A universal study on Cyber Crime and Investigation special reference to Indian Reforms

- **Sonam Research Scholar, Department of Law,**
- **Dr. Mukhram Chouhan Assistant Professor, Department of Law, Shri Khushal Das University Hanumangarh Rajasthan-335801**

Abstract:

The fast growth of digital technologies and communication tools in India has caused a big increase in cybercrimes. Crimes like online financial fraud, phishing, cyber stalking, digital harassment, and even serious forms of cyber terrorism have made the online world more at risk for misuse. The internet's global and ever-changing nature makes it hard for traditional legal and investigation systems to keep up. This paper looks at the current situation of cybercrime in India. It examines the changing trends in cyber offences and carefully reviews the legal tools used to fight them. The paper pays close attention to the roles and performance of law enforcement groups like cyber units, forensic departments, and specialized investigation teams, looking at their preparedness, technical skills, and the challenges they face in dealing with cyber evidence and online criminal groups. The study also highlights major problems such as legal jurisdiction issues, lack of advanced training for law enforcement, low digital awareness among the public, and weak international cooperation. It uses a legal and analytical approach to study important laws like the Information Technology Act, 2000, and relevant parts of the Indian Penal Code, while also looking at new laws like the Digital Personal Data Protection Act, 2023. In the end, the paper suggests practical changes to improve investigation efficiency, update cyber policing systems, and strengthen cooperation both within the country and internationally to build a strong and resilient cyber security and crime prevention system in India.

Keywords - Cyber Crime, Cyber Law in India, Information Technology Act, 2000, Digital Forensics, Phishing and Online Fraud, Cyber Stalking and Harassment, Data Protection Act, 2023, Cyber Security, Infrastructure, Digital Evidence, Cyber Terrorism, Cyber Crime Trends

Introduction: Cybercrime is a general term that includes a wide range of activities, from hacking into computer systems to launching attacks that stop services by overwhelming networks. Computers and the internet can be used as tools, targets, or locations for illegal actions. Cybercrime can also involve using technology to help commit traditional crimes. It can stop trains, send wrong signals to planes, leak important military information to foreign countries, block online media, and bring down entire systems in seconds. The purpose of this research is to explore the different aspects, effects, and future of cyber technology, especially how cybercrime threatens India. The study also looks at the legal frameworks in India that can help deal with cybercrime. To understand this, it's important to first define what crime means. Crime is a concept that varies across societies but is common in all cultures throughout

history. Each society has its own idea of what constitutes a criminal act based on the values and beliefs of the society it governs. Over time, these values have shaped what is considered a crime. As information technology has evolved, so too have the ways in which crimes are committed and the people who commit them. In Indian society, crime definitions have been shaped by religious beliefs, especially during ancient times. During this period, religion played a central role, and many actions, including crimes, were seen as influenced by supernatural forces. This led to the Demonological Theory of Crime Causation. In the middle Ages, there were periods of renewal and change that gave crime a fresh perspective. This era introduced ideas like utilitarianism, positive thinking, analytical approaches, natural justice, and theories based on pleasure and pain, all of which helped develop new ways to understand crime. Later, during the scientific and industrial revolutions, rational thinking became more dominant.

Objectives of the Study

A. Understanding the type and pattern of cyber crime in India

i. Looking at different kinds of cyber crimes such as fraud, hacking, stalking, and ransomware

ii. Checking new kinds of threats like crypto scams, deepfakes, and AI-based

iii. phishing attacks Using official data to look at statistics, where these crimes happen, and who is affected to understand how big and harmful the problem is.

2. India has created a detailed legal system to deal with the increasing problem of cyber crimes. This system includes a mix of specific cyber laws, regular criminal laws, and rules that apply to different sectors. This helps in providing a full legal solution. The main laws are explained below:

A) The Information Technology Act, 2000 (IT Act) The Information Technology Act, 2000, is the cornerstone of cyber law in India. Enacted to provide legal recognition to electronic transactions and combat cyber threats, it was later amended in 2008 to incorporate emerging cyber offenses.

Key provisions include:

 Section 66 – Covers hacking, unauthorized access, and data theft. Punishes any person who dishonestly or fraudulently damages, deletes, alters, or disrupts any data or computer network.

 Section 66C – Pertains to identity theft involving the fraudulent or dishonest use of electronic signatures, passwords, or other unique identification features. Section 66D – Penalizes cheating by personation using a computer resource, commonly applied in phishing, fake job scams, and fraudulent online impersonation.

 Section 67, 67A & 67B – Deal with publication or transmission of obscene material in electronic form.

 67A: Sexually explicit content 67B: Child sexually abusive Section 70 – Designates certain systems as Critical Information Infrastructure (CII), such as systems related to defense, banking, or public utilities, and provides for their protection.

 Sections 71 to 72A – Deal with the breach of confidentiality and privacy of personal information accessed by service providers, intermediaries, or officials. Section 79 – Provides “safe harbor” to intermediaries like social media platforms, subject to them following due diligence and content takedown obligations. The IT Act also empowers the government to issue directives to block public access to certain websites (Section 69A) and intercept, monitor or decrypt information conditions (Section 69).

B. Indian Penal Code (IPC), 1860 specified Although the IT Act is the primary cyber legislation, the Indian Penal Code (IPC) complements it by covering broader criminal behavior, even when committed through digital means. Important sections include

Section 420 – Cheating and dishonestly inducing delivery of property. Frequently invoked in cases of online banking fraud, ecommerce scams, and crypto investment frauds.

 Section 463/465 – Deals with forgery of electronic records.

 Section 499 – Criminal defamation, applicable in cases of reputation damage through social media or email.

 Section defamation. 500 – Punishment for Section 503/506 – Criminal intimidation, often applicable in cyberstalking or threatening The Information Technology Act, 2000messages.

 Section 507 – Criminal intimidation through anonymous communication, commonly invoked in cases involving threatening emails, fake profiles, or hidden phone numbers.

 Section 354D – Specifically addresses stalking, including cyberstalking, where a man follows a woman’s online activity persistently and without consent. Thus, IPC provisions act as a supplementary legal mechanism to ensure that even if certain acts are not directly covered under the IT Act, they do not go unpunished.

CATEGORIES OF CYBER CRIME

Data Crime Data Interception To get information, an attacker watches the flow of data going to or from a target. This could be done to collect data for a future plan, or the data itself might be the main goal of the attack. This is usually done by listening to network traffic, but it can also involve watching other types of data signals, like radio waves. The attacker is often just watching and not actively sending or receiving data. However, in some cases, the attacker might try to create a data stream or change what kind of data is being sent. In most cases, the attacker isn't the person who is supposed to receive the data, which makes this different from other ways of collecting information. Unlike other types of data leaks, this attack involves

watching and accessing actual data streams, like network traffic. This is different from attacks that collect more general data, like the amount of communication, which is not sent through a data stream.

Data Modification To keep data safe, communication needs to be private so that data can't be changed or seen while it is moving. In a networked environment, a harmful third party might commit a computer crime by altering data as it travels between different locations. During a data modification attack, an unauthorized person on the network catches data that is being sent and changes part of it before sending it again. For example, someone could change the amount of a financial transaction from $100 to $10,000. In a replay attack, a full set of real data is sent again and again onto the network. For instance, a genuine $100 bank transfer could be sent 1,000 times.

Data Theft This term is used when information is taken or obtained without permission from a company or another person. Information that is often taken includes user details like passwords, social security numbers, credit card numbers, other personal info, or private company data. Since this information was taken illegally, the person who stole it may face serious legal consequences if caught.

Landmark Judgments

1. **Shreya Singhal v. Union of India (2015)**

(a) Section 66A of the IT Act was struck down as unconstitutional.

(b) Established that vague restrictions on online speech violate Article 19(1)(a).

(c) Read down Section 79, clarifying intermediary liability.

2. **Anvar P.V. v. P.K. Basheer (2014)**

(a) Held that electronic evidence requires Section 65B certification.

(b) Shifted Indian evidentiary law from flexible admissibility to strict compliance

3. **K.S. Puttaswamy v. Union of India (2017)**

(a) Recognized privacy as a fundamental right.

(b) Paved the way for data protection legislation.

Effect OF CYBER Wrongdoing

Crime as a Fiendish Figure of Society

Even in spite of the fact that a crime-free society is a myth, wrongdoing is an ubiquitous, inseparable perspective of social presence. The address, "Why is there so much ado almost wrongdoing?" may chafe a few individuals. No one can deny that wrongdoing is a social

wonder; it is all over, and it is nothing unused; it is one of the characterizing characteristics of all civilizations that have ever existed, civilized or unrefined, and it is one of the most essential slants of all human action! In any case, it is fundamental to keep in mind that tall wrongdoing rates are a source of societal stress not since of their character but since of the potential for social disturbance. Moreover, a few individuals are casualties of wrongdoing more seriously. Casualties of wrongdoing may lose everything they possess. Security, peace, cash, and property are maybe principal values since they offer assistance fulfill different wants.

Impact of Cyber Wrongdoing over Youngster

These days, the most exceedingly bad fear in teenagers' Cyberbullying is bullying through the Web. Concurring to the examination, it has gotten to be broader in the final five a long time, and children beneath eighteen are more inclined to and frightful of cyberbullying. In our culture, it is getting to be a disturbing development. Agreeing to investigate, the most common target of cybercrime is female youngsters. Cyberbullying is a stress that emerges when a individual gets dangers or unfavorable criticism comments, or negative pictures or comments from another individual. This is finished primarily through the utilize of the above-mentioned fundamental advances, which are gotten to essentially through the Web. Chatting, moment informing, and other shapes of cyberbullying can be utilized. Clients of social organizing locales such as Facebook, Orkut, and Twitter are more defenseless to cyberbullying. By and large feared individuals, in my supposition, can reach a point of despairing, mortification, and dangers. We may conclude from this information that if a individual gets Bullied online, they may be discouraged to the point of self-harm.

Effect of Cyber Wrongdoing over Shopper Behavior

The data transformation and the vital utilize of the Web have made a part of by and large open social orders powerless to cybercriminal and cyber-terrorist assaults, especially in commercial commerce operations. This dull commercial side has been known as cybercrime, and it has taken on various shapes that modify our impressions of how we shop online, much obliged to the rise of e-commerce. Organizations ought to recognize that these perils to their online undertakings have key results for their long-term victory. They ought to take suitable steps to kill or impressively diminish these dangers to keep up customer certainty on the Web as a shopping elective. These countermeasures, named "cyber security," were made to secure customer security and data whereas permitting for a worry-free shopping encounter. There is a require to create models that will empower businesses to assess the impacts of cybercrime on online buyer certainty and react by utilizing the benefits of later cyber security headways. With these two perspectives of ecommerce affecting the online buyer, businesses must guarantee that the security measures in put will eventually win out, guaranteeing that clients will proceed to utilize the Web to meet their buying demands.

Passionate Affect of Cyber Wrongdoing

The consider, which is the to begin with to see into the enthusiastic affect of cybercrime, finds that casualties are most likely to feel irate (58 percent), irritated (51 percent), and hoodwinked (40 percent) and that they frequently fault themselves for the assault. As it were 3% do not accept it will happen to them, and over 80% do not think, so cybercriminals will be indicted, driving to an unexpected hesitance to act and a sense of weakness. "We acknowledge cybercrime since of a 'learned helplessness,'" said Loyola Marymount College relate teacher of brain research Joseph La Brie, Ph.D. "It's like getting tore off at a carport — you do not debate with the workman if you do not know anything almost vehicles." Individuals essentially acknowledge a circumstance, indeed if it is unsuitable." Individuals aren't changing their behavior in spite of the passionate toll, the all-inclusive danger, and cybercrime rates, with scarcely half (51%) of grown-ups showing they would alter their conduct if they were a casualty.

A casualty of cybercrime, "I was candidly and fiscally ill-equipped since I never expected I would be a casualty of such a wrongdoing," Todd Vinson of Chicago commented. I felt damaged as if somebody had entered my domestic to get this data and as if my whole family had been subjected to this intolerable wrongdoing. Presently I can't offer assistance but ponder if other information has been gotten unlawfully and is essentially sitting in the hands of the off-base individuals, holding up to be misused." The report's "human impact" segment burrows more profound into the minor violations or white lies that clients commit against companions, family, cherished ones, and ventures. About half of those surveyed accept it is reasonable to download a single melody, collection, or motion picture without paying for it. Twenty-four percent say that surreptitiously seeing somebody else's e-mails or browsing history is allowable or satisfactory. A few of these propensities, like downloading information, uncover buyers to extra security dangers.

Conclusion

The future of the Web is still up for snatches between offenders and regular clients. Fears of a cyber end of the world proliferate, and the breadth of harm that large-scale extortion may cause is essentially perpetual. These tensions ought to be appropriately tempered by the information that the issues are being taken care of, yet gradually. The Internet's advantage has been appeared in a assortment of ways, which ought to be sufficient to keep it from getting to be a center of criminal action and a protect for the fiendish. In spite of the fact that the government has an vital part to play, private computer program suppliers and those with the capacity to distinguish and anticipate extortion must do the lion's share of the work.Others must be secured consequently by non-stressing forms that require noteworthy interest. Security must be straightforward and compelling if it is to succeed. In a few ways, it's incomprehensible to decide whether cybercrime will still be a important issue in ten a long time, but if the Web is to proceed to develop, cybercrime must be illuminated to the point where it's on standard with, if not superior than, real-world violations

References

1. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ijlr.iledu.in/wp content/uploads/2025/04/V4I53.pdf
2. chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.jetir.org/papers/JETIR 2202222.pdf
3. chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ijnrd.org/papers/IJNR D2509185.pdf
4. Rita Dewanjee and Dr. R. Vyas, Cyber Crime: Critical View, vol.5 Issue. 1, International Journal of Science and Research, 85-87, (2016)
5. Sumanjit Das and Tapaswini Nayak, IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES, 6 IJESET, 142-153, (2013)
6. Digital Personal Data Protection Act, 2023 (MeitY). Information Technology Act, 2000.
7. Bharatiya Nyaya Sanhita, 2023 (PRS India).
8. Shreya Singhal v. Union of India, AIR 2015 SC 1523.
9. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
10. K.S. Puttaswamy v. Union of India (2017) 10 SCC 1. NCRB, Crime in India (2021–2023).
11. Times of India and Indian Express reports on cybercrime trends (2023–24).
12. Ministry of Home Affairs (MHA) advisories
13. Various case law from SCC Online, Indian Kanoon.
14. National Crime Records Bureau (https://ncrb.gov.in)
15. The Information Technology (Reasonable Security Practices and Procedures and Senstive Personal Data or Information) Rules, 2011