Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0050

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

The Functioning of Criminal Courts in Cybercrime Cases

By : Mrs. Mohini Dhanaskar,
Research Scholar

Abstract:
In today's world, cybercrimes are becoming a big problem, and India is facing these challenges as well. As more people rely on the internet for work, shopping, and communication, crimes like hacking, online fraud, identity theft, and cyber bullying are on the rise. This paper looks at how Indian courts handle these cybercrimes and the legal systems in place to deal with them. It explains how laws like the **Information Technology Act, 2000** (IT Act) and the **Indian Penal Code** are used to punish cybercriminals and how important digital experts are for proving the crimes in court. The paper also explores the need for special cybercrime courts and how judges need to understand technology to make fair decisions. It talks about the difficulties the courts face, such as tracking criminals across borders, dealing with anonymous offenders, and handling complex digital evidence. Through real-life examples and a look at current practices, the paper aims to show how India's legal system is working to fight cybercrimes and what improvements are needed. It highlights the importance of better technology, international cooperation, and public awareness to stop these crimes and protect people online.

Introduction :
In today's digital world, cybercrime is a growing problem, affecting people, businesses, and even governments. As more of our lives move online, criminal courts play a key role in ensuring that cybercriminals are held accountable.

Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe.

Until recently, many information technology (IT) professionals lacked awareness of and interest in the cyber crime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust— between the two most important players in any effective fight against cyber crime: **law enforcement agencies** and **computer professionals.** Yet close cooperation between the two is crucial if we are to control the cyber crime problem and make the Internet a safe "place" for its users.

Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cyber criminal.

IT professionals need good definitions of cybercrime in order to know when (and what) to report to police, but law enforcement agencies *must* have statutory definitions of specific crimes in order to charge a criminal with an offense. The first step in specifically defining individual cybercrimes is to sort all the acts that can be considered cybercrimes

into organized categories.

In the present global situation where cyber control mechanisms are important we need to push cyber laws. Cyber Crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber crime. The 7 stage continuum of a criminal case starts from **perpetration** to **registration** to **reporting**, **investigation**, **prosecution**, **adjudication** and **execution**. The system can not be stronger than the weakest link in the chain. In India, there are 30 million policemen to train apart from 12,000 strong Judiciary. Police in India are trying to become cyber crime savvy and hiring people who are trained in the area. Each police station in Delhi will have a computer soon which will be connected to the Head Quarter.. The pace of the investigations however can be faster; judicial sensitivity and knowledge need to improve. Focus needs to be on educating the police and district judiciary. IT Institutions can also play a role in this area.

Over 740,000 cases of cyber crime were reported to the Indian Cyber Crime Coordination Centre (I4C) in India within the first four months of 2024 alone. The number of cyber crimes in the country saw a massive spike between 2019 and 2020 and have been on the rise ever since. Roughly 85 percent of the reports in 2024 were related to online financial fraud

Like many countries, India is suffering increasingly from cyber crime. The number of cyber-related crimes reported in 2018 was 208,456. In the first 2 months of 2022 alone, there were 212,485 reported cyber crimes, more than the entirety of 2018.

The figures rose more sharply through the pandemic, with reported crime jumping from 394,499 cases in 2019 to 1,158,208 in 2020 and 1,402,809 in 2021. Between Q1 and Q2 2022, cyber crime across India increased by 15.3%.

Additionally, there have been an increasing number of Indian websites hacked in recent years. In 2018, some 17,560 sites were hacked. In 2020, an additional 26,121 sites were hacked.

78% of Indian organisations experienced a ransomware attack in 2021, with 80% of those attacks resulting in the encryption of data. In comparison, the average percentage of attacks was 66%, with the average encryption rate at 65%.

The most common form of cyber crime in India is financial fraud. This accounted for 75% of cyber crime in India between 2020 and 2023, with a high point of over 77% of crimes committed during the period.

In India, the functioning of criminal courts in cybercrime cases is governed by a combination of laws, specialized procedures, and the involvement of technical experts. Here's an overview of how criminal courts in India handle cybercrime cases:

1. Cybercrime Investigation in India

- **Law Enforcement Agencies**: Cybercrimes are primarily investigated by specialized units like the Cyber Crime Cells within state police departments, or central agencies like the **Central Bureau of Investigation (CBI)** and **National Investigation Agency (NIA)**. In many cases, the **Cyber Crime Investigation Division (CCID)** handles cases related to cybercrimes.
- **Indian Cyber Crime Coordination Centre (I4C)**: This body, set up by the Ministry of Home Affairs, coordinates between various agencies to address and combat cybercrimes more effectively. The I4C is responsible for tracking cybercrimes, coordinating investigations, and training law enforcement agencies.

2. Cybercrime Laws in India

India has specific legislation to deal with cybercrimes:

- **Information Technology Act, 2000 (IT Act)**: The IT Act is the primary legal framework for addressing cybercrimes in India. It includes provisions for:
  - **Section 66**: Punishment for hacking and unauthorized access to computer systems.
  - **Section 66C and 66D**: Penalties for identity theft and cyber fraud.
  - **Section 72**: Punishment for the breach of confidentiality and privacy.
  - **Section 67**: Punishment for publishing or transmitting obscene material in electronic form.
- **Indian Penal Code (IPC)**: In cases where cybercrimes intersect with traditional crimes like fraud, defamation, or harassment, provisions of the IPC (such as Section 420 for cheating or Section 503 for criminal intimidation) are also applied.
- **The Data Protection Law**: As of 2025, India is in the process of implementing the **Personal Data Protection Bill**, which will regulate how data is processed, stored, and used, providing additional safeguards against cybercrimes like data theft and breaches.

3. Pre-Trial Procedures

- **Complaint Filing**: Cybercrimes can be reported to the police via an online portal (e.g., the **National Cyber Crime Reporting Portal**), or victims can directly approach local police stations.
- **Cyber Forensics**: To investigate cybercrimes, law enforcement agencies often rely on **digital forensics experts** who collect, analyze, and preserve digital evidence. These experts use specialized software and tools to retrieve data from computers, mobile devices, and servers.
- **Expert Testimony**: In many cases, the court may require expert testimony from a cyber forensics expert to authenticate digital evidence and explain the technical aspects of the crime to the judge.

4. Trial Proceedings in Cybercrime Cases

- **Digital Evidence**: In a cybercrime trial, the collection and presentation of digital evidence are crucial. Indian courts rely on experts to explain the process of evidence collection, ensuring that the chain of custody is maintained and that evidence has not been tampered with.
- **Admissibility of Evidence**: Digital evidence, such as emails, chat logs, IP addresses, and files from devices, must comply with the rules of evidence laid down by the **Indian Evidence Act**. For example:
  - **Section 65B** of the Indian Evidence Act allows for the admissibility of electronic records in court if they are properly authenticated.
  - Courts must ensure that electronic records are not tampered with and are retrieved through lawful means.
- **Role of Judges**: In India, many criminal courts still lack judges with specialized training in technology. However, in major cities, there are courts or panels with judges who have experience in handling cybercrimes. In complex cases, courts may rely heavily on the testimonies of digital forensics experts.

5. Sentencing in Cybercrime Cases

- **Punishments under IT Act**: The severity of punishment for cybercrimes varies according to the offense. For example:
  - **Hacking (Section 66)**: Punishable with imprisonment for up to three years, or a fine, or both.

  - **Identity Theft (Section 66C)**: Punishable with imprisonment for up to three years, or a fine of up to ₹1 lakh, or both.
  - **Cyber Fraud (Section 66D)**: Punishable with imprisonment for up to three years, or a fine of up to ₹1 lakh, or both.
- **Victim Compensation**: In cases of identity theft or online harassment, victims may seek compensation or damages, though the legal process for securing restitution can be lengthy.

6. Appeals Process

- If a party is dissatisfied with the verdict, they can appeal the decision to higher courts such as the **High Court** or **Supreme Court**. Appeals may be filed on the grounds of incorrect interpretation of the law or errors in the handling of digital evidence.
- In some cases, appellate courts may revisit the technical aspects of the case, particularly regarding the authenticity of digital evidence.

7. Specialized Cybercrime Courts

- In response to the rise of cybercrimes, some Indian states have experimented with specialized **cybercrime courts**. These courts aim to streamline the process of adjudicating cybercrime cases, making the judicial process more efficient by utilizing specialized judges and expert testimony.
- However, specialized cybercrime courts are not yet widespread, and many cases are still handled by regular criminal courts.

8. Challenges in Cybercrime Cases in India

- **Jurisdictional Issues**: Cybercrimes often have a cross-border element, making jurisdiction an issue. India collaborates with other countries through international agreements like the **Budapest Convention** and INTERPOL to address crimes that span multiple jurisdictions.
- **Technical Challenges**: The rapid advancement of technology often leaves law enforcement agencies struggling to keep up. The need for continuous training and access to the latest digital forensics tools is critical.
- **Anonymity of Offenders**: Cybercriminals often use tools like VPNs, the dark web, and encrypted communications to remain anonymous. Tracing the origin of crimes and linking suspects to specific activities can be challenging.
- **Lack of Cyber Awareness**: There is often a gap in public awareness regarding cybersecurity. The lack of awareness can lead to delayed reporting of crimes or mishandling of digital evidence, which impacts investigations.

9. International Cooperation

- **Cross-Border Cooperation**: Cybercrimes frequently cross international borders, and cooperation with foreign agencies is essential in prosecuting offenders. India cooperates with countries and organizations like **INTERPOL**, **Europol**, and the **FBI** to tackle cybercrimes that involve multiple jurisdictions.
- **Extradition**: In cases where cybercriminals operate from foreign countries, India may seek extradition based on international treaties.

Cybercrime Statistics and Data

India has seen a significant rise in cybercrime cases over the years. According to the **National Crime Records Bureau (NCRB)**, there has been a steady increase in cybercrime incidents. In 2020 alone, around **50,000+ cases** were reported under the **IT Act** and **IPC** relating to cybercrimes.

Furthermore, the **National Cyber Crime Reporting Portal** registered a notable surge in complaints related to online fraud, cyberbullying, and phishing, particularly during the COVID-19 lockdowns, when people increasingly relied on digital platforms for work, study, and social interaction.

ANN
EXURE-I RS USQ. NO.
234 FOR 27.11.2024

STATE/UT-WISE CASES REGISTERED UNDER CYBER CRIMES DURING 2018-2022

SL	State/UT	2018	2019	2020	2021	2022
1	Andhra Pradesh	1207	1886	1899	1875	2341
2	Arunachal Pradesh	7	8	30	47	14
3	Assam	2022	2231	3530	4846	1733
4	Bihar	374	1050	1512	1413	1621
5	Chhattisgarh	139	175	297	352	439
6	Goa	29	15	40	36	90
7	Gujarat	702	784	1283	1536	1417
8	Haryana	418	564	656	622	681
9	Himachal Pradesh	69	76	98	70	77
10	Jharkhand	930	1095	1204	953	967
11	Karnataka	5839	12020	10741	8136	12556
12	Kerala	340	307	426	626	773
13	Madhya Pradesh	740	602	699	589	826
14	Maharashtra	3511	4967	5496	5562	8249
15	Manipur	29	4	79	67	18
16	Meghalaya	74	89	142	107	75
17	Mizoram	6	8	13	30	1
18	Nagaland	2	2	8	8	4
19	Odisha	843	1485	1931	2037	1983
20	Punjab	239	243	378	551	697
21	Rajasthan	1104	1762	1354	1504	1833
22	Sikkim	1	2	0	0	26
23	Tamil Nadu	295	385	782	1076	2082
24	Telangana	1205	2691	5024	10303	15297
25	Tripura	20	20	34	24	30
26	Uttar Pradesh	6280	11416	11097	8829	10117
27	Uttarakhand	171	100	243	718	559
28	West Bengal	335	524	712	513	401
	TOTAL STATE(S)	**26931**	**44511**	**49708**	**52430**	**64907**
29	A&N Islands	7	2	5	8	28
30	Chandigarh	30	23	17	15	27
31	D&N Haveli and Daman & Diu+		3	3	5	5
32	Delhi	189	115	168	356	685
33	Jammu & Kashmir *	73	73	120	154	173
34	Ladakh	-	-	1	5	3
35	Lakshadweep	4	4	3	1	1
36	Puducherry	14	4	10	0	64
	TOTAL UT(S)	**317**	**224**	**327**	**544**	**986**
	TOTAL (ALL INDIA)	**27248**	**44735**	**50035**	**52974**	**65893**

Source: Crime in India

SL	State/UT	2018						2019					
		CR	CCS	CON	PAR	PCS	PCV	CR	CCS	CON	PAR	PCS	PCV
1	Andhra Pradesh	195	21	0	29	26	0	703	36	0	68	54	0
2	Arunachal Pradesh	0	0	0	0	0	0	0	0	0	0	0	0
3	Assam	6	0	0	6	0	0	83	32	0	58	58	0
4	Bihar	357	227	0	355	328	0	1008	276	4	993	503	17
5	Chhattisgarh	18	4	0	16	15	0	35	14	0	25	25	0
6	Goa	0	0	0	0	0	0	0	0	0	0	0	0
7	Gujarat	139	29	0	197	100	0	107	53	0	242	242	0
8	Haryana	0	0	0	0	0	0	107	6	0	8	8	0
9	Himachal Pradesh	0	0	0	0	0	0	0	0	0	0	0	0
10	Jharkhand	175	5	0	120	120	0	18	2	2	2	2	2
11	Karnataka	49	2	0	0	2	0	7	1	0	1	1	0
12	Kerala	14	1	0	1	1	0	14	7	0	12	12	0
13	Madhya Pradesh	43	19	3	44	44	8	25	6	1	14	18	1
14	Maharashtra	1036	159	0	349	294	0	1681	144	0	289	315	0
15	Manipur	0	0	0	0	0	0	0	0	0	0	0	0
16	Meghalaya	0	0	0	0	0	0	0	0	0	0	0	0
17	Mizoram	0	0	0	0	0	0	0	0	0	0	0	0
18	Nagaland	0	0	0	0	0	0	0	0	0	0	0	0
19	Odisha	392	58	0	59	65	0	956	58	0	70	82	0
20	Punjab	7	3	1	10	10	2	35	4	0	29	5	0
21	Rajasthan	72	5	0	6	6	0	324	14	1	17	17	1
22	Sikkim	0	0	0	0	0	0	0	0	0	0	0	0
23	Tamil Nadu	5	2	0	4	2	0	11	0	0	19	0	0
24	Telangana	347	89	0	242	114	0	282	91	2	172	132	3
25	Tripura	0	0	0	0	0	0	0	0	0	0	0	0
26	Uttar Pradesh	454	204	2	311	312	2	813	367	8	503	491	16
27	Uttarakhand	28	13	0	25	25	0	3	0	0	1	0	0
28	West Bengal	4	1	0	3	1	0	0	0	0	0	0	0
	TOTAL STATE(S)	**3341**	**842**	**6**	**1777**	**1465**	**12**	**6212**	**1111**	**18**	**2523**	**1965**	**40**
29	A&N Islands	2	0	0	0	0	0	0	0	0	0	0	0
30	Chandigarh	2	0	0	0	0	0	0	1	0	0	1	0
31	D&N Haveli and Daman & Diu+	0	0	0	0	0	0	0	0	0	0	0	0
32	Delhi	3	1	0	1	1	0	11	7	0	16	14	0
33	Jammu & Kashmir*	3	1	0	0	1	0	6	0	0	0	0	0
34	Ladakh	-	-	-	-	-	-	-	-	-	-	-	-
35	Lakshadweep	2	0	0	0	0	0	0	0	0	0	0	0
36	Puducherry	0	0	0	0	0	0	0	0	0	0	0	0

	TOTAL UT(S)	12	2	0	1	2	0	17	8	0	16	15	0
	TOTAL (ALL INDIA)	3353	844	6	1778	1467	12	6229	1119	18	2539	1980	40

Source: Crime in India

Note : '+' Combined data of erstwhile D&N Haveli UT and Daman & Diu UT for 2018, 2019
*'Data of erstwhile Jammu & Kashmir State including Ladakh for 2018, 2019

Conclusion and Results:

In today's digital world, cybercrime is growing at an alarming rate in India. With more people relying on the internet for work, shopping, and socializing, crimes like hacking, online fraud, identity theft, and cyberbullying are becoming more common. The legal system is trying to keep up, with laws like the Information Technology Act (IT Act) and the Indian Penal Code (IPC) addressing these crimes, but there are still many hurdles to overcome.

Key Findings:

1. **Rising Cases of Cybercrime**: The number of cybercrimes reported in India is staggering, with over 740,000 cases in the first few months of 2024 alone. The majority of these are financial frauds. This surge reflects how much we depend on digital platforms and how vulnerable we are to cybercriminals taking advantage of these platforms.
2. **Challenges in the Legal Process**: India's courts face many challenges in dealing with cybercrimes. Cybercriminals often operate across borders, making it difficult for law enforcement to track them down. Moreover, the complexity of digital evidence, and the fact that many judges lack specialized tech knowledge, means that handling these cases effectively can be a real struggle.
3. **The Need for Expertise**: Digital forensics experts play a crucial role in these cases, as they help gather and present evidence that can be understood in court. While India has set up specialized agencies like the Cyber Crime Cells and the Indian Cyber Crime Coordination Centre (I4C), there is still a need for more training for law enforcement and judges to handle digital evidence properly.
4. **Specialized Cybercrime Courts**: Some states have set up dedicated cybercrime courts, which help streamline the process. However, these courts are still not widespread, and many cases are still handled by regular courts. This can lead to delays and make the legal process feel more cumbersome than it needs to be.
5. **International Cooperation is Key**: Since cybercrime is a global issue, international cooperation is crucial. India works with agencies like INTERPOL to track down and prosecute cybercriminals who operate in multiple countries. But cross-border cases still pose significant challenges, making global cooperation even more important.

In Summary: India's legal system is working hard to catch up with the rise of cybercrime, but there's still a lot of work to be done. Improving tech education for law enforcement, setting up more specialized cybercrime courts, and increasing international collaboration are all necessary steps. With more awareness and better systems in place, India can make significant strides in tackling the growing threat of cybercrime.

References:

- **National Cyber Crime Reporting Portal (cybercrime.gov.in)**: A platform to report cybercrimes directly to the authorities.

- **National Crime Records Bureau (NCRB)**: Provides annual statistics on cybercrime cases registered across India.
- **State Cyber Crime Cells**: Many states have their own dedicated cybercrime cells that track and investigate cybercrime cases.
- https://cybercrime.gov.in/
- **https:**//cybercrime.gov.in
- https://www.mha.gov.in/MHA1/Par2017/pdfs/par2024-pdfs/RS27112024/234.pdf
- https://aag-it.com/the-latest-cyber-crime-statistics/
- https://delhicourts.nic.in/viewdocuments/QTdPc0VsdjNtNDhWaUV3Z0x3VGVwYTU4NXVNL0hGUUVDYkVydEJFcEZJUGlxT0Yrd01MLzhENWxvVVVDYWFVMnM5bHJkTmVUd29kWmw1STV3L1UwRWc9PQ_EQUALS__EQUALS_
- ANNEXURE-I RS USQ. NO. 234 FOR 27.11.2024
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5001545
- International Journal of Law, Crime and Justice, Volume 43, Issue 4, December 2015, Pages 412-423