**Summary**

The original Act contained 94 sections, divided in 13 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.

The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The formations of Controller of Certifying Authorities was directed by the Act, to regulate issuing of digital signatures. It also defines cyber crimes and prescribed penalties for them. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law. The Act also amended various sections of Indian Penal Code, 1860, Indian Evidence Act 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934 to make them compliant with new technologies.

### **Amendments**

A major amendment was made in 2008. It introduced the Section 66A which penalized sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced penalties for child porn, cyber terrorism and voyeurism. It was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the then President (Pratibha Patil) on 5 February 2009.

### **Offences**

List of offences and the corresponding penalties:

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Offence** | **Description** | **Penalty** |
| 65 | Tampering with computer source documents | If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)200,000 |
| 66 | Hacking with computer system | If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)500,000 |
| 66B | Receiving stolen computer or communication device | A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)100,000 |
| 66C | Using password of another person | A person fradulently uses the password, digital signature or other unique identification of another person. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)100,000 |
| 66D | Cheating using computer resource | If a person cheats someone using a computer resource or communication. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)100,000 |
| 66E | Publishing private images of others | If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)200,000 |
| 66F | Acts of cyberterrorism | If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism. | Imprisonment up to life. |
| 67 | Publishing information which is obscene in electronic form. | If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. | Imprisonment up to five years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)1,000,000 |
| 67A | Publishing images containing sexual acts | If a person publishes or transmits images containing a sexual explicit act or conduct. | Imprisonment up to seven years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)1,000,000 |
| 67B | Publishing child porn or predating children online | If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18. | Imprisonment up to five years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)1,000,000 on second conviction. |
| 67C | Failure to maintain records | Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence. | Imprisonment up to three years, or/and with fine. |
| 68 | Failure/refusal to comply with orders | The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)200,000 |
| 69 | Failure/refusal to decrypt data | If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime. | Imprisonment up to seven years and possible fine. |
| 70 | Securing access or attempting to secure access to a protected system | The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.  The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence. | Imprisonment up to ten years, or/and with fine. |
| 71 | Misrepresentation | If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)100,000 |

### **Section 66A and restriction of free speech**

From its establishment as an amendment to the original act in 2008, Section 66A attracted controversy over its unconstitutional nature:

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Offence** | **Description** | **Penalty** |
| 66A | Publishing offensive, false or threatening information | Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine. | Imprisonment up to three years, with fine. |

## Notable cases

### *Section 66*

* In February 2001, in one of the first cases, the Delhi police arrested two men running a web-hosting company. The company had shut down a website over non-payment of dues. The owner of the site had claimed that he had already paid and complained to the police. The Delhi police had charged the men for hacking under Section 66 of the IT Act and breach of trust under Section 408 of the Indian Penal Code. The two men had to spend 6 days in Tihar jail waiting for bail. Bhavin Turakhia, chief executive officer of directi.com, a webhosting firm said that this interpretation of the law would be problematic for web-hosting companies.
* In February 2017, M/s Voucha Gram India Pvt.Ltd, owner of Delhi based Ecommerce Portal www.gyftr.com made a Complaint with Hauz Khas Police Station against some hackers from different cities accusing them for IT Act / Theft / Cheating / Misappropriation / Criminal Conspiracy / Criminal Breach of Trust / Cyber Crime of Hacking / Snooping / Tampering with Computer source documents and the Web Site and extending the threats of dire consequences to employees, as a result four hackers were arrested by South Delhi Police for Digital Shoplifting.

### *Section 66A*

* In September 2012, a freelance cartoonist Aseem Trivedi was arrested under Section 66A of the IT Act, Section 2 of Prevention of Insults to National Honour Act, 1971 and for sedition under the Section 124 of the Indian Penal Code. His cartoons depicting widespread corruption in India were considered offensive.
* On 12 April 2012, a Chemistry professor from Jadavpur University, Ambikesh Mahapatra, was arrested for sharing a cartoon of West Bengal Chief Minister Mamata Banerjee and then Railway Minister Mukul Roy. The email was sent from the email address of a housing society. Subrata Sengupta, the secretary of the housing society, was also arrested. They were charged under Section 66A and B of the IT Act, for defamation under Sections 500, for obscene gesture to a woman under Section 509, and abetting a crime under Section 114 of the Indian Penal Code.[[16]](https://en.wikipedia.org/wiki/Information_Technology_Act,_2000#cite_note-Mamata-16)
* On 30 October 2012, a Puducherry businessman Ravi Srinivasan was arrested under Section 66A. He had sent tweet accusing Karti Chidambaram, son of then Finance Minister P. Chidambaram, of corruption. Karti Chidambaram had complained to the police.
* On 19 November 2012, a 21-year-old girl was arrested from Palghar for posting a message on Facebook criticising the shutdown in Mumbai for the funeral of Bal Thackeray. Another 20-year-old girl was arrested for "liking" the post. They were initially charged under Section 295A of the Indian Penal Code (hurting religious sentiments) and Section 66A of the IT Act. Later, Section 295A was replaced by Section 505(2) (promoting enmity between classes). A group of Shiv Sena workers vandalised a hospital run by the uncle of one of girls. On 31 January 2013, a local court dropped all charges against the girls.
* On 18 March 2015, a teenaged boy was arrested from Bareilly, Uttar Pradesh, for making a post on Facebook insulting politician Azam Khan. The post allegedly contained hate speech against a community and was falsely attributed to Azam Khan by the boy. He was charged under Section 66A of the IT Act, and Sections 153A (promoting enmity between different religions), 504 (intentional insult with intent to provoke breach of peace) and 505 (public mischief) of Indian Penal Code. After the Section 66A was repealed on 24 March, the state government said that they would continue the prosecution under the remaining charges.

**What is the IT Amendment Act (ITA-2008)?**

The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team ([CERT-In](http://searchsecurity.techtarget.in/definition/CERT-In)).

The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; making the owner of a given [IP address](http://searchwindevelopment.techtarget.com/definition/IP-address) responsible for content accessed or distributed through it; and making corporations responsible for implementing effective data security practices and liable for breaches.

The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals. Section 69, for example, authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion. According to Pavan Duggal, a cyber law consultant and advocate at the Supreme Court of India, "The Act has provided Indian government with the power of surveillance, monitoring and blocking data traffic. The new powers under the amendment act tend to give Indian government a texture and color of being a surveillance state."