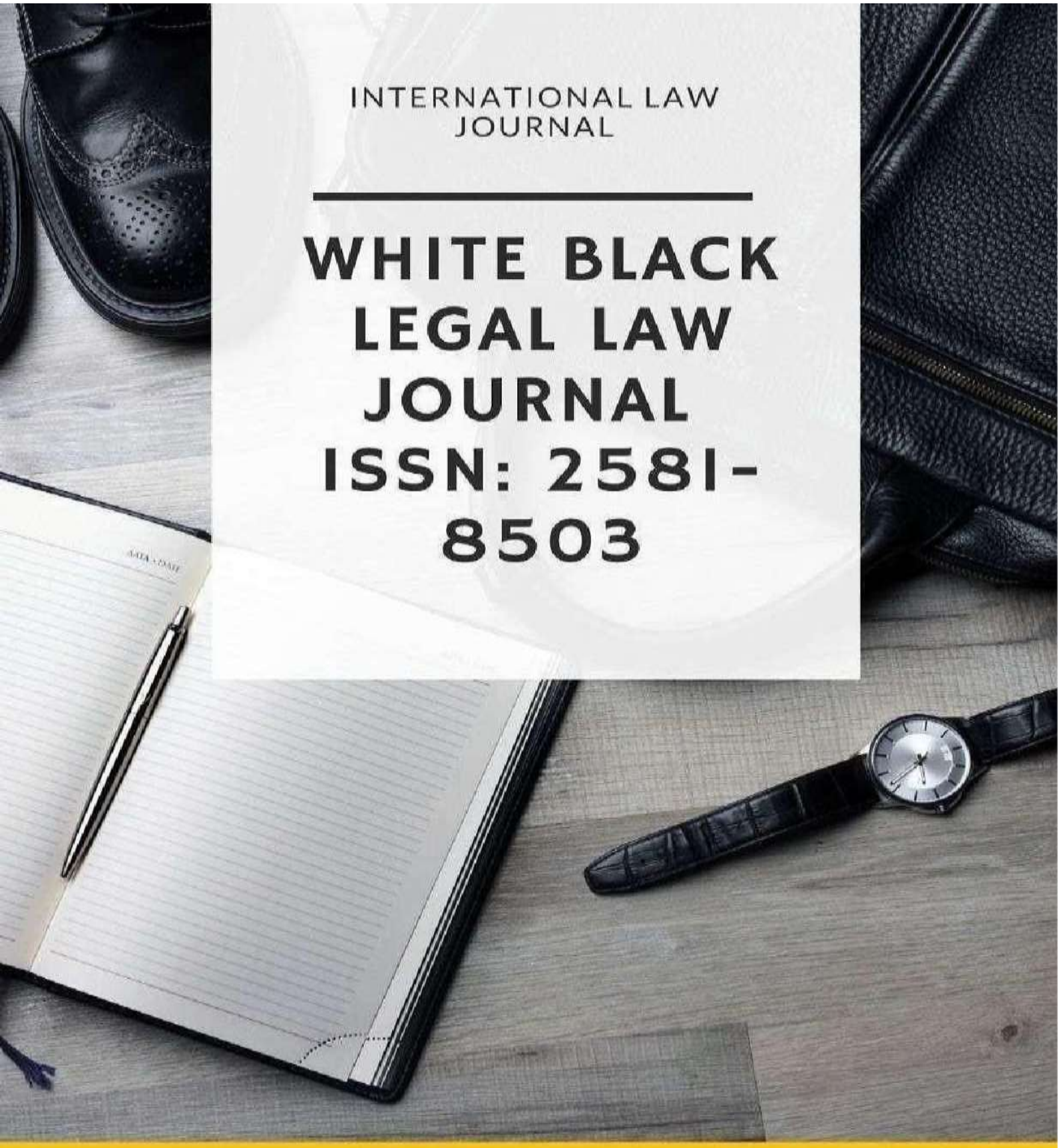

INTERNATIONAL LAW JOURNAL

# 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

www.whiteblacklegal.co.in
Volume 3 Issue 1 | July 2025 ISSN: 2581-8503

# 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 providededicated 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 1 | July 2025 ISSN: 2581-8503

# CYBERCRIME AND INVESTIGATING BODIES IN INDIA: BRIDGING THE GAP BETWEEN VICTIM AND JUSTICE

AUTHORED BY - SHRISTY SINGH

## INTRODUCTION

In recent years of development, India has achieved the milestone of becoming the country with the highest online transactions; along with that, India has now officially become the fourth largest economy in the world, replacing its previous position with Japan; the nation is on its right track of development, but unfortunately, with its tremendous magnification, the crime rates have also increased, particularly a new domain of crime that is to say 'cybercrime' has been emerged. Even in cybercrime, financial fraud is a type of crime that has topped the charts of cybercrime. With the extravagant use of 'online platforms', cyberbullying is also increasing day by day, which leads to 'breaches of users' privacy,' the reason cybercrime is taking place is mainly because of fraudulent and false websites that the user uses and accepting the 'cookies' of various website that provides entire activities of users to the hackers.

With all these developments alongside the crime rates, India's rampant growth in its industries, projects, and infrastructure has also seen the trajectory simultaneously in recent years, in the era where social media platforms have accelerated as a result, the domain of cybercrimes is expected to rise. The crime rates are increasing alarmingly; hence, to minimize the risk and maximize safety, the government and law enforcement agencies should develop strategic action plans to combat and tackle cybercrime.

To bridge the gap between the victim and the wrongdoer, our law enforcement agencies, more precisely, these respective 'investigating bodies', act as a link. These investigating bodies do not just investigate; instead, they safeguard the interest, putting cyber-safety of the citizens at first and law enforcement bodies protect the people from the distress that has caused to them. From national bodies to private bodies, they can investigate the case, and apart from that, they can also collect electronic evidence that can be found helpful for the court proceedings.

The repercussions of any crime would be horrendous, so in the case of cybercrimes, more than the wrongdoer 'victim' became the main culprit of such crime, mainly because of victim blaming. Most importantly, the torment that they suffer from is incomparable, the distress, the trauma they feel completely neglected by society; just because they are the victims of cyberbullying does not make them less of the victim, if the case was murder or some other outrageous crime. The role of investigating bodies becomes crucial as they are the key players who work for the betterment and upliftment of the victims and help the entire nation combat the problem to work together for these vital crimes.

Cybercrime is increasing so rapidly that even keeping track of it seems like a daunting task as already in Indian Courts, the total number of cases pending is to be of fifty-two million[1] meanwhile the cases of cybercrime seem to be contributing to the list of pile up cases as well, cybercrime cases alone have 2.5 million complaints[2].

In today's era of technology, several users of Unified Payments Interface, commonly known as UPI and along with that, millions of users of social media platforms have also contributed to making India an empowering nation that boosts its economy by bringing technology as its key contributor with 18.67 billion transactions[3]. India is leading by becoming the global leader in online payments. Unfortunately, in this digitized era, cybercrime is spreading rapidly, with millions of victims.

Cybercrime is an aggregate, an umbrella term in which various other offenses take place and not just cybercrime as a whole; the other crimes associated with cybercrime are burglary, theft, breach of trust, fraud, defamation, and so on. Cybercrime takes place with the help of a computer, network computer, or with the help of any other computer device. In simpler terms, cybercrime is any usual crime that involves technology. Usually, the hacker or the criminal

[1] Advay Vora, 'SUPREME COURT OBSERVER' (January 2025: Pendency increases by over 2600 compared to last January, 6 Feb 2025) <https://www.scobserver.in/journal/january-2025-pendency-increases-by-over-2600-compared-to-last-january/> accessed 7 June 2025.

[2] 'THE ECONOMIC TIMES'(Indian entities may lose Rs 20,000 Cr to cybercrimes in 2025: Cloud SEK Report, 1 March 2025) <https://economictimes.indiatimes.com/industry/banking/finance/indian-entities-may-lose-rs-20000-cr-to-cyber-crimes-in-2025-cloudsek-report/articleshow/118651127.cms?from=mdr> accessed 10 June 2025.

[3] PIB Delhi, 'Government of India Press Information Bureau' (pib.gov.in/Press Release frame Page PIB.GOV.IN, 27 February 2025) <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2106794#:~:text=present%20among%20others.-,Unified%20Payments%20Interface%20(UPI)%20provides%20an%20opportunity%20to%20other%20countries,retail%20payments%20across%20the%20> accessed 10 June 2025.

commits the crime with two major intentions: first, for the wrongful gain in monetary terms, and second, for extorting the essential documents or data that the hacker may use for blackmailing or for committing some other offense in that very genre.

The hacker targets both the individual and company; in the case of companies, the hacker hampers them by extorting money, gaining any illegal money, or sabotaging any ongoing or future endeavors of the company, whereas in the case of individuals, these hackers' jeopardies the individual by trapping them into scams by playing with their vulnerability and provoking them to surrender themselves to these scamsters. In the ordinary course of life, it is the human tendency to act under pressure when there is a time bound attached to their work, as in the case of cybercrime; the behavior of such hackers when committing cyber-bullying does not change, but it remains the same; they act in haste, and it becomes extremely tough to comprehend the repercussions that the victims are going to face if they disobey the hackers. Ultimately, scamsters have complete control in their hands.

Government agencies, business companies, and enterprises heavily rely on the data and figures curated by social media and other reliable sources for their operations, the latest news, investigations, etc. However, due to the immense growth of cybercrime, the reliability is now reduced alone in 2025, it is estimated that India may lose a whopping amount of ₹20,000 crore to cybercrime.

Cybercrime has affected different areas of interest and has had a drastic impact on the nation, from places like the financial sector where the hackers have committed theft, burglary, and extortion because of which it has caused monetary loss, affecting companies in different ways, such as maximizing financial plan, generating revenue, to the public who have lost their interest and trust from these companies, not just in this one sector but in areas like the healthcare sector where the hackers have installed malware, a type of virus, in the computer system of the hospitals, collecting all sorts of data of the patients illegally, like their sensitive information breaking the doctor-patient confidentiality, eventually hackers can exploit this sensitive information for some further illegal monetary gain.

## TYPES OF CYBERCRIME

I. *Phishing*: By fraudulent means or by disguising oneself as a credible person, the hacker derives the personal and sensitive information of the victim, such as their username, password, and credit card details. In phishing, generally, hackers send fraudulent e-mails, messages, links, and QR codes to trick people into sharing their personal information, and as a result, the victims suffer monetary loss.

II. *Spamming*: Is an unsolicited and irrelevant text message or e-mail sent in bulk mostly to all internet users, mainly associated with advertising their product or company.

III. *Spoofing*: When the senders send mail from a fraudulent and incorrect e-mail address to the recipient, these e-mails ask for the personal details of the recipient or any other sensitive data; when the recipients allow these e-mail addresses, they fall for this trap of fraud as the websites are already connected to malware.

IV. *Cyberstalking*: The individual, group, or organization is harassed or stalked on the Internet or by another electronic means; it often attracts defamation, harassment, slander, and libel.

V. *Hacking*: By illicit and unnotarized means, the hacker breaks down a computer or any other electronic device and unlawfully steals the essential data to gain some profit. As per Section 43[4], it suggests whoever uses, harms, or interferes with somebody else's computer, electronic device, or data without seeking their permission or if anybody finds helping in committing the same, then in the said case, the person will be held liable to pay the compensation for the damage that the victim incurs. Sec 66[5] comes into play as it outlines the punishment for the offense caused in sec 43, which is that the person will be imprisoned for three years and liable to pay a fine of five lakh rupees.

VI. *Identity Theft*: Punishment for identity theft has been defined under section 66 (c)[6], which states that in cases of theft or any other case of cybercrime, the hackers have the entire sensitive data and personal information of the other person, such as their name and password, and credit card, which they can further use to gain some unlawful gain or to commit further related crimes if anyone is found to commit said offence then they will be imprisoned for a term of three years and shall also be liable to pay a fine of rupees one lakh or more.

[4]The Information Technology Act 2000, s 43.
[5] The Information Technology Act 2000, s 66.
[6] The Information Technology Act 2000, s 66 (c).

VII. *Cyber obscenity*: Sec 67, 67A, and 67B are clubbed together as these sections together talk about the punishment if the person commits cyber obscenity and pornography.

Sec 67[7] states that if the person sends the obscene material in electronic form, there will be imprisonment of five years and a fine of rupees ten Lakhs.

Sec 67A[8] states that if the person sends any material that is sexually explicit via electronic means, then imprisonment of seven years and a fine of rupees ten Lakhs will be imposed.

Sec 67B[9] states that whoever shares any material that depicts children in an explicit form via electronic means will be imprisoned for seven years, and a fine of rupees ten Lakhs will be imposed.

VIII. *Cyber defamation*: When the offender jeopardizes the reputation of the victim online by stating some false allegations, posting violent videos or photographs, or writing something offensive about them online.

Cyber defamation is not defined either in Bhartiya Nyaya Sanhita or in the Information Technology Act of 2000, and only as per Section 499 of IPC[10] and Section 356 of BNS[11] defines defamation.

Cybercrime can also be portrayed as a bouquet where each label represents the crime, scams of various kinds, from traditional e-mail scams where the misleading e-mails have portrayed themselves to be authentic but instead they are just a sham, to emerging scams such as social media scams where platforms like Facebook, Instagram, Twitter consist of plethora of fake and dummy accounts that catfish and defraud the victims and apart from that they also encourage violent behavior, to cease this activity social media platforms have come up with community guidelines to protect the privacy of the victims.

## INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act 2000[12] is a cornerstone in the Indian domain for combating cybercrime, regulating electronic commerce and digital communication, and protecting digital privacy.

[7] The Information Technology Act 2000, s 67.
[8] The Information Technology Act 2000, s 67 (A).
[9] The Information Technology Act 2000, s 67 (B).
[10] Indian Penal Code 1860, s 499.
[11] Bharatiya Nyaya Sanhita 2023, s 356.
[12] The Information Technology Act 2000.

To protect the interest, to cease the breach of privacy of users of social media platforms, and to protect the integrity of the government that heavily relies on online resources from various credible sites, the Indian Parliament introduced the Information Technology Act of 2000, also known as IT Act, 2000; this act curates for lawfully conducting the digital transactions and to curb the growth of cybercrime.

The bill of this act was passed in the Budget by parliamentarians, and the group was headed by then Minister of Information Technology Mr. Pramod Mahajan. Later, the bill became an act when former president Mr. K.R Narayanan signed it on May 9, 2000 and ultimately came into effect on October 17, 2000.

To protect the country's sovereignty, the existing laws must act in such a way that they maintain law and order and curtail the crime rate. Currently, in India, the only act that briefly discusses cybercrime and electronic transactions is The IT Act of 2000; its main objectives are as follows:

- Penalties for data theft, spoofing, spamming, cyberbullying, cyberstalking, and so on have been made necessary so that internet users feel safe and sound.
- The act is the sole framework that provides rules and regulations on cyber activity and where the mode of communication is electronic.
- It further encourages ideas, projects, and encourages innovation and entrepreneurship in IT sectors.
- It gives legal validity to electronic records, contracts, and documents, making them as valuable and necessary as any other evidence, that is, to make them admissible in court.

## AMENDMENT OF THE INFORMATION TECHNOLOGY ACT, 2000

With time, the need for better laws became necessary as crimes are now spiking in such a short period, with an evolving and never-ending society for such reasons, the Parliament has come up with the Information Technology Act, 2000 so that they could try to reduce the ongoing concern with the cybercrime.

The act primarily deals with tackling cybercrime, maintaining cybersecurity, and allowing credible and transparent electronic commerce; it also recognizes electronic records, contracts, and evidence, which shall be admissible in a court of law. The act has laid down sections defining cybercrime, types of cybercrime, and punishments.

As the digital world started to progress it became prudent to act more diligently to bring new laws for tackling crimes with more stringent plans and make them more advanced and efficient. Two significant amendments were brought in the Information Technology Act 2000.

- The IT (Amendment) Act of 2008

  This amendment brings some necessary changes that were previously absent from the main act. This amendment is a mere stretch and concentrates primarily on the needs of citizens and proceeds to bring more refined changes in the sections.

  The Parliament passed the IT (Amendment) Act of 2008 in December 2008, and the president gave their assent in February 2009, the bill introduced by former Minister of Communications and IT, A. Raja. The act came into force in October 2009.

  The main change that the act brought was making electronic signatures relevant. In this way, the electronic signature on data, records, and contracts will be valid and, hence, admissible in court.

  Because of the amendment, it has introduced Section 66 A[13], which states that if any person is found guilty of sending 'offensive messages' while communicating, then the person will be imprisoned for a term of three years and liable to a fine.
- The IT (Amendment) Bill, 2015

  Section 66 A makes the act of sending offensive and derogatory messages or any information by computer or any other computer device.

However, this section was violative of Art 19[14] (freedom of speech and expression) and Art 21[15] (right to life and personal liberty) mainly because of a few primary reasons these are as follows:

Firstly, as per the said act, it does not define what particular 'words' make the information offensive, or which word will trigger and attract art 19 or 20; it must provide with a clear definition.

Secondly, this problem has made the line of violation blurry, because of which any person would file a complaint if talking about this section particularly. There is no straight-jacket formula for identifying which word will become 'annoyance' or 'grossly offensive' as the idea

[13] The Information Technology 2000, s 66 (A).
[14] The Constitution of India 1950, art 19.
[15] The Constitution of India 1950, art 21.

here is that everyone is different from one another in the same manner. For anyone, any word may be offensive, but for another, it may not. In inconsequence, section 66 A became 'subjective' in nature and law as a field that believes in certainty. As a result, said section completely fails to stand; hence, section 66 A was held ultra vires and was omitted.

To limit the surge in rampant cybercrime cases, the government of India has established investigating bodies. These bodies not only help to implement the laws but also tries to bring new vision in the society, these are as follows:

1. *Indian Cybercrime Coordination Centre (I4C)*

   It is the nodal agency, an initiative by the Ministry of Home Affairs, it came into existence in 2020 with an objective to protect netizens from cybercrime and familiarize them with its pattern and provide with the long-lasting solution; it is a parent body under which plenty of agencies come into place. This body bridges the gap between law enforcement agencies and netizens, so the concept should be familiar and make the entire process transparent for both sides. It focuses on solving the problem that hampers the said act's effect, such as improving coordination between various agencies and laypeople.

   Since this scheme has come into existence, it has worked to achieve the nation's goal of development and security. Cybercrime is spreading internationally and nationally, making coordination amongst the various agencies essential for the initiative to be carried out perfectly.

   To solve cybercrime, I4C came up with an ‘expert group.’ These groups of experts will find the dip where the problem arises and prepares their report to resolve the issue as soon as possible; once these expert groups see the problem and make the ways by which they may solve the problem with then they make recommendations to the agencies they may think fit. I4C makes the entire process of filling out the report easy and time effective. It also works to increase the number of police officers and judicial officers in all states and UTs in the areas of cyber investigation, forensics, and so on.

2. *National Cybercrime Reporting Portal*

   It helps victims to file their complain on an online portal; this portal is user-friendly, especially for women and children, so they can report the crime anonymously and privately. The victim must share only the necessary details. The portal is available for all kinds of cybercrime, such as phishing, spamming, hacking, spoofing, etc.

   After lodging their report online, the complainant can track their report's progress,

making the entire process transparent, safe, and reliable.

3. *National Cyber Forensic Laboratory (NCFL)*

   Set up in Delhi, a laboratory for the forensic analysis and investigation of cybercrime with the help of the latest technology for the investigations taken up by law agencies. By identifying the evidence found at the crime scene helps the team to figure out the elements of cybercrime and further helps to lead the investigation.

   In a digital world where crime is also present in online mode, the need for online investigation has become important; hence, NCFL is necessary.

4. *National Cybercrime Training Centre (NCTC)*

   It offers a standard course for the prevention and curbing of cybercrime that has a direct impact on society at large. It also offers practical cybercrime detection, which helps the officers to provide them with a caricature of the real problem that may arise in the future; it replicates the crime by which the officers must act exactly like they might do on an actual crime scene. It helps to train their mind by giving them the exact environment of the tense situation.

   It also constitutes Cyber range for the advanced level environment, which would train them for future endeavors.

## TIMELINE OF CYBERCRIME CASES

Law, with time, has evolved over the years with an increase in technology, gadgets, and overall growth in the recent years; earlier, particularly in the Indian context, the concept of 'cybercrime' and 'cyber activity' was alien. No one knew any information on this topic, and even if they did, it was in bits and pieces; with the fastest growing economy, being the most populated country, and lack of awareness, by combing all these factors together it thus makes the nation prone to cybercrime more easily.

Throughout the years, the Hon'ble Supreme Court and High Court have come across with variety of cases as the society evolved and now in the era of Internet they also come across 'cybercrime,' where they deliver judgments on the said topic and are trying to make their stance on the subject matter.

As in the case of *Yahoo!, Inc. V. Akash Arora* (1999)[16], this case was the first to appear in India.

[16] *Yahoo!, Inc. v Akash Arora* (1991) IIAD DELHI 229.

Akash Arora (Defendant) created a website named Yahooindia.com that replicates Yahoo!, an American webpage that provides a platform for e-mails and news from around the world.

The defendant faced repercussions as he was found guilty of copying the name of the webpage that already has a trademark, misleading the internet users, and giving them thought that yahooindia.com is an exaggeration of Yahoo! Hence, the Delhi High Court ruled in favor of Yahoo! by giving importance to Intellectual Property and domain names under trademark law.

Tarnishing anyone's reputation, digging their name into mud, making false accusations, and creating fake and fabricated news these all factors are clubbed together to form an offence named 'defamation' defined under Section 356 of BNS and earlier in Section 499 of IPC; this offence comes under Law of Torts, a civil wrong; if anyone is found guilty of defamation, then they will be incarcerated for a term of two years and will also be accountable to pay fine as per Section 500 of IPC[17] and now Section 356 of BNS.

The same was the scene in *State of Tamil Nadu v Suhas Katti* (2004)[18] herein; the defendant was a friend of Ms. Roselind (victim) as she denied the defendant's marriage proposal; as a result, he harassed her, posted illicitly, and false information of her online, posted her phone number online because of which she also received obscene phone call. The plaintiff complained to the police station, and the defendant was booked under Section 469 of IPC[19], now Section 339 of BNS[20], which deals with forgery to harm reputation, Section 509 of IPC[21], now Section 79 of BNS[22], which deals with insulting modesty of a woman, and Section 67 of IT Act, 2000[23] that deals with publishing obscene content online. The court ruled in favor of the victim by giving the accused imprisonment of two years and charged him to pay a fine of rupees four thousand under section 67 of the IT Act, 2000.

Cyberattacks are strong and attract more danger when it comes to different variations of cybercrime; with multiple international tie-ups, with different collaborations on various overseas projects, cybercrime can severely damage these relations easily by targeting the

[17] Indian Penal Code 1860, s 500.
[18] *State of Tamil Nadu v Suhas Katti* (2004) CC No. 4680 of 2004.
[19] Indian Penal Code 1860, s 469.
[20] Bharatiya Nyaya Sanhita 2023, s 339.
[21] Indian Penal Code 1860, s 509.
[22] Bharatiya Nyaya Sanhita 2023. S 79.
[23] The Information Technology Act 2000, s 67.

software, introducing malware, thus resulting in retrieving sensitive information. As seen in the COSMOS Bank Cyber Attack held in 2018, where hackers stole a whopping amount of rupees 94.42 Crores by installing malware into the bank's ATM server in Pune's COSMOS Cooperative Bank, by acting maliciously, the hackers intruded with the security system of the bank and gained ill-gotten money therefore, the negligence on their path caused India's most significant cyber-attack.

## WAY FORWARD

No wonder the Internet binds urban and rural India together; with the help of the Internet, the nation has been able to achieve connectivity, bring digitalization, enhance the scope of communication, bridge the gap amongst nations, strengthen ties, make trade and business easy, and efficient, and so on. However, somewhere along the line, cybercrime has activated and has spread like no other, where netizens are already facing problems due to crimes. Now, cybercrime has also become part of the list. The Internet can be a dark place if not stepped correctly, but by acting cautiously, one can put a stop on cyber-attacks and cyberbullying.

The height at which cybercrime has increased in recent years is triggering for every one of us, especially for the youth, as 55.3% of the nation's youth are active users of the Internet, and out of this percentage, we get the actual number of hackers and cybercriminals mainly.

The issue has now deepened in recent times with new technologies and gadgets, the problem has just escalated, and to de-escalate the situation, the government, ministry, and law enforcement agencies must develop certain action plans. In the age of social media, AI has also emerged. In its presence, it has contributed the most to cybercrime, not only in framing the victim but also in impersonating the culprit into someone who may have direct connections with the victim and can easily attack their vulnerability; that is how both AI and cybercrime go hand in hand. They complement each other very well by helping execute perfect cybercrime.

Furthermore, it is not just about AI but also of the variations of AI, the tools that are now out in the world, are pretty easy to access but are incompetent, as stated in the latest reports by Forbes 16 billion passwords of users from the entire world like in Apple, Google, Facebook

and other platforms have been leaked[24]. Data protection is not a light work to procure, and for the people working behind these giant companies their work is to be trying and saving to protect people from data getting breached but is all a sham. It is so hard to digest that the violation of rights, more precisely cyber rights, is getting easier day by day.

Policymakers are trying to change the entire scenario of the nation by improving the nation's current deteriorating conditions in area of cybercrime. However, in this case of causality, the question of protecting cyber rights and safeguarding people's interests becomes questionable because of the significant leak of passwords. This has caused an escalation of misconduct and hampers safety concerns for users, thus raising questions about the department's arrival with a new and stringent action plan.

The act has laid down enormous sections explaining e-transactions, cybersecurity, and cybercrime. However, the act has failed to dig deeper into 'cyber law.' Society is not perfect; these imperfections resonate with time, and as society evolves, it attracts new crime, thus making strong requirements of stringent laws; the same is in the case of said act as well. Herein, the most highlighted shortcoming that the lawmakers come across is 'unaware of rights'; the society is itself not aware that they possess cyber rights, and the question of violation of such shows the incompetencies of the system and the executive branch. People do not even know that they possess such rights, which would help them in ascertaining their value and reputation, and even if someone tries to violate their rights, there are very rare occasion when they get punished for their wrong.

Another thing is that Indian courts already face a problem of piled-up cases because of several factors, such as an inadequate number of judges, low judge-to-population ratio, and limited use of technology. On top of that, these cybercrime cases have also been added to the list, making court to work with more haste, for soling the query fast-track cybercrime courts have become crucial. In an initiative by the Ministry of Home Affairs, they recently introduced 'e-Zero FIR' by making lodging an FIR for cybercrime easy, especially for high-value financial fraud cases. Section 173(1) briefly talks about information in cognizable cases and talks about Zero-FIR, which means that anyone can proceed to file their FIR even in a police station that is outside

[24] Davey Winder, 'Forber' (16 Billion Apple, Facebook, Google And Other Passwords Leaked, 20 June 2025) <https://www.forbes.com/sites/daveywinder/2025/06/20/16-billion-apple-facebook-google-passwords-leaked---change-yours-now/> accessed 20 June 2025.

of their jurisdiction. Once an FIR has been filed, the police shall proceed with their investigation once the case is transferred to its proper jurisdiction. E-Zero FIR or Electronic-Zero FIR is same just like Zero FIR with no difference in concept whatsoever. The only distant feature between the two is that FIR is in electronic form in the former, and in the latter, it is not.

Suppose the financial fraud occurred in the amount of ten lakh or more, and the complaint was filed through the National Cybercrime Reporting Portal (NCRP). In that case, the complaint will be converted into an E-Zero FIR instantly without any hurdle.

With time things have emerged and some were invented with the help of Internet from technology to latest developments no doubt these have helped the society at large and freed them with daily life struggles but it is not always perfect as it seems to be. Along with Internet it has created cybercrime that has severely hampered not only individuals, but also targeted businesses, corporations and so on. But with the law enforcement agencies and their stringent action plan the future of netizens looks promising.