)(a)** (Freedom of Speech and Expression). The Court held that Section 66A was unconstitutionally vague, overbroad, lacked clear definitions, and created an intolerable "chilling effect" on free democratic discourse.

5. Intermediary Liability and the Section 79 "Safe Harbor" Protection

An Internet Intermediary is any entity that receives, stores, transmits, or provides services with respect to electronic records generated by third parties. Intermediaries include telecom service providers, Internet Service Providers (ISPs), search engines (Google), web hosting companies, online marketplaces (Amazon, Flipkart), and social media platforms (Meta, X, YouTube).

The Section 79 Safe Harbor Framework

If an internet intermediary were held strictly liable for every single piece of copyright-infringing content, defamatory tweet, or fraudulent listing uploaded by its millions of third-party users, modern

digital platforms could not exist. Under Section 79 of the IT Act, intermediaries enjoy statutory **Safe Harbor (Immunity from Third-Party Liability)**, provided they satisfy three statutory prerequisites:

- The function of the intermediary is limited strictly to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; and
- The intermediary does not initiate the transmission, does not select the receiver of the transmission, and does not select or modify the information contained in the transmission; and
- The intermediary observes **Mandatory Due Diligence** while discharging its duties, complying with the guidelines prescribed by the Central Government.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

To retain Safe Harbor immunity, intermediaries must comply with strict due diligence mandates: (1) Publish clear user agreements, privacy policies, and rules informing users not to host, display, or upload harmful, defamatory, or unlawful content; (2) *Notice-and-Takedown Procedure:* Under the Supreme Court's ruling in *Shreya Singhal*, an intermediary loses safe harbor only if it fails to remove unlawful content within 36 hours upon receiving **actual knowledge** via a formal court order or authorized government notification; (3) Significant Social Media Intermediaries (SSMIs, platforms with ≥ 5 million registered Indian users) must mandatorily appoint a resident Chief Compliance Officer (personally liable for non-compliance), a resident Nodal Contact Person for 24/7 law enforcement coordination, and a resident Grievance Officer, publishing monthly transparency compliance reports.

6. Cyber Forensics: Digital Evidence Acquisition, Analysis, and Chain of Custody

Cyber Forensics (Digital Forensics) is the rigorous scientific discipline that identifies, collects, preserves, analyzes, and presents digital electronic evidence stored on magnetic, optical, or electronic media in a manner acceptable in courts of law.

A. Volatile vs Non-Volatile Memory and the Order of Volatility

Digital evidence is categorized based on its permanence: (1) *Volatile Memory:* Data stored in registers, CPU cache, and RAM (Random Access Memory), active routing tables, running process lists, open network sockets, and unencrypted temporary session keys. Volatile evidence is permanently wiped the microsecond power is terminated; (2) *Non-Volatile Memory:* Data stored in permanent physical media (hard disk drives - HDDs, solid-state drives - SSDs, optical DVDs, USB flash drives, cloud block storage) that survives power cycles. Forensic investigators adhere strictly to the **Order of Volatility**: capturing volatile RAM memory first (Live System Triage) before powering down or disconnecting machine power.

B. Methodological Stages of a Digital Forensic Investigation

1. **Identification and Crime Scene Securing:** Isolating the physical scene, seizing target hardware, and placing wireless devices (smartphones) immediately into **Faraday Isolation Bags**

to block external radio frequency signals (preventing suspects from triggering remote wipe commands via iCloud or Find My Device).

2. **Forensic Acquisition (Imaging):** The cardinal rule of digital forensics dictates that **investigators NEVER examine or conduct analysis on the original physical storage drive**. The suspect drive is connected to a hardware **Write-Blocker** (a physical electronic interface that permits reading data while physically preventing any writing, modifying, or deleting of bits). The investigator creates an exact, sector-by-sector, bit-stream duplicate copy (Forensic Image, typically in .E01 or raw .dd format) of the entire physical drive, including hidden unallocated space, slack space, and deleted file fragments.
3. **Cryptographic Hash Verification:** Immediately before and after imaging, the investigator computes a cryptographic hash (SHA-256) of the original physical drive and the resulting forensic image. A byte-exact mathematical match proves that the forensic duplicate is an identical replica of the original drive, validating evidentiary integrity.
4. **Forensic Analysis:** Searching the verified forensic image using specialized tools (EnCase, Autopsy, FTK) to recover deleted files, inspect browser histories, analyze metadata, examine Windows Event Logs, extract prefetch execution artifacts, and carve unallocated drive clusters.
5. **Documentation and Chain of Custody:** Maintaining an unbroken, meticulous **Chain of Custody Form** documenting every individual who took physical possession of the evidence, the exact date, time, physical location, purpose of transfer, and secure anti-tamper evidence bag serial numbers. Any unaccounted gap in the chain of custody renders the evidence inadmissible in court.

7. Admissibility of Electronic Evidence: Section 65B of the Indian Evidence Act, 1872

Under traditional common law, physical original documents represent "Primary Evidence," whereas copies represent "Secondary Evidence," which requires special foundational proof. Because digital computer records (emails, server log printouts, WhatsApp chats, CCTV footage) are inherently reproducible secondary electronic outputs, the Parliament introduced **Sections 65A and 65B** into the Indian Evidence Act, 1872 to govern digital admissibility.

The Mandatory Section 65B Certificate

Section 65B(1) establishes that any information contained in an electronic record printed on paper, stored, recorded, or copied in optical or magnetic media produced by a computer shall be deemed to be a document and admissible in legal proceedings without further proof or production of the original physical device, **PROVIDED the conditions specified in Section 65B(2) and 65B(4) are strictly satisfied**.

Section 65B(4) mandates that electronic evidence must be accompanied by a formal **Section 65B Evidentiary Certificate**, signed by a responsible official holding a management or operating position with respect to the computer system. The certificate must affirmatively state:

- Identifying the electronic record containing the statement and describing the manner in which it was produced.

- Certifying that the computer was in regular lawful use by a person having lawful control over it during the relevant period.
- Certifying that information of that kind was regularly and systematically fed into the computer in the ordinary course of business.
- Certifying that throughout the material period, the computer was operating properly, or if not, the period of breakdown did not affect the electronic record's production or accuracy.
- Giving details of the device used to produce the electronic printout or output.

The Settled Jurisprudence: Arjun Panditrao Khotkar Landmark Ruling (2020)

Conflicting rulings by two-judge benches of the Supreme Court (e.g., *Navjot Sandhu 2005* vs *Anvar P.V. 2014*) created widespread confusion over whether the 65B certificate was mandatory. A three-judge constitutional bench in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)** definitively resolved the law:

- The Supreme Court held that the production of a **Section 65B(4) Certificate is a MANDATORY CONDITION PRECEDENT** to the admissibility of any secondary electronic evidence in Indian courts. Oral testimony cannot substitute for a written 65B certificate.
- The only exception is where the original physical hardware device itself (e.g., the suspect's original physical smartphone, laptop, or server hard drive) is physically brought into the courtroom and exhibited directly by the owner (Primary Evidence under Section 62). In all other cases involving printouts, CD copies, or flash-drive transfers, the absence of a valid 65B certificate renders the electronic evidence strictly inadmissible.

In conclusion, the Information Technology Act, 2000, combined with robust intermediary governance, forensic rigor, and statutory evidence certification, forms the indispensable legal framework that protects digital society. By providing statutory validity to online transactions, establishing severe penalties for cyber offenses, safeguarding free speech against overbroad censorship, and establishing rigorous forensic standards for courtroom evidence, cyber law guarantees that the rule of law reigns supreme across Indian cyberspace.

8. Critical Information Infrastructure (CII) and the Role of NCIIPC

Under Section 70 of the IT Act, 2000, the Central Government is empowered to declare any computer system, network, or database as **Critical Information Infrastructure (CII)**. The statute defines CII as *"the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."*

To safeguard strategic assets, the Government established the **National Critical Information Infrastructure Protection Centre (NCIIPC)** as the national nodal agency under Section 70A. NCIIPC oversees cybersecurity across six designated critical national sectors: (1) Power and Energy; (2) Banking, Financial Services, and Insurance (BFSI); (3) Telecom and Information Technology; (4) Transportation (Civil Aviation, Indian Railways, Maritime Ports); (5) Strategic and Public Enterprises (Atomic Energy, Defense Production, Space Systems); and (6) Government and Public Administration.

Unauthorized access or attempted hacking of a protected CII system carries a mandatory statutory criminal punishment of **imprisonment up to 10 years** and fine under Section 70(3).

9. CERT-In Incident Reporting Directives and Log Retention Mandates

The **Indian Computer Emergency Response Team (CERT-In)**, established under Section 70B of the IT Act, serves as the national nodal agency for responding to computer security incidents. In 2022, CERT-In issued historic regulatory cybersecurity directives:

- **Mandatory 6-Hour Incident Reporting:** All commercial corporate service providers, intermediaries, data centers, and corporate bodies must report specified cybersecurity incidents (such as ransomware attacks, data breaches, identity theft, denial of service attacks, targeted scanning) to CERT-In **within 6 hours** of noticing or being brought to notice of the incident.
- **Mandatory 180-Day Log Retention:** All enterprise organizations must mandatorily enable logging on all ICT systems and maintain secure, chronological system logs physically within Indian territorial jurisdiction for a minimum rolling period of **180 days** to facilitate digital forensic investigation.
- **NTP Server Synchronization:** All corporate and government IT infrastructure must synchronize system clocks to the official Network Time Protocol (NTP) servers of the National Physical Laboratory (NPL) or NIC to ensure precise, standardized timestamps across digital evidence.

10. The Digital Personal Data Protection Act, 2023 (DPDP Act): Modern Data Governance

Enacted in August 2023 following years of parliamentary deliberation, the **Digital Personal Data Protection Act, 2023 (DPDP Act)** establishes India's comprehensive statutory framework for personal data governance, establishing explicit rights and duties for individuals and corporations:

- **Key Institutional Entities:** The *Data Principal* is the individual to whom personal data relates. The *Data Fiduciary* is the entity that determines the purpose and means of data processing. The *Data Processor* processes data on behalf of a Data Fiduciary.
- **Significant Data Fiduciaries (SDFs):** Central Government designates entities as SDFs based on volume and sensitivity of data processed, risk of harm to sovereignty, and electoral democracy. SDFs must mandatorily appoint a resident Data Protection Officer (DPO), engage independent external data auditors, and conduct periodic Data Protection Impact Assessments (DPIA).
- **Children's Personal Data Protections:** Data Fiduciaries are strictly prohibited from tracking, behavioral monitoring, or serving targeted advertising directed at children (individuals under 18 years), mandating verifiable parental consent.
- **The Data Protection Board of India (DPBI):** An independent digital-first adjudicatory board established to investigate data breaches, adjudicate non-compliance, and levy severe financial penalties. For failure to take reasonable security safeguards to prevent a data breach, the DPBI can impose monumental statutory penalties up to **INR 250 Crores** per incident.

DegreeLive

11. Mobile and IoT Digital Forensics: Technical Methodologies

Over 80% of modern cyber crimes involve smartphones and interconnected Internet of Things (IoT) devices, presenting unique forensic extraction challenges:

- **Levels of Mobile Device Extraction:** (1) *Logical Extraction:* Communicating with the smartphone operating system via official API protocols (ADB) to extract active user files, call logs, SMS, and contacts; (2) *File System Extraction:* Extracting database structures, application sandbox directories, and system logs, often requiring temporary privileged access; (3) *Physical Extraction (Bit-by-Bit):* Bypassing the operating system using specialized bootloaders (Cellebrite, Oxygen Forensic) to dump raw NAND flash memory, allowing recovery of deleted records from unallocated space.
- **SQLite Database Carving:** Most mobile messaging applications (WhatsApp, Signal, Telegram) store local chats and media metadata in structured relational SQLite database files. Forensic examiners carve deleted chat records from SQLite Freeblocks and Write-Ahead Logs (WAL), reconstructing complete conversational timelines.

12. Electronic Discovery (E-Discovery) and the EDRM Framework

In modern corporate litigation, regulatory investigations, and criminal cyber trials, over 95% of relevant evidence exists in electronic format. **Electronic Discovery (E-Discovery)** is the legal and technical process of identifying, preserving, collecting, reviewing, and exchanging Electronically Stored Information (ESI) in response to court discovery orders. E-discovery follows the internationally recognized **Electronic Discovery Reference Model (EDRM)**:

- **Information Governance:** Institutional policies ensuring electronic files are categorized, managed, and securely retained or disposed of in the ordinary course of business.
- **Identification:** Locating potential custodians of relevant evidence (e.g., identifying which corporate executives exchanged emails regarding an alleged antitrust price-fixing scheme).
- **Legal Hold and Preservation:** Issuing formal written *Legal Hold Notices* to employees, mandating the immediate suspension of routine automated document deletion schedules, preserving relevant emails, WhatsApp chats, and local hard drives. Failure to preserve evidence constitutes statutory *Spoliation of Evidence*, attracting severe judicial sanctions.
- **Collection, Processing, and Review:** Gathering forensic copies using write-blockers, de-duplicating identical email threads, converting proprietary files to text, and loading evidence into review platforms (such as Relativity) where legal teams review documents for attorney-client privilege.

13. International Cybercrime Cooperation: The Budapest Convention and MLATs

Because cyber attackers routinely operate across foreign sovereign jurisdictions, domestic law enforcement agencies cannot unilaterally seize servers or arrest suspects located overseas without

DegreeLive

violating international law. Transnational cybercrime investigation relies upon formal international cooperation mechanisms:

- **The Budapest Convention on Cybercrime (2001):** The first international multilateral treaty addressing internet crimes (copyright infringement, computer fraud, child pornography, network security violations). It harmonizes domestic criminal substantive laws, provides domestic procedural investigation powers (expedited preservation of stored data, real-time collection of traffic data), and establishes a fast-track 24/7 international contact network.
- **Mutual Legal Assistance Treaties (MLAT):** Formal bilateral legal agreements between sovereign governments that establish procedural mechanisms for exchanging evidentiary materials, taking formal witness testimonies, executing search warrants, and seizing criminal assets across borders. While legally robust, MLAT requests historically require 6 to 18 months, leading nations to negotiate fast-track direct cloud provider data disclosure agreements (such as the US CLOUD Act).

14. Adjudication Mechanism and the Cyber Appellate Tribunal (TDSAT)

To provide fast, specialized administrative adjudication of civil cyber contraventions under Chapter IX of the IT Act (such as unauthorized access, data extraction, virus injection, and system disruption under Section 43), the IT Act established an administrative judicial hierarchy:

- **Adjudicating Officers (Section 46):** The Central Government appoints officers of the rank of Director to the Government of India or State IT Secretaries as statutory Adjudicating Officers. An Adjudicating Officer possesses all the formal powers of a Civil Court under the Code of Civil Procedure (CPC 1908), including summoning witnesses, compelling the discovery and production of electronic records, and awarding unlimited compensatory financial damages to affected corporate or individual victims.
- **Telecom Disputes Settlement and Appellate Tribunal (TDSAT):** Historically, appeals against orders of Adjudicating Officers were heard by the Cyber Appellate Tribunal (CyAT). Under the Finance Act, 2017, the Cyber Appellate Tribunal was merged into the **TDSAT** under Section 57 of the IT Act. Any person aggrieved by an order made by an Adjudicating Officer or the Controller of Certifying Authorities can prefer an appeal to TDSAT within 45 days. TDSAT decisions can be appealed strictly on questions of law to the High Court of the respective state.

15. Bail Provisions and Compoundability Under Section 77B of the IT Act

The classification of cyber offenses as bailable or non-bailable is governed under **Section 77B of the Information Technology Act, 2000**:

- **Bailable Offenses:** The statute mandates that all offenses punishable with imprisonment of **three years or less** are bailable offenses as a matter of legal right under the Code of Criminal Procedure (CrPC 1973). This includes hacking under Section 66, identity theft under Section 66C, cheating by personation under Section 66D, and privacy violation under Section 66E.
- **Non-Bailable Offenses:** Cyber offenses carrying statutory punishment exceeding three years—including Cyber Terrorism under Section 66F (punishable with imprisonment for life), publishing child sexual abuse material under Section 67B, and repeat convictions under Section 67 and 67A—

are classified as serious **Non-Bailable Offenses**, where granting bail remains entirely at judicial discretion based on the severity of threat to national security or public order.

DegreeLive