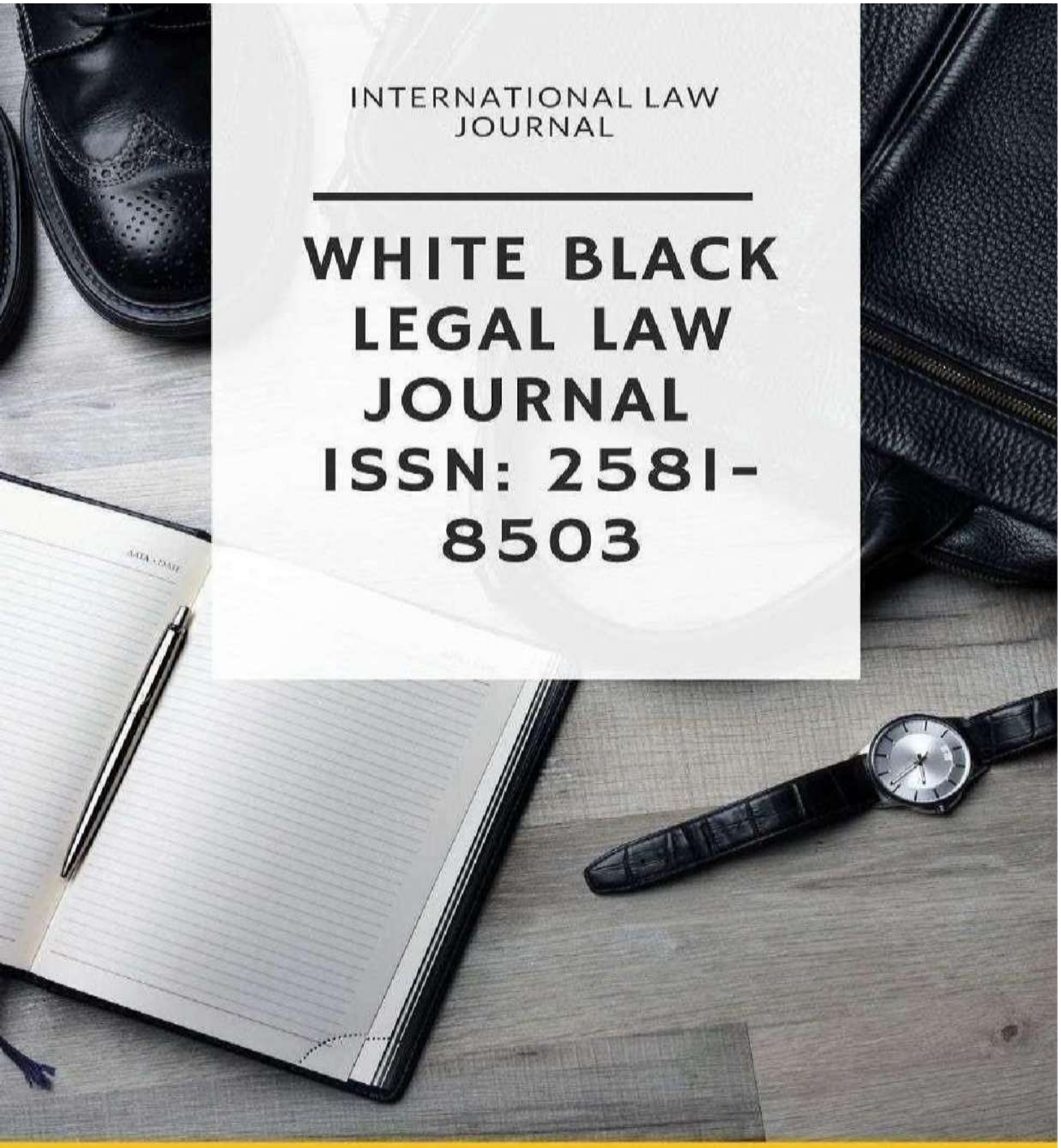

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 2 | Aug 2025 ISSN: 2581-8503

CYBER CRIME AND LEGAL FRAMEWORK IN INDIA

AUTHORED BY - PRACHI & TEJAS BIRLA
COLLEGE NAME: GEETA INSTITUTE OF LAW, PANIPAT (DELHI NCR)

Abstract

In the modern world, the internet has become a regular part of our daily lives. It helps us stay connected, do online shopping, access bank accounts, and find information easily. But along with these benefits, the internet also brings many risks. One of the biggest is cyber crime. Cyber crime means crimes that are done using computers, mobile phones or the internet. It creates many problem likes **cyber bulling, cyber crimes, cyber stalking, hacking, stealing personal information, spreading false or harmful content and other online fraud.** In India, as more people go online, the number of cybercrimes has also increased. This paper looks at how cyber crimes growing and how Indian laws are trying to deal with it.

Information Technology Act, 2000 is the main law for the cyber crime in India. Others act like the **Bharatiya Nyaya Sanhita, 2023** and the **Digital Personal Data Protection Act, 2023** also help protect people from cyber threats. Even though these laws exist, there are many challenges. Many police officers are not fully trained to handle online crimes. Victims often don't report such crimes, tracking criminals in other countries is difficult. The paper also talks about the role of government agencies, global cooperation, and public awareness.

Overall, this study highlights the importance of strong, updated, and practical legal system to deal with cyber crimes. It concludes that continuous improvement in legal measures, better law enforcement, and active participation from citizens are necessary to create a safe and secure cyber space in India.

Keywords: cybercrime, cyber bulling, stalking, hacking, cyber law, world-wide, information, technology etc.

Introduction

Cyber crimes can be defined as "offences that are committed against individuals or group of individuals with criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (network including chat room, email, notice boards and group) and mobile phone.[1]Cybercrime means crimes that are done using computers, mobile phone, or the internet. As our world becomes more digital, cybercrimes is becoming more common. People use the internet for shopping, banking, studying, and staying connected. Cybercriminals take advantage of people by stealing their money, personal information, or even their identity.

There are many type of cyber crimes. Some common examples are include online fraud, hacking into social media or bank accounts, spreading viruses, sending fake messages, and cyber bullying. These crimes can affect anyone like students, workers, business owners, and even the government.

Cybercrimes is dangerous because it can happen without warning and from anywhere in the world. Unlike traditional crimes, the criminal does not need to be physically present. This makes it harder to track and catch them. To fight cybercrime, many countries, including India, have made laws and setup cybercrimes police units. People are also being educated about online safety, like not sharing passwords, avoiding suspicious links, and using strong security settings.

Evolution of cyber crime in India

The emergence of cyber crime is a significant step in human history.[2] Cyber crime in India has come a long way over the past few decades. As technology has grown, so have the ways people misuse it more than to use it in right manner. In the early days, computers and the internet were limited to a few government offices, banks, and big business. But as the internet spread to homes, schools, smart phones, the risks of cyber crimes increased too. In the 1990s, India began to see its first few cases of cybercrimes. These were mostly cases of hacking – where people broke into computer systems without permissions. At the time, there weren't many laws or

[1] Debrati Halder & K. Jaishan kar, cyber crime against women in India.
[2] Dr. sanjeev kumar," Historical genesis and evolution of cyber crime and cyber security laws in India", International research journal of engineering and technology , volume 9 issue:8, Aug 2022.

security system in places, so it was easy for skilled hackers to break in. Most of the targets were large organizations, and the goal was often to steal information or dispute services.

By the early 2000s, with the IT boom in India, internet use became more common. This was also when email scam and virus attacks became popular among cyber criminals. People started receiving fake emails asking for personal details or promising prize money. Some computers got infected with viruses that could damage data or steal passwords. Cyber cafés were popular back then, and they became hotspots for anonymous cyber activists.

As smart phones and digital payments became common in the 2010s, cybercrime took a new shape. Now, the criminal weren't just targeting businesses; they were targeting regular people too. Fake mobile apps, phishing messages, and online frauds became everyday problem. One popular trick s sending SMS or Whats App messages with fake links that, when clicked, would steal money or data from the user. The rise of social media also led to a different kinds of cybercrimes. Identity theft, cyber bullying, and online harassment became serious issues. People started misusing platforms like facebook, Instagram, and Twitter to spread fake news blackmail others, damage someone's reputation.

Digital banking and UPI (Unified payments Interface) made transactions easier, but they also became a target for scammers. Many people fell victim to fraud calls pretending to be from banks or customer support, asking for OTPs or account details. In recent years, India has also seen the rise of organized cybercrimes group. These are not just individuals but entire networks that plan and carry out large scale attacks. They use advanced tools like ransom ware, which locks your data and demand money to unlock it. Some of these attacks have even targeted government websites and major businesses.

The Indian government has taken several steps to fight his growing threat. Laws like the Information technology (IT) act were introduced cybercrimes cells were setup in many cities. Campaigns have been launched to raise awareness about online safety. However, with technology changing so fast, it's constant race between cyber security experts.

Leal framework in India for the cyber crime

As cybercrime continues to grow in India, having a strong legal system to deal with it is very important. India has created specific laws to prevent, investigation, and punish cybercrimes. The main law for cyber crime in India is **Information Technology Act, 2000 (IT Act)**. This act was made to give legal recognition to online activities and to handle crimes done using computers, networks, or the internet. The IT Act defines various types of cybercrimes, such as hacking, identify theft, sending the offensive messages, and stealing data. In 2008, the Act was amended to include new crimes like **Cyber stalking, cyber terrorism, and phishing.** Apart from the IT Act, some sections of **The Bharatiya Nyaya Sanhita, 2023 (BNS)** are also handle cyber crimes. For example cheating by personation using computer (section 319), criminal intimidation (section 351), and publishing obscene material (section 294) can be applied to online cases.

To support law enforcement, India has setup **cyber crime cells** in major cities. These special units help in investigating and solving cyber crimes case. The **Ministry of home affairs** also launched the **cyber crime reporting cells** (cybercrime.gov.in) where people can file complaints online, especially for cases like online fraud and cyber bullying. India is also working with international bodies to fight cross-border cybercrimes. Public awareness campaign are being run to educate people about online safety and legal rights.

Challenges in cyber law enforcement

Cyber crime in India is growing fast, but the law enforcement system is still trying to catch up. There are many challenges that make difficult for police and legal authorities to deal with cybercrimes effectively.

1. **Rapidly changing Technology:** Technology is changing every day. Hackers and cyber criminals quickly learn new methods to hide their identity and attack systems. Laws and enforcement methods often lag behind. It takes time to update laws, while criminals keep getting smarter. With approximately 688 million active users, India is the second largest internet market in the world.[3] Now 900 million in 2025.
2. **Lack of Awareness and Training:** Many police officers and officials are not fully trained in handling cybercrime cases. Unlike traditional crimes, cybercrimes need technical knowledge, such as tracking IP addresses, analyzing digital data, or

[3] Digital population in India as of January, 2020, STATISTA, (JAN, 21,2021).

understanding malware. Without proper training, it becomes hard to investigate and solve such cases.

3. **Jurisdiction Issue:** Cybercrimes can happen across borders. A person sitting in one country can commit a crime against someone in another. This makes difficult for Indian police to catch them. International cooperation is required, and that takes time and legal permission.
4. **Lack of cybercrimes Experts:** There are not enough cyber security professionals working with the police and legal system.[4] Experts who can investigate and present digital evidence in court are limited, especially in smaller towns and cities.
5. **Poor Infrastructure:** Many police stations do not have proper technology or tools to investigate cybercrimes[5]. Digital forensic labs are available only in big cities, so people in rural areas don't get quick help.
6. **Low Reporting by Victim:** Many victim of cyber crime, especially those who face online harassment or financial fraud, are afraid or ashamed to report the crimes. Some don't even know where or how to file complaint. This makes it harder to track the real numbers of cybercrimes.
7. **Legal Loopholes and Delays:** Sometimes the existing laws are not clear or strong enough for new kinds of cybercrimes. Even when a case is filed, legal delays make justice slow.

Judicial Interpretation and Landmark Judgments

The Indian Judiciary has played an important role in shaping how cybercrimes are understood and handled in the country. As cyber laws are still developing, the courts have helped interpret the information Technology (IT) Act, 2000 and related laws trough various judgments. One of the most important cases was **Singhal v. Union of India (2015).[6]** In this case, the supreme court struck down **Section 66A** [7]of the IT Act, which allowed the police to arrest people for

[4] Thomas T. Kubic, Deputy Assistant Director, FBI, before the house committee on crime federal Bureau of investigation, june12, 2001.
[5] Ibid
[6] See R.f.nariman, Indiankanoon.org, shreya singhal v. U.O.I, ON 24 march 2015 SC. 1523.
[7] Information Technology Act,2000
Section 66 A. Punishment to sending offensive message through communication services, etc.
1. Any person who send, by means of a computer source or a communication device-
   a) Any information that is grossly offensive or has menacing character; or
   b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will, persistently by making use such computer resource or a communication device;

posting "offensive" content online. The court said the section was too vague and violated the **freedom of speech** guaranteed under Article 19(1)(a) of the constitution. This judgment protected citizens from misuse of the law and was a big moment in cyber law history.

Another major case was **State of Tamil Nadu v. Suhas Katti (2004).**[8] It was one of the first cases where a person was convicted for **cyber stalking and sending obscene messages online.** The case was handled quickly and set an example for dealing with cyber harassment. The judiciary has also handled cases related to **cyber fraud, data theft, and privacy violation,** interpreting sections of both the IT Act and BNS together. Courts have repeatedly emphasized the need for stronger enforcement and quicker trials in cybercrimes cases.

Role of Regulatory Authorities for Cybercrime in India

In India, several regulatory authorities play a key role in controlling and managing cyber crime[9]. Their main job is to create rules, investigate cyber offences, protect digital infrastructure, and raise awareness. The **Ministry of Home Affairs (MHA)** is the central body for responsible for cyber crime control. It has launched the **National Cyber Reporting Portal** (www.cybercrime.gov.in), where citizens can report online crimes, especially those related to women, children, and financial fraud. The **Indian Computer Emergency Response Team (CERT-In)**, under the **Ministry of Electronics and Information Technology (MeitY)**, handles cyber security incidents. It monitors cyber threats and advises government and private organization on how to protect their system. The cyber crime cells of state police department investigation crime hacking, online fraud, and cyber bullying. These cells often work with forensic experts to gather digital evidence.

Other regulators like Reserve Bank of India (RBI) and Securities and Exchange Board of India (SEBI) also issue cyber security guidelines for banks and financial institution to prevent online financial fraud. Together, these authorities work to ensure India's digital space remain safe.

c) Any electronic mail or email message for the purpose of causing annoyance or inconvenience or to device or to misled the addresses or recipient about the origin of such message, shall be punishable with imprisonment for a term which may extend to three years with fine.

Explanation:- for the purpose of this section "electronic mail" and "electronic messages" means a message or information created or transmitted or received on a computer, computer system, computer resources or communication device including attachments in text, images, audio, vedio, and any other electronic record, which may be transmitted with the messages.

[8] See state of tamil nadu v. suhas katti, 4680of 2004, 5th nov, 2004

[9] Cyber law in India: A comprehensive guide to key regulation, 10 oct, 2024

However, as cyber threats grow, these agencies need more advanced tools, trained staff, and better coordination to effectively fight cybercrime.

International Cooperation in Cyber crime Investigation

Cyber crime is not limited by borders. A criminal sitting in one country can hack a system, steal data, or scam someone in another country using the internet. Because of this global nature, international cooperation is very important in fighting cyber crimes. When a cyber crime involves two or more countries, it become difficult for one nation to investigate or take action alone. Different countries have different laws, language, and legal system to deal with, nation must work together by sharing information, evidence, and expertise.

One important way countries cooperate is through **Mutual Legal Assistance Treaties (MLATs).** These are agreements between countries that help them share legal information and assist in investigation. India has signed MLATs with several countries to get help in cyber crimes cases. India is also a member of organization like **Interpol**, which helps in international investigations. Interpol provides a secure communication network and supports tracking law enforcement often coordinate with Interpol to locate and arrest offenders hiding in other countries.

The **Budapest Convention on Cyber crimes** is the first international treaties that deal with internet crimes. It promotes international cooperation, legal standards, and training. Although India is not a member yet, the country follows many of its principles during investigation. India also part in global forums and training programs to build capacity and stay updated on the latest cyber threats. Agencies like CERT-In collaborate with foreign cyber security teams to share threat intelligence and improve response. However, international cooperation also has challenges. Some countries do not share data easily, and legal procedure can be slow. Political tensions and lack of trust can also affect joint investigation. Data privacy laws in different countries may also restrict how much information can be shared.

Data Protection and Privacy Concern in Cyber crimes

In today's digital world, people share a lot of personal information inline. We use the internet for shopping, banking, studying, and social networking. Every time we go online, we leave behind data such as names, phone numbers, bank detail, passwords, and even our location. This

personal information needs to be protected, but cyber crime makes it a big concern. Cybercriminals often target personal data to commit like identity theft, financial fraud, and blackmail. They can hack into databases, steal user information, and misuse it for illegal purpose. When a company or government agency is attacked, the private data of thousands even millions of people can exposed.

Data protection means keeping this personal information safe from misuse. Privacy means people should have control over how their information is collected and used. But in many cases, users are unaware of where their data is going and hoe its being handled. In India, the **Information Technology Act, 2000** has certain provision related to data protection. Recently, the **Digital Personal Data Protection Act, 2023** was passed to give more rights to users and make companies more responsible for data safety. Still, many challenges remain. Cyber laws are not always clear or updated. Companies may not follow best practices, and users often don't understand privacy settings or risks.

Cyber Crime and Women Protection

In the digital age, cybercrime has become a growing threat to everyone, but women are especially vulnerable to certain types of online crimes. With more women using the internet for education, work, social media, and communication, they are also facing more risks related to privacy, safety, and dignity.

Women face online harassment such as **cyber stalking, threatening messages, morphing of photos, and sharing of private or fake images** without consent. Social media platforms are often misused to send abusive comments, spread false rumors, or create fake profiles. Some women also fall victim to online blackmail or sextortion, where criminal demand money or favour by threatening to leak personal information or picture. Around 50% of the total websites on the internet show pornographic material wherein photos and picture of women and posted online that are dangerous to women integrity.[10] Sites like Facebook, Youtube, Twitter, Instagram, Whatsapp, and snapchat are the most app use by Indian people. According to a report published by IAMAI (Internet and Mobile Association of India) on internet usage in India, about 900 million people use internet only 423 million female use internet and most of

[10] Apoorva Bhangla and Jahanvi tuli pake, A Study on cyber crime and its legal frame work in India, volume4 issue 2

this are fakes.[11]

1. **Emotional and Social Impact:** cybercrimes against women can have serious emotional and mental effects. Victims often feel scared, embarrassed, or depressed. They may stop using social media, avoid public interactions, or even face social stigma. In some cases, online abuse has led to severe emotional trauma and self-harm.
2. **Legal Protection in India:** Indian law provides certain protections to women against cyber crime. The **Information Technology Act, 2000** along with the **Bharatiya Nyaya Sanhita, 2023** includes section to deal with offences like sending obscene messages, stalking, and defamation.

Some important legal provisions include:

- Section 66E of IT Act- Punishes violation of privacy.
- Section 67 and 67A – Deal with publishing obscene or sexually explicit material online.
- Section 78- stalking
- Section 79-Word, gesture or act intended to insult the modesty of a women's.

Victim can report cyber crimes through the **National Cyber Crime Reporting Portal (www.cybercrime.gov.in)** or by visiting local cyber crime cells.

3. **Need for Awareness and Support:** Many women do not report cyber crimes due to fear, shame, or lack of knowledge. More awareness campaigns, support groups, and gender-sensitive police handling are needed to help victim come forward and get justice.

Conclusion

Cyber crime has become one of the most serious challenges in today's digital age. With the rapid growth of the internet, smart phones, and online services in India, cyber criminals have found news way to commit fraud, steal data, and harm individuals and organizations. From financial scams to cyber bullying and identity theft, the nature of cyber crimes is constantly changing and becoming more complex. India has taken important steps to build a legal framework to fight cyber crimes. The **Information Technology Act, 2000** is the primary law like the bharatiya nyaya sanhita, 2023 are also used for crimes such as harassment, fraud, and defamation done through digital means. In addition, **Digital Personal Data Protection, 2023**

[11] India internet 2025, IAMAI

aims to protect the privacy and data of citizens.[12]

Despite these efforts, many challenges remain. Law enforcement agencies often lack proper training and tools. Legal procedures are sometimes slow, and public awareness is still slow. Women and children are particularly vulnerable to online threats. Also, as cyber crimes often cross borders, international cooperation is essential. To make cyber law enforcement more effective, India needs to update its laws regularly, invest in training police and judicial staff, improve digital infrastructure, and promote cyber safety education. Citizens must also be made aware of their rights and safety measures online.

In conclusion, cyber crime is growing threat, but with a strong legal framework, better enforcement, and public participation, India can move towards a safer and more secure digital future.

Reference

- **https://papers.ssrn.com**
- **https://www.irjet.net**
- **https://dict.mizoram.gov.in**
- **https://blog.ipleaders.in**
- **https://ijersonline.org**
- **https://www.nextias.com**
- **https://socialwelfare.vikaspedia.in**
- **https://ncw.nic.in**
- **https://www.researchgate.net**
- **Bare act of BNS,2023 OR IT ACT, 2000**
- **BOOK : CYBER LAWS AND CRIME BY DR. BAROWALIA AND DR.AARUSHI JAIN**

[12] SEE INDIAN DPDP ACT EXPLAINED: THE LATEST GUIDE FOR COMPLIANCE, 17 JUNE 2025