Cyber Law: Definition Nature, Scope, Utility of Cyber Law, Origin and Development of Cyber Law and Internet

**1. WHAT IS CYBER LAW?**

Cyber Law or IT Law is referred to as the Law of the Internet. The Cyber law definition says it is a legal system designed to deal with the Internet, computing, Cyberspace, and related legal issues. The apt introduction to Cyber Law is: It is ‘paper laws’ in the ‘paperless world’.

Cyber law encompasses aspects of intellectual property, contract, jurisdiction, data protection laws, privacy, and freedom of expression. It directs the digital circulation of software, information, online security, and e-commerce. The area of Cyber Law provides legal recognition to e-documents. It also creates a structure for e-commerce transactions and e-filling. Hence, to simply understand the Cyber law’s meaning, it is a legal infrastructure to deal with Cybercrimes. An increase in the usage of E-commerce has made it pivotal that there are proper regulatory practices set up to ensure no malpractices take place.

The laws implemented for cybersecurity largely vary from country to country and their respective jurisdiction. The punishments for the same also vary from fine to imprisonment based on the crime committed. It is very important for citizens to know the cyber laws of their respective countries to make sure they are well aware of all information regarding cybersecurity. The first cyber law to ever exist was the Computer Fraud and Abuse Act in 1986 that prohibited Unauthorized access to computers and illegal usage of digital information.

**2. THE IMPORTANCE OF CYBER LAW**

Just like any other law, Cyber law consists of rules that dictate how people and companies should use the internet and computers. While other rules protect people from getting trapped in Cybercrime run by malicious people on the internet. Although it is close to impossible to curb 100% of all cybercrimes, laws implemented all around the world assist Now the question arises, what are Cyber law and its importance? The importance of Cyber law can be understood by the following points:

* It dictates all actions and reactions in Cyberspace.
* All online transactions are ensured to be safe and protected
* All online activities are under watch by the Cyber law officials.
* Security for all data and property of individuals, organizations, and Government
* Helps curb illegal cyber activities with due diligence
* All actions and reactions implemented on any cyberspace has some legal angle associated with it
* Keeps track of all electronic records
* Helps to establish electronic governance

**3. WHY IS CYBER LAW REQUIRED?**

Now you must be thinking why do we need Cyber Law?

As of early 2021, the number of people that use the internet is over [4.66 Billion](https://datareportal.com/reports/digital-2021-global-overview-report#:~:text=Internet%3A%204.66%20billion%20people%20around,now%20stands%20at%2059.5%20percent.). With that number increasing by 7% annually. This also means every day can account for almost [8,75,000 new users](https://datareportal.com/reports/digital-2021-global-overview-report#:~:text=Internet%3A%204.66%20billion%20people%20around,now%20stands%20at%2059.5%20percent.). Given this swift increase in the use of Cyberspace, implementation and the usage of strict cyber rules helps establish a safe and secure environment for the users.  Living in a rapidly progressing world, the one thing to keep pace with it is the Internet. Although it initially started off as an information tool, today it helps with communication and commerce. Being highly sophisticated and developing every single day, the usage of cyberspaces has become common, hence the increase in cybercrimes is inevitable.

 with maintaining order during online activities. If somebody is found breaking rules or Cyber laws, the victim person/firm can take action against that person.

**4. THE VARIOUS COMPONENTS OF CYBER LAW**

**Safeguarding data and privacy**– Both private and professional information and data must be secured thoroughly. Personal and financial information always attracts cybercriminals. Misuse of this information by any other person is illegal and that is where these laws come into play. The basic steps to safeguard your data and privacy is elaborated below

* Two-factor authentication for financial platforms and any other forums that provide this function.
* Initiate Virus protection software.
* Use only verified payment methods on reputed websites.
* Avoid giving out personal information

**Cybercrimes-**These crimes are any illegal activities that occur on a networked technological device. These crimes include online and network attacks, extortion, harassment, money laundering, hacking, and many more.

**Intellectual property-**Intellectual property is basically an individual or group’s work, designs, symbols, inventions, or anything owned by them which are intangible and are usually patented or copyrighted. Now cyber theft would mean the stealing or illegal use of the same intangible items.

**Electronic and digital signatures-** Nowadays most individuals and companies use electronic signatures to verify electronic records. This has become reliable and regular. The wrong usage by another of this signature is illegal and hence a cybercrime.

**5. CATEGORIES OF CYBERCRIME**

**Individual-**Cybercrimes against individuals involve crimes like online harassment, distribution and trafficking of child pornography, manipulation of personal information, use of obscene data, and identity theft for personal benefit.

**Property-** Usage, and transmission of harmful programs, theft of information and data from financial institutions, trespassing cyberspace, computer vandalism, and unauthorized possession of information digitally are some of the crimes under the property.

**Government-**The crimes that come under this are cyber terrorism, manipulation, threats, and misuse of power against the Government and citizens. Groups or Individuals terrorizing Government websites is when this form of cyber terrorism occurs.

**6. FEATURES OF CYBER LAW**

Due to the rapid progress in the technology sector, the usage of cyberspace has become a common practice. With this increase, it has a large number of pros but also a higher number of cons. Hence during the 21st century, the IT Act 2000 was introduced. This was implemented to ensure all online records and activities are brought under the spectrum of legal governance. India has been ranked to be in the top 5 amongst other nations for cyber threats. But it has only one strong law in place to face and fight any cybercrimes that are the IT ACT of 2000 and its amendments.

The Cyber Law IT act 2000 came into consideration on 17th October 2000 to deal with e-commerce and Cybercrime in India.  Cyber law came into existence after the making of the Indian Constitution. So, it is a residuary subject handled by the Central Government and is not included in the three lists namely, Union, State, and Concurrent. According to the act following is the list of features of Cyber Law:

* All the electronic contracts made via secure electronic channels are valid legally.
* There are security measures in place for e-records and digital signatures.
* The Cyber law act defines a process for the appointment of an adjudicating officer for carrying out inquiries.
* The IT law act provides recognition for digital signatures legally. Also, the digital signatures are obligated to use an asymmetric cryptosystem and a hash function.
* The senior police officials and other officials are authorized to search any public case without a warrant.
* There is a provision in the act to establish a Cyber Regulation Appellate Tribunal. This tribunal handles appeals made against the final order of the Adjudicating Officer or the Controller. But an appeal against the tribunal’s order can only be made in the High Court.
* There is also a provision in the act to form a Cyber Regulations Advisory Committee that will advise the Central Government and the Controller.
* The nature of the Cyber law act even applies to online crimes or offenses that are committed outside India.
* There is also a provision to form the Controller of Certifying Authorities which licenses and regulates the working of the Certifying Authorities. All the digital signatures are stored by the Controller in such a case.

**7. AREAS WHERE THE CYBER ACT IS NON-APPLICABLE**

* Transactions and documents initiated by the Central Government
* Financial and legal acts done by someone who is legally claimed as the Power of attorney
* Contract for sale or transfer of immovable property

**8. IMPACT OF COVID ON CYBER-SAFETY**

Although strict laws have been implemented, due to the pandemic there has been a drastic increase in the use of online financial transaction methods which has, in turn, led to an increase in frauds. The education and health sector has also undergone severe attacks after the pandemic hit. There has also been a[hike of 500%](https://ciso.economictimes.indiatimes.com/news/experts-see-500-surge-in-cyber-attacks-post-lockdown/76645043) in the number of security breaches that have affected many in India after the lockdown was announced.

**9. ADD-ONS TO THE CYBER LAW IN INDIA AS OF 2021**

With social media being the new-found forum for everyone to communicate and express their views, the Government of India has established new rules to regulate social media and OTT (over-the-top) platforms. It was duly established to curb the usage and propagation of hate speech. Another crucial reason is to address grievances people have faced. They will also track inappropriate messages and tweets to the first originator. This will be done by the Government or a court order directed to that particular platform. The Government also made it ascertain that they will not encourage anything that could be a possible threat to National Security.

The need for Social Media and OTT  directives

* Defamation and hate speech- Due to the sudden rise of visibility on social media, it is imperative to curb hate speech and defamation as it can have severe implications on the public.
* Misuse of content and misinformation- Another major issue is the misuse of personal content and even obscene content on the same platforms.
* Online Protection- Need for protecting women and men from sexual offenses that occur on these platforms.

There were no previously effective rules that ensured the content-driven on OTT Platforms were watched by an appropriately aged audience or not. However,  now with the new rules & strict parent locks content will be delivered to the right audience

**10. DRAWBACKS OF THIS NEW AMENDMENT**

* Privacy Concerns- Any information can be misused and the usage of propaganda of any sorts can affect digital publishers
* Contradicting the Right to Freedom of Speech and Expression- According to Article 19(a), this right allows citizens to express any opinion on any channel of communication, be it speech or writing. Curbing and regulating social media is basically stripping citizens of their Right to freedom of speech and expression.
* Issues with tracking- For the Government to track hate speech and first originators of tweets, personal data like WhatsApp messages is required. But the question arises of how they will be able to derive such information when WhatsApp is encrypted.

 Although all of the above mentioned has been announced by the Government the formal version of the guidelines will be published in the coming months for a detailed understanding.

**11. OBJECTIVES OF CYBER LAW**

Cyber law came with the major objective to maintain law and order in all kinds of online activities and reduce Cybercrime. There are other objectives of Cyber Law as well. These will help you understand Cyber law better. These are:

* Unlike paper-based communication, the legal recognition of all the transactions via electronic media whether data or e-commerce is granted by the Cyber law.
* Digital Signatures became legal only due to the introduction to Cyber law.
* One of the biggest advantages of Cyber Law is that it facilitates the e-filing of documents with Government departments and agencies.
* It also grants legal sanctions and also allows electronic fund transfer between financial institutions and banks.
* It also legally authorizes the bankers to keep the books of accounts in electronic form.

**12. TYPES OF CYBER LAW**

Now let us discuss what are the types of Cyber law? The law has rules dictating behavior while using computers and the internet. It also prevents unscrupulous activities online. Some major types of Cyber Law are:

* **Copyright:**These days’ copyright violations come under Cyber law. It protects the rights of companies and individuals to get profit from their creative work. In earlier days, online copyright violation was easier. But due to the introduction of Cyber law, it has become difficult to violate copyright. Which is very good!
* **Defamation:** Generally, people use the internet to speak out their minds. But in the case of fake public statements on the internet that are bound to hamper someone’s business and reputation, that is when defamation law comes into the picture. Defamation Laws are a kind of civil law.
* **Fraud:**What is Cybercrime law? The major motive of this law is to protect people from online fraud. Consumers these days depend on Cyber Law to prevent online fraud. IT law prevents credit card theft, identity theft, and other money-related crimes that are bound to happen online. People who commit online fraud,  face state criminal charges. They may also witness a civil action by the victim.
* **Harassment and Stalking:**Some statements made by people can violate criminal law that refuses stalking and harassment online. When somebody posts threatening statements repeatedly about somebody else, this violates both criminal and civil laws. Cyber lawyers fight and defend people when online stalking occurs.
* **Freedom of Speech:**The internet is used as a medium of free speech. But there are laws to avoid free speech that may cause immorality online. Cyber lawyers should advise their clients about the amount of free speech allowed online. Sometimes the Cyber lawyers fight cases for their clients where they debate whether their client’s actions are within the permissible limit of free speech.
* **Trade Secrets:** Businesses depend on Cyber laws to preserve their trade secrets. For example, some organizations might steal online algorithms or features designed by another firm. In this case, Cyber laws empower the victim organization to take legal action to protect its secrets.
* **Contracts and Employment Laws:**You might have agreed upon many terms and conditions while opening a website or downloading some software. This is where the Cyber law is used. These Terms & Conditions are designed for online privacy concerns.

**13. APART FROM THE IT ACT OF 2000, THERE ARE OTHER LAWS THAT ENTAIL CYBERSECURITY WHICH ARE-**

* Companies Rules 2014 under the Companies Act 2013, makes it mandatory for all companies to ensure that all digital records and security systems are tight and sealed to avoid tampering and illegal access
* The Indian Penal Code Act 1860 punishes any crime committed in cyberspace (such as cheating, harassment, hacking, breach of privacy, etc)
* Sector-specific regulations are also established in The department of telecommunication, The Reserve Bank of India, and the Insurance Regulatory. Strict cybersecurity rules have been implemented

**14. INCENTIVES PROVIDED BY THE GOVERNMENT TO INCREASE CYBERSECURITY AMONG COMPANIES**

The Government has provided some beneficial measures for both public and private sector organizations to increase their standards of cybersecurity. One is the Public Procurement Order 2018 for Cyber Security Products where cybersecurity was named a strategic sector. It further mentioned that government agencies will prefer cybersecurity products that will be procured from domestically manufactured entities

**CONCLUSION**

You must now be aware of what is the definition of Cyber law and why we need Cyber law. Here are a few advantages of it. The organizations are now capable of handling e-commerce transactions using the legal infrastructure designed by the law. The law easily addresses issues of security and enables successful electronic transactions. The response time of any business deal is reduced considerably due to the storage of valid digital signatures.  In short, the IT law has made our life simpler online but it advises us to stay vigilant always!