**ISSN (O): 2584-2196**

# INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND EXPLORATION

**Volume 3 | Issue 1**

**2025**

**Website: www.ijlae.com**
**Email: editor@ijlae.com**

**ISSN (O): 2584-2196**

# INDIA'S REACTION TO CYBER CRIMES, FROM THE JUDGEMENT AND THE LAWS

***Fatehh Singh Majithia***

***Amity university Noida***

## INTRODUCTION

The internet is a worldwide platform. Being a powerful region in the world, India also felt a shift in the technological setup that occurs with the waves of information technology accelerated and made the establishment of the Ministry of Information Technology necessary in the nation during 1999.The information society, of course, provides a wide range of together with chances for people to recognize information, assess information, additionally, to share information for the benefit of people worldwide. The Information technology creates a new workplace culture, new surroundings, and new networks for trade and business. It permits knowledge-based and information-based work to exist anywhere. It is revolutionizing and essentially changing the planet. Because of the intrinsic lack of spatiality and time in cyberspace, new types of e-trade that was nonexistent before. Cybercrime is becoming a problem for economic and national security. Numerous institutions, businesses, and both governmental and private organisations in the industry, especially those in the essential infrastructure, are at substantial danger. In contrast, some organisations have discovered organized cybercrime and criminal networks as the biggest risk to cyber security, and some are prepared to protect against such security risks[1].

The growing prospects for productivity, efficiency, and globalization communications attracted a large number of new consumers. The dependability and accessibility of one of the most important operational factors is the internet. Actions that put these at risk its user community is severely impacted by features like spamming, spoofing, etc. The activity of solicitors and legal experts is also included in the developments interest in regulating the legal industry has grown in what appears to be a significant step in the profession's advancement

[1] Abhijit Kumar Pandey, "Cyber Crimes in Cyber Age and its Response by Indian Judiciary", available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1097695>, accessed on 22/04/2025.

considering the significance of this essential sector and its significant impact on the legal system[2].

Due to the exponential growth of cybercrime worldwide, anyone involved in the illegal the realm of justice has lacked current and appropriate understanding about pedestrians reality of contemporary cybercrime. The perception of cybercrime has been shaped by popular media. It implies a single hacker circumventing seemingly insurmountable security measures to gain access to profitable confidential information. These kinds of crimes are extremely uncommon, but cybercrime is all too typical[3].

It is possible to visualize the increasing significance of information technology from the reality that a businessman from Delhi has made a maiden venture in India digital will containing the confidential data stored in his email account. Will digitally is a foreign idea that is also gaining traction in India. The effectiveness of the country's legislative, judicial, and executive branches is what makes it strong authorities. The judiciary's role is to advance equality and justice by means of the appropriate implementation of laws and rules to ensure that each person receives what is rightfully his[4].

The court and legislature are crucial components of any nation's success in fostering positive international ties, drawing in investment, and enacting adequate legislation. To gain the trust ofthe public, a contemporary and equitable legal system is necessary, worldwide community and for the coordinated efforts of multiple organisations in in order to accomplish the intended goal. For society to function, there must be a certain amount of continuity and order in a decent and systematic manner, as safety and security have long been just a concern about safeguarding against physical threats since the previous century, the ancient world and online coexisted. Using this conventional offline the world needs a better legislative response. The current

---

[2] Christine Conradt, "Online Auction Fraud and Criminological Theories: the Adrian Ghighina Case", International Journal of Cyber Criminology, vol. 6, No. 1, Jan.- June, 2012, p. 912 available at: <http://www.cybercrimejournal.com/christine2012janijcc.pdf >, accessed on 22/04/2025.

[3] Atul Bamara, Gajendra Singh, et.al., "Cyber Attacks and Defense Strategies in india: An Empirical Assessment of Banking Sector", International Journal of Cyber Criminology, vol. 7 No. 2, Jan.- June, 2013, pp. 49-50 available at : <https://www.researchgate.net/publication/236682638_ Cyber_Attacks_and_Defense_Strategies_in_India_An_Empirical_Assessment_of_Banking_Sector>, accessed on 22/04/2025.

[4] Hassan Arab, "The Development of The Judiciary- Challenges and outlook", available at: <http://www.tamimi.com/en/magazine/law-update/section-7/October-november-1/the-developmentof-the-judiciary-challenges-and-outlook.html>, accessed on 22/04/2025.

**ISSN (O): 2584-2196**

chapter makes an effort to been created to talk about the national legislation enacted to stop cyberattacks offences in India. The following is a discussion of these:

## THE INFORMATION TECHNOLOGY ACT OF 2000

The use of electronic means for international trade was growing daily, and numerous E-commerce has replaced conventional paper-based commerce in several countries. With as trade and business became more globalized, the world community realized that a law that would establish consistent guidelines for online sales. This idea prompted the United Nations to approve the Model Law on Electronic Commerce UNCITRAL, the Commission on International Trade Law[5].

The first piece of legislation passed by the Indian Parliament in the 51st year of the Republic known as the Information Technology Act 11 of India 2000, which is predicated on the resolution approved by the UN General Assembly with reference to the Model. The January 30, 1997, Law on Electronic Commerce, which was first approved by the UNCITRAL stands for United Nations Commission on International Trade Law. This resolution suggests that this model be given favorable attention by all states law when states are planning to pass or amend their legislation with the intention of consistency of the law as a substitute for communication methods based on paper and information storage. Additionally, India signed this Model Law and was required to

amend its national laws in accordance with the aforementioned Model Law. Consequently, India also passed the Information Technology Act of 2000, which gives the transaction legal recognition

conducted via electronic data interchange and additional technological methods correspondence and to make it easier to electronically file papers with the government organisations. Additionally, the Act modifies the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Reserve Bank of India Act, 1891, and the Bankers Books Evidence Act, 1934[6].

[5] Jose R. Agustina, "Exploring Internet Crimes and Criminal Behaviour", Book Review of Cyber Criminology, vol. 6 No. 2, July- Dec., 2012, p. 1044, available at: <<http://www.cybercrime journal.com/Augustinabookreview2012julyijcc.pdf,accessed on 22/04.2025
[6] Ibid.

**ISSN (O): 2584-2196**

Certain documents are exempt from the provisions of this Act, such as negotiable any other testamentary document, such as a will, trust, power of attorney, or disposal, any agreement for the purchase or transfer of real estate, or any stake in the property in question as well as any type of transaction or document that may be published in the Official Gazette by the Central Government.

Although India's Information Technology Act has been in effect since 2000 to reduce cybercrimes, however the issue is that this law is still more based on paper than on execution because judges, prosecutors, police officers, and attorneys feel disabled difficulty comprehending its extremely complex jargon. First and foremost, the IT Act of 2000 is intended as a law to encourage e-commerce, but it isn't particularly successful in addressing a number of additional new cybercrimes, including as defamation, cyber-harassment, stalking, etc. The Information Technology Act of 2000 needed to be amended for the with the intention of making it more pertinent to the situation of today. In order to achieve this, the 2006 Information Technology (Amendment) Bill was put forth, and it was further modified by the 2008 Information Technology (Amendment) Bill, which was approved in Lok Sabha on December 22, 2008, and in the Rajya Sabha on December 23. Next, The Information Technology (Amendment) Act amends the Technology Act of 2000[7].

## INFORMATION TECHNOLOGY ACT OF 2000 AMENDMENTS TO VARIOUS LAWS

Additionally, the Information Technology Act of 2000 was passed with the additional goal of modify the Indian Evidence Act of 1872, the Indian Penal Code of 1860, the Reserve Bank of India Act of 1934 and the Bankers Books Evidence Act of 1891 as stated in its justifications and objectives. To accomplish the goals of the IT Act, resulting changes were made to the aforementioned Acts because according to the Model Law, there must be no distinction made between the typical records, both electronic and paper. The laws listed below were modified in a result of the IT Act of 2000. These are listed as follows[8]:

[7] It received the assent of the President on June 9, 2000 and notified in the Official Gazette on October 17, 2000.
[8] Supra note 54.

**ISSN (O): 2584-2196**

**Modifications to the 1860 Indian Penal Code**

Some changes have been made to the Indian Penal Code by the Information Technology Act of 2000. These changes have been implemented in accordance with the First the Indian Penal Court's extraterritorial jurisdiction. Additionally, Code, 1860 was broadened to cover all offences that affect computers. India-based resources and certain portions pertaining to a fraudulent document were moreover changed to incorporate a fraudulent electronic record. With these changes after then, section 29 A, which specifies the term "electronic record," was added section 29, which provides a definition of "document" in order to preserve the statutory balance.

For the phrase "such public servant, charged with the preparation or repair of translation of any document, either by framing or translating it," the phrase "such public official tasked with preparing or translating any kind of document or the term "electronic record" has been replaced. The Act modifies this section, which addresses the intentional harm caused by a public servant creating an inaccurate document, by changing the phrase to "electronic record." A public servant as a result of this amendment could face charges for intentionally harming someone by fabricating an inaccurate electronic record.

Absconding to avoid being served with a sentence is punishable under Section 172. summons, notice, or order, and section 173 penalises deliberate obstruction of the serving an order, notification, or summons. By using "electronic record" instead of a person will be held accountable under these sections if he does not provide a document or electronic document in a justice court. Section 175 penalises an individual who declines to provide the documents that he is required by law to present to a public official or in an impartial court. By using the term "electronic record" instead, one will be responsible under this section if he neglects to provide an electronic record or document to a in a court of justice or as a public worker.

**Modifications to the 1872 Indian Evidence Act**

A few changes have been made to the Information Technology Act of 2000 in India. 1872's Evidence Act. These changes have been implemented in the way outlined in Section 92 was read in the Second Schedule. Section 3 of the 1872 Indian Evidence Act the definition of "evidence" has been changed to encompass electronic records for the Court's examination. The

**ISSN (O): 2584-2196**

definition of "admission" in Section 17 has been modified to incorporate automated admissions. Following the insertion of section 22, section 22A[9].

It outlines the conditions under which an oral acknowledgement regarding the contents of an electronic documents are important. The places where entries in the books of account are pertinent are highlighted in Section 34. The section has been modified to incorporate electronic accounts books. Section 35 is modified to preserve the birth, death, and marriage register, income data, etc. in digital format. Section 39 has been modified to take the evidence into account value of a statement that is a component of an electronic document. Additionally, Section 131 is changed to incorporate the creation of electronic documents that another individual, possessing possession, might decline to provide. Additional significant portions are added by when applicable, this Act relates to opinions regarding electronic signatures[10].

**Modifications to the 1891 Banker's Books Evidence Act**

Certain changes to Banker's laws have been made by the Information Technology Act of 2000. These changes have been implemented in the way in accordance with section 93 of the Third Schedule. The meanings of "banker's"certified copies" as defined by Section 2(3) and "books" as defined by Section the Banker's Books Evidence Act of 1891's 2 (8) is revised to incorporate information kept in technological gadgets and printouts of that kind of information. Additionally, Section 2A is added to certificates to go with these printouts[11].

**Modifications to the 1934 Reserve Bank of India Act**

Reserve Bank has undergone some changes as a result of the Information Technology Act of 2000 of India Act of 1934. These changes have been implemented in the way outlined in the Section 94 is read with the Fourth Schedule. The subclause pp is added to section 58 after the goal of clause p of subsection 2 is to introduce and control electronic funds method for electronic funds transfers (EFT) between banks and other financial organisations[12].

[9] Sections 4, 192, 463, 464, 466, 468, 469, 471, 474, 476 and 477A of Indian Penal Code, 1860 (Act No. 45 of 1860).
[10] Section 92 and Second Schedule has been repealed by the Information Technology (Amendment) Act, 2008.
[11] Section 93 and Third Schedule has been repealed by the Information Technology (Amendment) Act, 2008.
[12] Section 94 and Fourth Schedule has been repealed by the Information Technology (Amendment) Act, 2008.

**ISSN (O): 2584-2196**

## INFORMATION TECHNOLOGY ACT OF 2000 CYBERCRIMES

Cybercrimes are especially addressed by this Act. The laws' provisions pertaining to Cybercrimes are listed in the Information Technology Act of 2000's Chapter XI under the "Offences" title, which addresses the several kinds of offences that is carried out electronically or in relation to computers, computer systems, networks of computers. Oddly enough, the phrase "cybercrime" or "cyber offence" is neither the 2000 Information Technology Act does not define or utilise this phrase. The

The following are India's cyber laws pertaining to several types of cybercrimes: as follows:

**Altering Documents from Computer Sources**

This is the first cybercrime for which there is an information technology penalty Act of 2000. According to Section 65 of the Act, if any individual who is aware of or purposefully hides, destroys, or modifies, or causes someone else to do so any computer program, computer system, or computer source code that is utilized or computer network, when it's necessary to preserve the computer source code, or maintained by law will face penalties for altering computer sources documents that carry a maximum sentence of three years in jail or a maximum fine of Rs. 2 lakh, or both. This provision's accompanying explanation clause describes the definition of "computer source code" by claiming that it refers to the compilation of programs, computer instructions, layout and design, and program analysis of any kind of computing resource.

The crime is associated with the destruction of data that is present in a computer. Additionally, the source code was illegal and had to be maintained under the law the deletion, alteration, or direct or indirect hiding of computer source code. Only when this act is performed with knowledge or intent is it punishable. This section's goal is to safeguard the invested intellectual property. the computer programs and to prevent infringement of copyright. This crime is Bailable, cognizable, and subject to trial by a First-Class Judicial Magistrate court[13].

In one case, the Honorable Court determined that the cell phones met the requirements for the term "computer" in the context of the Information Technology Act and the distinct Electronic Serial numbers that are preprogrammed into every phone, such as ESN and SID (System MIN

[13] Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr., (2005) Cri LJ 4314 AP.

**ISSN (O): 2584-2196**

(Mobile Identification Number) and Identification Code are the "computer source code" in accordance with the Information Technology Act's definition, which must be upheld and preserved by the law. It was decided that creating an electronic record or engaging in forgery through CD interpolations used as proof in a court is subject to penalty under this clause[14].

**Offences Associated with Computers**

Under this clause, offences involving computers carry a sentence of one year in prison duration that might last up to three years or with a fine of up to five lakh rupees, or both. "Data Theft" is defined by the Information Technology (Amendment) Act of 2008. As mentioned in section 43, section 66 is being referred to by making this section more strong, and the term "hacking" is not employed. Prior to this change, the offence Section 66 addressed "Hacking with Computer Systems." However, hacking is now supplanted by charges relating to computers that read as though any individual, dishonestly or fraudulently, engages in any of the activities listed in section 43, and the section was all encompassing to include all computer-related offences. However, hacking is now covered in principle by the recently added section 43(i) of the Amendment Act of 2008. It has to do with illegal access to computer systems. According to Section 66, hacking is only illegal when done dishonestly or dishonestly. Hacking in and of itself is not illegal under Section 66, although it depends on mens rea.

If an individual causes a computer resource to execute a task using deceptive or dishonest attempt to gain access, knowing that the access he plans to this section holds the person responsible if the security is not authorised. Section 43 of the Information Technology Act, as modified by the 2008 Amendment Act declares that anyone will be responsible for paying damages as restitution, not beyond one crore rupees to the individual impacted if the individual does so without authorisation

of the proprietor or another individual responsible for a computer, computer system, or as a computer, computer system, or computer network that provides or secures access to computer resource or computer network; extracts, copies, or downloads any data, information or data from a computer, computer system, or computer network, including data or information kept on any detachable storage device media; brings about the introduction of any computer contamination or any computer, computer system, or computer network with a computer virus;

[14] Bhim Sen Garg v. State of Rajasthan and Others, (2006) Cri LJ 3463 Raj 2411.

harms or causes any computer, computer network, computer system, or data to be harmed, computer database or any other programs that are installed on such a machine, system or computer network; interferes with or creates interference with any computer system or computer network; it prevents or results in the denial of access to any individual permitted to enter any computer, computer network, or computer system by any meaning; offers any help to anyone in order to make it easier for them to access a computer, computer system or computer network that violates this Act's provisions, rules or regulations pertaining thereto; charges for the services that an individual uses to the account of another individual through computer manipulation or tampering, computer system, or computer network; obliterates, removes, or modifies any data inhabiting a computer resource, reducing its usefulness or worth, or having an impact on it harmful in any way; steals, hides, destroys, modifies, or causes someone to steal, hide, destroy, or modify any computer resource's source code with a desire to do harm[15].

The Information Technology Act's Section 70(3) stipulates that anyone who obtains access to a protected system or attempts to gain access in violation of the punishment for violating this section will be either type of imprisonment for a period of time that could last up to ten years and be subject to a fine. In one instance, the accused obtained unapproved access to the Joint Academic

network, removed files, added files, and modified passwords to prevent access to the authorised users. The investigations showed that Kumar was using the internet to the BSNL broadband connection as though he were the legitimate, authorised user and changed the computer database that contained information about broadband Internet users subscriber accounts. Egmore, the Additional Chief Metropolitan Magistrate, Chennai condemned him to a year of severe incarceration and a fine under Section 66 of the Information Code and Section 420 of the Indian Penal Code for cheating technology Act for offences involving computers via communication services, etc[16].

**Using communication services to send offensive messages, etc.**

The Information Technology Act's Section 66 A stipulates that incarceration is the penalty for a period that might last up to two or three years, along with a punishment for transmitting

[15] R.K . Chaubey, An Introduction to Cyber Crime and Cyber Law, 2009, p. 45.
[16] H. Chander, Cyber Laws and IT Protection, 2012, p.76.

**ISSN (O): 2584-2196**

offensive communications via communication services, etc. In this section, anyone who transmits, via a communication device or a computer resource:

a) any material that is extremely insulting or threatening in nature; or

b) any information that he knows to be untrue but spreads in order to annoyance, inconvenience, danger, obstruction, insult, harm, and illegal activity intimidation, animosity, hatred, or malice, consistently employs such a communication device or computing resource,

c) any electronic mail or electronic mail message intended to cause irritation, trouble, or to mislead or deceive the receiver or addressee regarding the source of these mails.

This section's first clause addresses the transmission of material that is "grossly" objectionable" or has a "menacing character," like internet harassment or defamation as well as cyberbullying, etc. However, the Act itself does not define these two terms. This section's (b) addresses repeatedly delivering misleading signals in order to cause annoyance such as hate mail, net extortion, online insults, and online intimidation. This section's clause (c) addresses spam and unsolicited emails, including emails internet phishing, spoofing, etc. The message can take any form under this provision.

As long as a computer resource or a communication tool, such as email, is used, blogs, tweets, pictures, voice over IP, Skype, and SMS, among other things. However, the Supreme Court ruled in its decision that section 66A was unconstitutional completeness, as well as in opposition to the right to free speech and expression, and put it down in ***Union of India v. Shreya Singhal & Others***[17].

This particular portion had been abused by Police in other places have arrested innocent people for making critical posts on social media regarding political and social topics. The arrest had resulted from this section of numerous individuals for publishing stuff that was thought to be reportedly offensive on the online.

**Receiving a communication device or computer resource that has been stolen dishonestly**

**Information Technology Act of 2000, Section 66 B, which was added by amendment**

The 2008 Act stipulates penalties for dishonestly obtaining computer resources that have been stolen or gadget for communication. This Act states that anyone who acts dishonestly obtains or holds onto any communication device or computer resource that has been stolen knowing

[17] AIR 2015 SC 1523: (2005) 5 SCC.

**ISSN (O): 2584-2196**

or have grounds to suspect that the same computer resource or communication was stolen gadget, will be punished with a maximum sentence of three years in jail or with fine that might be up to one lakh rupees or both.

This offence is punishable by bail, cognisable, and subject to trial by the Judicial Magistrate of First-class. It would be applicable to anyone who purchase or hold onto computer resources that have been stolen or any kind of communication tool. Within the scope of this section, it encompasses gadgets such PCs, laptops, and cell phones, as well as in other computing resources like as software and data that have been stolen. For instance, suppose A bought a stolen cell phone for that the A stuff is stolen and pays Rs. 40,000 for Rs. 3000, then A is responsible under section 66B for fraudulently obtaining computer resources that have been stolen or gadget for communication.

**Theft of Identity**

The Information Technology Act of 2000's Section 66C was added by amendment. Identity theft is punishable under the 2008 Act. This clause states that anyone who uses the electronic signature dishonestly or falsely, any other person's password or other distinctive identifying characteristics must be punished by a fine that can reach three years in prison and with could go up to one lakh rupees. This section addresses identity theft, which is the fraudulent or dishonest use of a unique

a person's identifying characteristics, such as identifiers like an electronic signature, a biometric identification, a PIN, a login password, or a picture. The words previously, "dishonest" and "fraudulent" were defined as having the aim to cause someone to experience financial benefit or loss, and the intent to do so via deceit, in turn. This section doesn't distinguish between a natural person and a legitimate entity, such as a business[18].

This offence is punishable by bail, cognisable, and subject to trial by the FirstClass Judicial Magistrate's court. For instance, suppose A created a duplicate copy of B's ATM card and takes money out of his account, then A is accountable under section 66C for identity theft.

Financial identity theft, criminal identity theft, and identity fraud are some examples of identity theft. Identity cloning, identity theft, and commercial identity theft. Theft of financial identities involves financial theft, such as utilising stolen identities for internet banking information via phishing and used it to buy things. Theft of criminal identities involves using someone else's

[18] Anirudh Rastogi, Cyber Law- Law of Information Technology and Internet, 2014, p. 109.

identity to carry out illegal actions, such as utilising using someone else's email to send spam. Theft is a component of commercial identity theft of identification of a firm, business or other commercial enterprises for obtaining benefit or engaging in criminal activity. Identity cloning involves replicating a person's identity for establishing new accounts or assuming control of all of his accounts.

In one instance, the question of whether the wife may access her husband's and without their consent, using their father-in-law's email account to obtain proof in an instance of dower harassment, one is responsible under section 66C of the Information the Technology Act prohibits anyone from using their password dishonestly or gaining unauthorised access. The wife was found to be accountable under this provision by the court[19].

**Personation-based cheating with computer resources**

The Information Technology (Amendment) Act of 2008 adds Section 66 D for imposing penalties for utilising computer resources to cheat by personation. According to this clause, if someone uses a communication device, or personation-based computer resource cheating, will result in a sentence of either description for a period of time that could last up to three years and be subject to liability to a fine that might reach one lakh rupees. This offence is cognisable, subject to bail, and subject to trial by the Judicial Magistrate of FirstClass court.

This section applies to any instance of personation-based cheating carried out by using a communication device or a computer resource. Personation-based cheating has been described in accordance with section 416 of the IPC, which describes an action taken by someone who pretends to be someone else, intentionally replaces someone with another person, or making any representation that he or another individual is someone else truly is, therefore tricking someone else into carrying out an action. It's obvious outlined how the crime is done regardless of whether the person being portrayed is a genuine or fictitious individual by adding the section's explanation phrase.

**Privacy Violation**

The Information Technology (Amendment) Act of 2008 adds Section 66 E for imposing penalties for invasions of privacy. This clause states that if any individual who knowingly or purposefully records, disseminates, or transmits a private area of any individual without that

[19] Vinod Kaushik and Ors. v. Madhvika Joshi and Ors., (2010) Cr. Comp 2.

person's consent, in a situation that violates the privacy of that individual, will result in any type of incarceration as a punishment for a term that might last up to three years, or a fine of up to two lakh rupees, with both. This offence is cognisable, bailable, and subject to judicial trial for First-class magistrate.

This section covers any infringement of someone's physical privacy committed by three phases, such as recording, publishing, and transmitting. This provision makes it illegal to certain phases that are carried out without the victim's consent. Capturing involves take a picture using any method, including videotaping, filmmaking, or recording using any technology, including cameras, CCTVs, webcams in PCs, video recorders, or other electronic surveillance methods, such as concealed cameras or spy cameras, publications, such as smartphones, etc. Publication involves printed copies, i.e. periodicals, books, newspapers, and in an electronic format, such as on CDs or internet.

Transmission refers to the purposeful or intentional electrical transfer of the picture through via Bluetooth, emails, the internet, texting, etc., so that it can be viewed instantaneously by others. As soon as the offence is sent, it is instantly mail. It makes no difference if the recipient reads the correspondence or not at all. Nowadays, sting operations are widespread in many nations, including the United States, although these in many nations, including Sweden, operations are prohibited.

It is stated that in contrast to the United States and a few other nations where sting operations are accepted as legitimate approach to law enforcement, albeit in a restricted way, the same is not the case in India.

On its own ***motion in court v. State*** case, the bench of the Division decided that where a private individual or agency conducts a sting operation, which could lead to Violations of another person's bodily privacy will be subject to section 66 E of the Act. The Act will make such a person responsible. Two aides and a 24-year-old cybercrime suspect are wanted in connection with cybercrime cases, pretended to be vigilantes and entered the Mumbai cybercrime police station.

officers and attempted to sting the investigating officer on February 17, 2017. They sought to extort the cybercrime cell's senior police inspector to not prosecute the accused in any way. But they were defeated by their spy pen camera.

The authorities later discovered that the three guys had fictitious Central Vigilance identity cards issued by the Commission (CVC) and phoney letterheads bearing CBI names officers. The spy camera has been taken away. Then he was charged by the police under Sections 174,

419 (cheating), 170 (posing as a public servant), and 34 (by personation), IPC sections 420 and 506.

**Terrorism Online**

Terrorism is a type of threat or terror directed at the general public or the government that is unpredictable. A recent development in terrorism is cyberterrorism, which takes advantage of the

system that we have implemented. The desire to computerise every procedure is constant in order to incorporate convenience of use, accuracy features, and remote access. In general, cyber use of computers for terrorist purposes is known as terrorism. This is particular kind of cybercrime may entail communicating with people online. One definition of cyberterrorism is the deliberate employment of disruptive tactics, or the danger of it, in cyberspace, with the goal of advancing social, ideological religious, political, or comparable goals, or to threaten someone in order to such goals[20].

According to the FBI, cyberterrorism is "the planned, politically motivated motivated assault on data, computer programs, and computer systems which leads to subnational organisations using violence against non-combative targets or secret agents. According to security specialist Dorothy Denning, cyberterrorism is hacking activities with political motivations that aim to do serious harm, like the loss of life or serious financial harm.

There is no reference to cyberwar or cyberterrorism in the Indian Cyber Law previously. The Information Technology (Amendment) Act of 2008, however, has now made the Section 66F, which addresses cyberterrorism, stipulates penalties for terrorism. This offence is cognisable, non-bailable, and subject to trial in the court of sessions. The following are the legislative provisions pertaining to cyberterrorism:

(1) Whoever (A) With the intention of endangering India's sovereignty, unity, integrity, or security

or to instill fear in the populace or any segment of the populace by (i) refusing or causing to be denied access to anyone who is permitted to access a computer resource; or (ii) trying to gain access to or breach a computer resource without authorisation or going beyond what is permitted; or (iii) introducing any computer contaminant or causing it to be introduced. and

[20] The Hindu, New Delhi, June 24, 2016, available at: <http://www.thehindu.com/news/national/stingoperation-not-a-legal-method-of-law-enforcement-supreme-court/article5944283.ece >accessed on 22/04/2025.

such behaviour results in or is likely to result in death or injury. to individuals, harm or destruction of property, disturbances or being aware that it could result in supply disruption or damage or services that are vital to the community's existence or negatively impact the vital data infrastructure as defined by Section 70, or

(B) purposefully or knowingly gains access to or penetrates a computer resource without permission or going beyond what is permitted, and via through such actions, one can gain access to data, information, or computer databases that is limited due to concerns about foreign relations or state security; or any restricted data, information, or computer database, along with justifications for think that the data, information, or computer database that has been accessed in this way may
be utilised to harm or have the potential to harm the sovereignty's interests and the integrity of India, the state's security, and cordial ties with foreign nations, public order, morality or decency, or in connection with disdain of court, slander, or incitement to commit a crime, or to the benefit of any foreign country, group of people, or otherwise perpetrates the crime of cyberterrorism[21].

(2) There are consequences for anyone who engages in or plans to engage in cyberterrorism with incarceration, which might lead to life in jail. This section's Clause 1(A) addresses cyberterrorism that directly impacts or threatens impacts the populace in order to jeopardise the security, integrity, and unity of the country and to instill fear in the minds of the populace. Section 1(B) of this section addresses cyberterrorism that has a direct impact on the state through unapproved access to computer databases, data, or restricted information.
A terrorist is someone who commits acts of violence, wanton murder, or in the interruption of community-critical services or communication channels, or in causing property damage with the intention of placing the general public or any segment of the public in dread; or negatively impacting the unity among various racial, religious, and linguistic groups or local communities, castes, or regional groups; or forcing or overthrowing the government that was formed by law; or jeopardising the integrity and sovereignty of the country.
Therefore, a cyber terrorist is someone who uses a computer system to accomplish the aforementioned goal, and each action taken to do so is referred to as cyberterrorism. Cyber

[21] Dorothy Denning, Activism, Hactivism and Cyber terrorism: The Internet as a tool for Influencing Foreign Policy, 2001, p. 241.

terrorists employ a variety of instruments to carry out their goal of cyberterrorism, which includes Trojan assaults, hacking, cryptography, and viruses, computer worms, denial-of-service attacks, crimes involving email, etc.

In one instance, the court was asked to decide if a defamation offence could be adequately covered by I.P.C. section 499, or it need IT section 66 F. It is noted that the court must distinguish between two, and that section the I.P.C.'s Section 499 addressed the offence of defamation against a person and the phrase States are not considered "persons," however section 66F addressed the defamation of State.

The most recent explosions in India are those that occurred in Ahmadabad, Delhi, Jaipur, and Bangalore instances of 2008 cyberterrorism. 2008 saw the Mumbai Taj Hotel attacked, which is frequently referred to as 26/11, and the 2010 Varanasi explosion featured cyber evidence. The primary goal of cyberterrorism is to compile the restricted information and to disseminate terror through the use of cyber communications to interfere with peace, integrity, unity, and national security, among other things[22].

**Distributing or publishing pornographic content online Cyber Pornography**

"Pornography" refers to the depiction of sexual behaviours with the purpose to can arouse sexual desire by using pornographic websites or content created with computers, the internet, and the ability to download and send sexual texts, images, movies, and more.

Information Technology Act of 2000, Section 67, as revised by Information the Technology (Amendment) Act of 2008 addresses information publication, which is pornographic in digital form. The penalty for publication is outlined in this section or sending pornographic content via electronic means. According to this Act, if an individual who publishes, transmits, or arranges for the publication of any content in an electronic format which is lewd, or if its effects tend to make people more corrupt and depraved who will be most likely to read, see, or hear the content included in it, will be penalised with a maximum sentence of three years in jail upon first conviction and with a punishment that might reach five lakh rupees, and in the case of a second or subsequent conviction with a maximum sentence of five years in jail and with a fine that might reach ten lakh rupees. This offence is punishable by bail, cognisable by subject to trial by the JMIC court.

[22] Parthasarathi Pati, "Cyber Crimes", available at: <http://www.naavi.org/ pati/pati cybercrimes dec03.htm>, accessed on 22/04/2025.

**ISSN (O): 2584-2196**

The Information Technology Act of 2000 addresses the problem of cyberspace in India. pornographic images. The Act permits the private viewing or storage of pornography because it doesn't prohibit it specifically. However, sending or publicising the information Pornographic content is prohibited. Section 67 was the only clause in place prior to the modification. Under the Information Technology Act, which addresses pornographic publications, such as all kinds of pornography, including child pornography. However, following the Amendment Act, 2008, it currently exclusively deals with the publication of pornographic material. Section 67A of the Act expressly forbids the publication of pornographic or sexually explicit content and child pornography is expressly forbidden by section 67B of the Act. Only this section makes it illegal to publish and distribute pornographic or sexually explicit content information in an electronic format, but accessing, downloading, owning, etc., is not an violation of this section.

The Information Technology (Amendment) Act of 2008 added Section 67 A, which states that anybody who publishes, transmits, or causes to be published something sent electronically any content that includes sexually explicit acts or on a first conviction, behaviour will be penalised with either type of jail for a maximum sentence of five years and a maximum fine of 10 lakh rupees, and if a second or subsequent conviction results in incarceration of either a fine or a description for a period that might last up to seven years. It might reach ten lakh rupees The Information Technology (Amendment) Act of 2008's Section 67 B has been only addressed child pornography, which stipulates that if any one whoever publishes, transmits, or arranges for the publication or transmission of content in any electronic format that shows youngsters acting or behaving in a sexually explicit manner or produces digital images or text, gathers, searches, peruses, downloads, and promotes, encourages, trades, or disseminates content in any electronic format that features children either cultivates, entices, or inspires in a sexually explicit, obscene, or indecent manner minors to engage in sexually explicit internet relationships with one or more youngsters behave in a way on the computer resources that could insult a reasonable adult, or

encourages child abuse online, keeps electronic recordings of abuse, or that of other offences related to sexually explicit acts with children will be dealt with first conviction accompanied by either type of incarceration for a period of time that could five years, along with a punishment that might reach 10 lakh rupees, and in the case of second or subsequent conviction

**ISSN (O): 2584-2196**

accompanied by a sentence of imprisonment of any kind which might last for up to seven years, along with a fine of up to ten lakh rupees.

According to section 77B, the only portions that are not subject to bail are 67A and 67B of the Act, while others are subject to bail. We also have Information Section 69A Technology Act of 2000, which allows the Central Government or an approved official to issue instructions to other governmental organisations and intermediaries to prevent such information to the general public whenever it is required or practical to do so in the interest of India's integrity and sovereignty, defence of the country, state security, amicable relationships with other governments, maintaining public order, or avoiding incitement to the commission of any crime pertaining to the aforementioned.

According to Section 67 C, which was added by the Information Technology (Amendment) Act, when the intermediary wilfully or consciously disregards the instructions for retention and preservation of data that is outlined by the central government in accordance with paragraph 1 of section 67 C, will be penalised with an imprisonment for a maximum duration of three years, in addition to being subject to Al. Additionally, this offence is cognisable and subject to bail.[23]

**Noncompliance with the Controller's instructions**

Section 68 of the Information Technology Act states that the controller has a authority to order any employee or the Certifying Authority to take such action or stop engaging in the activities necessary to ensure compliance with the Act. However, anyone who wilfully or consciously disobeys such an instruction will be found guilty of a crime and will be punished upon conviction by a sentence of jail not going beyond two years, or to a fine of not more than one lakh rupees, or both. This offence is also non-cognizable and subject to bail.

The language of this clause makes it seem that the Controller could only provide the instructions given to a Certifying Authority or any of its employees, but by the Section 18 (1) permits him to likewise extend his authority to the subscribers of a certificates for digital signatures as this part stipulates that the Controller also possesses the authority to settle any disputes between the Certifying Authority and the subscribers.

[23] B.N. Firos v. State of Kerala, AIR 2006 Ker 279.

**ISSN (O): 2584-2196**

**Getting into a secured system**

Any computer, computer system, or computer network is considered a protected system it needs to be secured against unauthorised access by the relevant the government. The Information Technology Act's Section 70 gives the relevant government to designate any computer, computer network, or computer system as a system that is protected, by publishing a notice in the government gazette. Additionally, the government possesses the authority to grant access to a protected system to the person who has been granted permission by order in text. Anyone who tries to secure access or secures access without authorisation is susceptible to punishment with a term of imprisonment under a protected system, which could last up to ten years and be subject to a fine under this clause.

This offence is also cognisable and not subject to bail, In one instance, the Keralan government sent a notice announcing an e-"FRIENDS" is a government program that the petitioner created under a contract as a safeguarded framework. In a writ petition, the petitioner contested section 70 of the Information Technology Act, along with the notification that incompatible with the Copyright Act and unconstitutional. It was believed that a Section 70 of the Information Technology Act's notification is a statement of copyright in accordance with the Copyright Act of 1957, section 17(d). Additionally, the court held that they could only designate a computer resource as a protected system under the Information Technology Act if that qualified as a copyrighted government production[24].

**Violating Privacy and Confidentiality**

The right of an individual to choose when, how, and to what degree they want to be private is known as privacy. His private information will be disclosed to third parties. A privacy breach entails unapproved use, dissemination, or revelation of private data, such as medical records, sexual financial situation, tastes, etc. Nondisclosure of information is what is meant by confidentiality to unwelcome or unapproved individuals.

In general, parties while safeguarding the confidentiality of such information under Section 72 exchange of information, establish a consensus over the process for managing information and to refrain from sharing it with any parties or using it in a manner in which third parties will be informed. Additionally, the worker might occasionally expose the organization's important

[24] Ibid.

information just for financial benefit or advantages and results in a breach of the confidentiality agreement. The Information Technology Act's Section 72 was added to penalize the wrongdoer for violating confidentiality and privacy about data and information. There are other kinds of information that are highly beneficial for business and if such information is disclosed to outside parties, it could harm a company or an individual. Such data ought to be safeguarded and kept confidential. The right to privacy is granted in this clause for any information obtained in official ability. When he made the decision, the individual will be held accountable under this provision divulging information without the authorised person's knowledge or approval. This offence is non-cognizable and subject to bail. According to this provision, if someone manages to gain access to any electronic record, information, documents, communication, books, or other materials without the permission of the individual in question or divulges such an electronic document, book, or registry, any communication, data, document, or other content sent to another individual must be

subject to a fine or a maximum two-year jail sentence as punishment This could include both or up to one lakh rupees.

**Information disclosure in violation of a valid contract**

By amending the Act on Information Technology, Section 72 A is added. Act of 2008, which stipulates penalties for information dissemination that violates legal agreement. This section applies to any anybody, including a middleman, who, while offering services in accordance with a valid contract, has gained access to any content that includes another person's personal information with the intention of cause or being aware that he could report unlawful gain or wrongful loss, without the interested party's approval or in violation of a valid contract, such material to any other individual will be penalised with a sentence of imprisonment that might last for either for three years, a fine of up to five lakh rupees, or both.

The Act's Section 72 makes it illegal to just divulge personal information without permission, but this clause also calls for knowledge or intent to cause probability of resulting in unjustified gain or loss. Additionally, it applies to everyone, including middlemen that divulge data that has been protected by service provision through a valid contract. Additionally, this offence is cognisable and subject to bail[25].

[25] "Electronic Signature Certificate" has been substituted for the "Digital Signature Certificate" by IT (Amendment) Act, 2008.

**ISSN (O): 2584-2196**

**Offences Associated with Certificates of Electronic Signature**

Additionally, the IT Act provides for the offences associated with electronic signatures according to sections 73 and 74 there is a penalty for publication under Section 73. The Electronic Signature Certificate is inaccurate in certain details, and Section 74 stipulates punishment for publishing something fraudulently. Section 73 penalises the offender who release an Electronic Signature Certificate or provide it in any other way on any additional individual who is aware that the Certifying Authority specified in the certificate either failed to issue it, the Subscriber specified in the certificate declined to accept it, or the certificate has been suspended or revoked, unless the publishing is intended to of confirming an electronic signature made before the suspension or revocation in question with the possibility of two years in prison or a fine the equivalent of increase by one lakh rupees or both.

The aforementioned section's subsection (1) makes it quite evident that it is illegal to intentionally publish an electronic signature certificate or provide it in another way on anybody else, once it's been suspended or revoked and it makes the Liability of the Certifying Authority for any failure on their part to issue a notice of such suspension or revocation in the repository that the electronic signature specifies certificate for the notice's publication. Additionally, this subsection clarifies that Publication of an Electronic Signature Certificate will not be considered a crime in order to confirm the electronic signature that was made before the suspension or Revocation.

Additionally, Section 74 penalises the offender who wilfully produces, disseminates, or provides an Electronic Signature Certificate for any fraudulent or otherwise illegal activity with a maximum sentence of two years in jail or with a fine that might reach one lakh rupees, or both. The term "publication" was defined by the Supreme Court in the ***Bennett Coleman & Co. v. Indian Union***

The phrase refers to the sharing, storing, and sending of data or information in electronic format if we discuss it in relation to digital media.

**Corporate Offences**

The Information Technology Act's Section 85 integrates the idea of corporate criminal culpability, or the punishment meted out to a business for violating of the Act or any regulation, guidance, or directive issued under it. The rationale behind this according to this clause, a company can be any corporate entity, including a business or association of people. The

business could be incorporated or corporate. The aforementioned clause stipulates that if an individual violates any of the clauses of this Act or any guidelines, directives, or orders issued under it, is a business, each individual responsible for overseeing and answering to the business for the business practices of the organisation as well as the organisation at the time the if a violation was made, they will face consequences. But if such a person can demonstrate that the violations occurred without his knowledge or he took the necessary precautions to avoid such a violation, then he has to not be held accountable under this clause. Additionally, in cases where it is demonstrated that such violations has occurred with the permission or convenience of or is attributed to to any carelessness on the part of any manager, secretary, director, or other official of the business, then the manager, secretary, director, or any other officer needs to be judged to have violated the rules
and must be subject to legal action and appropriately disciplined.

The Honourable Court ruled in one case that "there is no statutory necessity that an officer or person in charge of the business may not face charges unless he is ranged with the business. They might all be prosecuted separately or along with the business in the event that the business violates the law. However, this stance was overturned by the Supreme Court in a joint ruling in the cases of ***M/S Godfather Travels & Tours Pvt. Ltd[26]. v. Aneeta Hada & Bajaj Avinash v. State[27]*** it established that the company's prosecution was a prerequisite for the prosecution of those who oversaw or were accountable to the business as well as the managing director or director.

[26] 54 AIR 2012 SC 2795.
[27] 55 (2009) Crl. Appl. 1483.