Cybercrime includes unauthorized access of information and break security like privacy, password, etc. of any person with the use of internet. Cyber theft is a part of cybercrime which means theft carried out by means of computers or the Internet.

The most common types of cyber theft include identity theft, password theft, theft of information, internet time thefts etc.

What are cyberlaws?

"Cyberlaw or Internet law is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation." (source: Wikipedia) Cyberlaws, same as any other branch of law, help define what is legal and illegal, and stipulate mechanisms to detect, convict and punish offenders, and protect electronic property and its rightful use.

Cyberlaws pertain to diverse aspects of the electronic world such as:

- software licences, copyright and fair use
- unauthorized access, data privacy and spamming
- export of hardware and software
- censorship
- computerized voting

INDIAN CYBER CRIME LAWS

How is cybercrime policed in the Indian context and what laws govern Indian cyberspace

A real-world scenario

If your mixer-grinder refused to start one day despite your best efforts, and knowing that you haven't fiddled around with any critical piece of the machinery, would you keep trying to start it, or approach an electrician? What would you do when he tells you that you've been sold a defective piece? Wouldn't your first thought be to take the device back to the outlet where you bought it from, and demand a replacement or a refund?

But when your spreadsheet software (which you have purchased legally) continues to crash throughout the day, regardless of the file you open, the setting you tweaked, or the programs you closed to free up memory, do you ever think about asking the software company for a refund? What causes this distinction between our experiences with offline and online products and services?

You would have noticed, as you try to install any software, that it asks you to read its "Terms and Conditions" (T&C), and indicate that you accept them by clicking on check box. You simply cannot install the software without accepting the T&C. But how many of us even view the T&C, leave along actually reading the 1000 word manuscripts?

One prime difference lies in the fact that we have seen stuff like home appliances and electronic goods for the past five decades, while the computer and internet have been with us only since the last twenty years, cyber laws are an even newer kid on the block.

The Internet: Its everywhere...

The fact that the internet pervades most aspects of our lives today, means that an increasing number of people have a parallel electronic existence. With millions of individuals interacting with each other, consuming online services, performing monetary transactions, and building viewpoints through cyberspace, monitoring, controlling, and policing the internet has become one of the prime concerns of almost all governments worldwide. The anonymous, decentralized and instantly “live” nature of the internet makes it that much tougher to assign responsibility, draw up jurisdictions, and effectively resolve genuine grievances. Increasing cases of criminal activities being conducted through this medium have been a growing concern and need to be tackled efficiently if we are ever to harness the true potential of the internet and convince even the most reluctant individuals in being connected to it.

A law behind every move you make

Every activity in the real world (e.g., buying a ticket, paying for groceries, signing an employment contract, etc.) has a legal underpinning. We rarely, if ever, consider the legal ramifications of our offline activities, because we are seldom the victims of a crime of fraud and resort to using the legal infrastructure (police, lawyers, courts) to resolve our grievances.

The same applies to any online activity. The underlying thought behind every email we reply to, every twitter post we re-tweet, every net-banking transaction we perform, or every news article we read is that it is “legal” to do so. So what happens when someone does something illegal online. But even prior to that, how do we know whether something is really illegal.

IT Act, 2000 and IT (Amendment) Act, 2008

These two pieces of legislation form the bedrock of cyberlaw infrastructure in India.

The Information Technology (IT) Act, 2000 was passed by the Indian Parliament in May 2000 and came into force in October of the same year. Its prime purpose is to provide the legal infrastructure for e-commerce in India. It was the first legal instrument to provide legal sanctity to electronic records and contracts expressed through electronic means of communication.

The act was later amended in December 2008 through the IT (Amendment) Act, 2008. Some of their salient points are:

- **Digital Signatures:** Electronic records may be authenticated by a subscriber by affixing digital signatures; further, the signature may be verified using the public key provided by the subscriber

- **Certifying Authorities:** domestic and foreign certifying authorities (which provide digital signature certificates) are recognized by the law; a “Controller of Certifying Authorities” shall supervise them

- **Electronic governance:** Documents required as per law by any arm of the government may be supplied in electronic form, and such documents are to be treated the same as handwritten, typewritten or printed documents

- **Offences and Penalties:** An Adjudicating Officer shall judge whether a person has committed an offence in contravention of any provision of the IT Act, 2000; the maximum penalty for any damage to computers or computer systems is a fine up to `1 crore

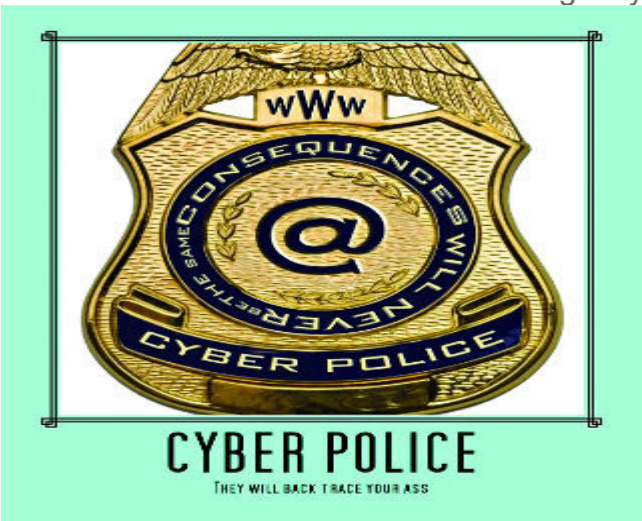
- **Appellate Tribunals:** A Cyber Regulations Appellate Tribunal shall be formed which shall hear appeals against orders passed by the Adjudicating Officers

- **Investigation:** Offences shall only be investigated by a police officer of the rank of the Deputy Superintendent of Police or above (amended to the rank “Inspector” or above by the IT (Amendment) Act, 2008)

- **Amendments to other laws:** Other acts such as the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers’ Books Evidence Act, 1891, the Reserve Bank of India Act, 1934 were to be amended to align them with the IT Act

- **Network Service Providers:** Intermediaries in the data transmission process, such as Internet Service Providers, are not liable in certain cases, so

long as the intermediary expeditiously acts to prevent the cybercrime on getting such instruction from the Government or its agency.



Why were these laws enacted?

As a result of the technological advancements in the IT industry, computers and internet became accessible to the common man in our country quite rapidly. Like any technology, IT too met with two kinds of people -- the users and the abusers. While cases of hacking came to light and identity, privacy and information security was found to be increasingly compromised by the new IT revolution, the need was felt for law and order mechanism in the electronic world too.

What offences are covered under these laws?

One viewpoint considered when drafting the IT Amendment Act, 2008, was that it should be a comprehensive piece of legislation with minimal dependence on other penal laws. Although this recommendation seems to have been overlooked, several new offences have been defined in the 2008 version. The two IT Acts together define the below offences and also recommend punishments for each of them:

1. Hacking

It is not defined in either of the IT Acts, which in itself may have considerably weakened the cybercrime legislation in India.

2. Data theft

This offence is defined as copying or extracting information from a computer system without the owners, including computer theft and theft of digital signals during transmission.

3. Identity theft (including Password Theft)

As per the IT (Amendment) Act 2008, this offence is defined as fraudulently or dishonestly making use of the electronic signature, password, or any other unique identification feature of a person. Identity theft pertains to illegally obtaining of someone's personal information which defines one's identity for economic benefit.

4. Email spoofing

This is commonly used by hackers to hide the actual email address from which phishing and spam message are sent. It may also be used in conjunction with other

fraudulent methods to trick users into providing personal/ confidential information. In SMS spoofing, the offender steals identity of another person in the form of phone number and sending SMS via internet and the receiver gets the SMS from the mobile number of the victim.

5. Sending offensive messages

The IT Act defines this offense as sending offensive or false information for the purpose of causing hatred, ill will, etc.

6. Voyeurism

This is defined as publishing/transmitting of “compromising” images/ videos of a person without his/her consent.

7. Child pornography

This covers offences against all individuals who have not completed 18 years of age. Despite being one of the most serious offences, it does not attract any severe punishment

8. Cyber terrorism

The addition of this offence was a major difference between the two IT Acts. Cyber terrorism is described in fair detail as denying access to a computer, attempting to access a computer resource without authorization, or contaminating a computer system.

Punishment

While all other offences are punishable by imprisonment up to 3-5 years and/or a fine of up to `3-5 Lakh, an individual convicted of cyberterrorism is punishable by imprisonment for life.

Who enforces the law? Where do I file a complaint?

What should you do if the password to your email account is stolen? Or if everyone on your Facebook friends list are receiving spam messages from your account? You may start by filing a complaint with the local police station. A major positive of the IT (Amendment) Act, 2008 over the original IT Act, 2000 was that police officers of the rank of “Inspector” or above were empowered to investigate cyber crimes, as against the rank of “Deputy Superintendent of Police” or above required by the original Act. This would have, at least theoretically, considerably increased the bandwidth of enforcement agencies in handling cybercrimes. However, try not to cross any fingers or toes hoping that you’d get your email account back, as you shall see in the next section.

Laws governing identity thefts in India

The crime of identity theft consists of two steps:

- Wrongful collection of personal identity of an individual
- Wrongful use of such information with an intention of causing legal harm to that person information

An identity theft involves both theft and fraud, therefore the provisions with regard to forgery as provided under the Indian Penal Code, 1860 (IPC) is often invoked along with the Information Technology Act, 2000. Some of the Sections of IPC such as forgery (Section 464), making false documents (Section 465), forgery for purpose of cheating (Section 468), reputation (Section 469), using as genuine a forged document (Section 471) and possession of a document known to be forged and intending to use it as genuine (Section 474) can be coupled with those in the IT Act.

The Information Technology Act, 2000 (IT Act) is the main act which deals with the legislation in India governing cybercrimes. Some of the Sections dealing with Cyber Theft are: -

- Section 43 If any person without permission of the owner damages to computer, computer system, etc. he/she shall be liable to pay compensation to the person so affected.
- Section 66 If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
- Section 66B Punishment for dishonestly receiving stolen computer resource or communication device is Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
- Section 66C provides for punishment for Identity theft as: Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.
- Section 66 D on the other hand was inserted to punish cheating by impersonation using computer resources.

Obscenity: Sections 67, 67A and 67B of the IT Act prescribe punishment for publishing or transmitting, in electronic form: (i) obscene material; (ii) material containing sexually explicit act, etc.; and (iii) material depicting children in sexually explicit act, etc. respectively. The punishment prescribed for an offence under section 67 of the IT Act is, on the first conviction, imprisonment of either description for a term which may extend to 3 (three) years, to be accompanied by a fine which may extend to Rs. 5,00,000 (Rupees five lac), and in the event of a second or subsequent conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac).

The provisions of sections 292 and 294 of the IPC would also be applicable for offences of the nature described under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC provides that any person who, inter alia, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 2 (two) years, and with fine which may extend to Rs. 2,000 (Rupees two

thousand) and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 5,000 (Rupees five thousand).

Section 65 of the IT Act: Section 65 of the IT Act prescribes punishment for tampering with computer source documents and provides that any person who knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code (i.e. a listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form) 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, shall be punishable with imprisonment for up to 3 (three) years or with a fine which may extend to Rs. 3,00,000 (Rupees lac) or with both.

Violation of privacy: Section 66E of the IT Act prescribes punishment for violation of privacy and provides that any person who intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to 3 (three) years or with fine not exceeding Rs. 2,00,000 (Rupees two lac) or with both.

Section 67C of the IT Act: Section 67C of the IT Act requires an 'intermediary' to preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

Cyber terrorism: Section 66F of the IT Act prescribes punishment for cyber terrorism. Whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people, denies or causes the denial of access to any person authorized to access a computer resource, or attempts to penetrate or access a computer resource without authorisation or exceeding authorised access, or introduces or causes the introduction of any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect critical information infrastructure, is guilty of 'cyber terrorism'.

With the increase in the number of frauds and cyber related crime, the government is coming up with refined regulations to protect the interest of the people and safeguard against any mishappenning on the internet. Further, stronger laws have been formulated with respect to protection of "sensitive personal data" in the hands of the intermediaries and service providers (body corporate) thereby ensuring data protection and privacy.