**MOD1**

**Introduction to Cyber Law**

Cyber Law also called IT Law is **the law regarding Information-technology including computers and the internet**. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.

**Cyber Law (IT Law) in India**

**Cyber Law** also called IT Law is the law regarding Information-technology including computers and the internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.

IT law does not consist of a separate area of law rather it encloses aspects of contract, intellectual property, privacy, and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

**According to the Ministry of Electronics and Information Technology, Government of India :**

*Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check*[*cyber crimes*](https://www.geeksforgeeks.org/information-security-cyber-crime/)*.*

**Importance of Cyber Law:**

1. It covers all transactions over the internet.
2. It keeps eye on all activities over the internet.
3. It touches every action and every reaction in cyberspace.

**Area of Cyber Law:**   
Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. ***Fraud*:**   
   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft, and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.
2. ***Copyright*:**   
   The internet has made copyright violations easier. In the early days of online communication, copyright violations were too easy. Both companies and individuals need lawyers to bring an action to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their creative works.
3. ***Defamation*:**   
   Several personnel uses the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone’s reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.
4. ***Harassment and Stalking*:**   
   Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is a violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.
5. ***Freedom of Speech*:**   
   Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allows people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.
6. ***Trade Secrets*:**   
   Companies doing business online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance, and flight search services to name a few. Cyber laws help these companies to take legal action as necessary to protect their trade secrets.
7. ***Contracts and Employment Law*:**   
   Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

**Advantages of Cyber Law:**

* Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
* Digital signatures have been given legal validity and sanction in the Act.
* It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
* It allows Government to issue notifications on the web thus heralding e-governance.
* It gives authority to the companies or organizations to file any form, application, or any other document with any office, authority, body, or agency owned or controlled by the suitable Government in e-form using such e-form as may be prescribed by the suitable Government.
* The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.
* Cyber Law provides both hardware and software security.

What is Cyber Law?

Cyber law, also known as Internet Law or Cyber Law, is the part of the overall legal system thet is related to legal informatics and supervises the digital circulation of information, e-commerce, software and information security. It is associated with legal informatics and electronic elements, including information systems, computers, software, and hardware. It covers many areas, such as access to and usage of the Internet, encompassing various subtopics as well as freedom of expression, and online privacy.

Cyber laws help to reduce or prevent people from cybercriminal activities on a large scale with the help of protecting information access from unauthorized people, freedom of speech related to the use of the [Internet](https://www.javatpoint.com/internet)

, privacy, communications, email, websites, intellectual property, hardware and software, such as data storage devices. As Internet traffic is increasing rapidly day by day, that has led to a higher percentage of legal issues worldwide. Because cyber laws are different according to the country and jurisdiction, restitution ranges from fines to imprisonment, and enforcement is challenging.

Cyberlaw offers legal protections for people who are using the Internet as well as running an online business. It is most important for Internet users to know about the local area and cyber law of their country by which they could know what activities are legal or not on the network. Also, they can prevent ourselves from unauthorized activities.

The Computer Fraud and Abuse Act was the first cyber law, called CFFA, that was enacted in 1986. This law was helpful in preventing unauthorized access to computers. And it also provided a description of the stages of punishment for breaking that law or performing any illegal activity.

## Why are cyber laws needed?

There are many security issues with using the Internet and also available different malicious people who try to unauthorized access your computer system to perform potential fraud. Therefore, similarly, any law, cyber law is created to protect online organizations and people on the network from unauthorized access and malicious people. If someone does any illegal activity or breaks the cyber rule, it offers people or organizations to have that persons sentenced to punishment or take action against them.

**What happens if anyone breaks a cyber law?**

If anyone breaks a cyber law, the action would be taken against that person on the basis of the type of cyberlaw he broke, where he lives, and where he broke the law. There are many situations like if you break the law on a website, your account will be banned or suspended and blocked your [IP (Internet Protocol)](https://www.javatpoint.com/ip-full-form)

address. Furthermore, if any person performs a very serious illegal activity, such as causing another person or company distress, hacking, attacking another person or website, advance action can be taken against that person.

## Importance of Cyber Law

Cyber laws are formed to punish people who perform any illegal activities online. They are important to punish related to these types of issues such as online harassment, attacking another website or individual, data theft, disrupting the online workflow of any enterprise and other illegal activities.

If anyone breaks a cyber law, the action would be taken against that person on the basis of the type of cyberlaw he broke, where he lives, and where he broke the law. It is most important to punish the criminals or to bring them to behind bars, as most of the cybercrimes cross the limit of crime that cannot be considered as a common crime.

These crimes may be very harmful for losing the reliability and confidentiality of personal information or a nation. Therefore, these issues must be handled according to the laws.

* When users apply transactions on the Internet, cyber law covers every transaction and protect them.
* It touches every reaction and action in cyberspace.
* It captures all activities on the Internet.

## Areas involving in Cyber Laws

These laws deal with multiple activities and areas that occur online and serve several purposes. Some laws are formed to describe the policies for using the Internet and the computer in an organization, and some are formed to offer people security from unauthorized users and malicious activities. There are various broad categories that come under cyber laws; some are as follows:

**Fraud**

Cyber laws are formed to prevent financial crimes such as identity theft, credit card theft and other that occurring online. A person may face confederate or state criminal charges if he commits any type of identity theft. These laws have explained strict policies to prosecute and defend against allegations of using the internet.

**Copyrighting Issues**

The Internet is the source that contains different types of data, which can be accessed anytime, anywhere. But it is the authority of anyone to copy the content of any other person. The strict rules are defined in the cyber laws if anyone goes against copyright that protects the creative work of individuals and companies.

**Scam/ Treachery**

There are different frauds and scams available on the Internet that can be personally harmful to any company or an individual. Cyber laws offer many ways to protect people and prevent any identity theft and financial crimes that happen online.

## Online Insults and Character Degradation

There are multiple online social media platforms that are the best resources to share your mind with anyone freely. But there are some rules in cyber laws if you speak and defaming someone online. Cyber laws address and deal with many issues, such as racism, online insults, gender targets to protect a person's reputation.

**Online Harassment and Stalking**

Harassment is a big issue in cyberspace, which is a violation of both criminal laws and civil. In cyber laws, there are some hard laws defined to prohibit these kinds of despicable crimes.

**Data Protection** People using the internet depends on cyber laws and policies to protect their personal information. Companies or organizations are also relying on cyber laws to protect the data of their users as well as maintain the confidentiality of their data.

**Contracts and Employment Law**

When you are visiting a website, you click a button that gives a message to ask you to agree for terms and conditions; if you agree with it, that ensures you have used cyber law. For every website, there are terms and conditions available that are associated with privacy concerns.

**Trade Secrets**

There are many organizations that are doing online businesses, which are often relying on cyber laws to protect their trade secrets. For example, online search engines like Google spend much time to develop the algorithms that generate a search result. They also spend lots of time developing other features such as intelligent assistance, flight search services, to name a few and maps. Cyber laws help these organizations to perform legal action by describing necessary legal laws for protecting their trade secrets

## How to protect yourself on the Internet

Although the Internet is a resource that contains multiple different types of content, there are many hackers or unauthorized users that may be harmful to you in order to thief your personal information. Below are given all of the steps that may help you to keep your personal information and computers safe while using the Internet. All of the given steps or suggestions can be beneficial for all computer users, even if what type of computer, device, or operating system they are using.

.



### Verify data is encrypted

When you are sending any confidential information, such as debit card numbers, credit card numbers, usernames, or passwords, send these types of information securely. In Internet browsers, look for a small lock (Internet browser security lock) to verify this; an icon will be shown in the right corner of the bottom of the browser address bar or browser Window. If you see the icon, it should be in a locked condition and not in an unlocked position. Also, make sure the [URL](https://www.javatpoint.com/url-full-form)

starts with [https (Hypertext Transfer Protocol Secure)](https://www.javatpoint.com/https)

, as displaying in the below screenshot:



If the lock icon is in the locked position and data is intercepted, the data is encrypted that helps to keep secure your data and prevent others to understand it. The data can be read by anyone if the lock is in the unlocked position or no lock is visible because all information will be in the form of plain text. For example, an online forum is not secure, use a password, but you will not use the password with protected sites like an online banking website.

### Use a safe password

Like online bank site or other websites that contain confidential information, need to use very strong passwords, it is also recommended; you must use the different and strong password for all websites that require login id and password. You could use a password manager if you required help to remember your password.

### Keep your software and operating system up-to-date

To protect yourself on the Internet, it is better to update your software installed on your computer and operating system regularly. It is necessary because many updates are released by the developers of the operating system that are related to computer security-related issues. Therefore, you should update your system when the latest updates are released.

### When available always enable two-factor authentication

You can use the two-factor authentication feature to make more secure your accounts, like Gmail or others that require a login and contain your private data. It offers advanced protection by adding an additional step in verifying you at the time of login. If you enable two-factor authentication and the service does not verify your computer or other devices after authenticating your password, it sends a text message with a verification code on your cell phone. It includes more powerful security; for example, if someone knows your password of any account and tries to access your account, but he does not have your phone, he cannot access your account even with a valid password.

### Always be cautious of e-mail links and attachments

The email attachments and hyperlinks sent through email are the most common resources to spread viruses and malware. It is recommended to always be extremely cautious to open any attachments and hyperlinks, which you have received through email from others, even if they have sent by friend or family.

### Be aware of phishing scams

There are many phishing scams and techniques that can be more harmful in respect to losing your secret information. Therefore, it is necessary to familiarize yourself with these types of techniques. Hackers mainly target websites that need a login, such as PayPal, eBay, Amazon, online banking sites, and other popular sites.

### E-mail is not encrypted

If you send any confidential information through email, it can be read or understood by unauthorized users as email is not encrypted. Therefore, confidential data like debit card information, credit card information, password and more should not be transmitted over e-mail.

### Use an alternative browser

For protecting your systems, Internet browsers also play an important role. For example, earlier versions of Internet Explorer are not more secure. If you are using a lass secure browser in terms of your [browser](https://www.javatpoint.com/browsers)

like [Internet Explorer](https://www.javatpoint.com/internet-explorer)

, you should switch to another browser like *[Mozilla Firefox](https://www.javatpoint.com/mozilla-firefox)*

or *[Google Chrome](https://www.javatpoint.com/google-chrome)*

. Also, if you are using Microsoft Windows 10 operating system on your computer and want to stay to use a Microsoft Internet browser, you can switch to the Microsoft Edge rather than Internet Explorer that is more secure in terms of protecting your systems.

### Use caution when accepting or agreeing to prompts

When you are indicated to install an add-on or any program, before clicking on the Ok button, you need to read and understand the agreement carefully. If you do not understand the agreement or feel it is not necessary to install, you should not install this kind of program, cancel or close the window, which may be harmful for you.

Also, when you are installing an add-on or any program, you need to care about any check box that asks if this third-party program will be ok to install. These often cause more issues and leave these boxes unchecked because these are never required.

### Be cautious where you are logging in from

**Business**

If you are working in any organization, your place of work can monitor your computer by installing key loggers or use other methods. In this case, someone can collect usernames and passwords and read these logs if he has access to this information. It can be more harmful to lose your personal information. Additionally, if your computer is shared with other co-workers, do not store any passwords in your browser.

**Wireless network**

When you are using a wireless network, you must be careful that all the information sent from your computer and to your computer can be read and intercepted by any unauthorized person. You can log in to the network securely with the help of using WPA or WEP and prevent losing your secret information. Furthermore, make sure the network is secure if it is a home wireless network.

**Friend's house**

Sometimes, you may use your friend's computer and log in to your account on that computer, which may not be fully secure. Intentionally or unintentionally, you can enter your username and password on your friend's computer or the computer with whom you are not familiar. Finally, never save the password information on your friend's computer browser when you are logging into any site on a friend's computer.

### Always think before you share something

There are many social media sites, such as Instagram, Facebook, that enable you to make online friends and connect with them. The networking sites are also the best place to share your personal information with your friends, family or others. When you share something on social networking sites or the Internet, make sure you are not sending any information that can be harmful to you if everyone sees it. The sent information on the social network or the Internet should be public. Also, make sure you are sharing such something that will not offend anyone or embarrass you, and you must not be uploaded on the Internet.

### Update Internet browser plugins

You should update Internet browser plugins or install the latest plugins to protect yourself while online on the computer. Due to browser plugins like Adobe Flash, attackers may find some easiness or security vulnerabilities to hack any system. Therefore, you need to check out regularly that all your installed Internet plug-ins are up-to-date.

### Be aware of those around you

If you are working on the computer at any public area, school, library and more, make sure anyone is not looking at your screen, as there will be many people around you. On the other hand, it can be cautious if anyone is looking at your system screen that is called shoulder surfing. If you are required to system screen private, you can use a privacy filter for the display.

### Secure saved passwords

There are many users that are habitual to save login information and password on the system, but it can be insecure. Therefore, make sure you are storing your personal details, such as credit card detail and account passwords, in a secure area. It is recommended for everyone to use a password manager to save your passwords.

A password manager is a software that holds all securely encrypts and login information, and password protects that information. If you save a password in a browser and anyone has access to your Internet browser, the password information may be seen by that person. For instance, in the Firefox Internet browser, anyone can see all stored passwords if you do not set up a master password.

### Do not always trust what you read online

You should be aware about that it is possible for anyone to publish a website on the Internet. There are various creators who may have intention for creating a site only for malicious purposes. For instance, a website can be created to gain unauthorized access and spread fear, lies, or malware.

**Topic -Cyber Jurisprudence**

Cyber jurisprudence is **the study of the legal issues surrounding the use of technology, particularly the internet**. It encompasses a wide range of topics, including freedom of speech, privacy, intellectual property, and cybercrime.

The English meaning of jurisprudence is “knowledge of law”. DEFINATION: **Cyber jurisprudence is the study of laws which is directly related to cyber crimes**. Cyber jurisprudence also describes the principles of legal issue, which exclusively regulates the cyberspace and internet.

**Topic -Cyber law**

Cyber law is the law which governing cyberspace. Actually this law is directly related with cyber crimes, intellectual property, data protection and privacy and electronic signature.

**CYBER LAW IN INDIA**

Cybercrime is unlawful acts. In which the computer are used as a tool or target. Cybercrime includes all those criminal activities that are traditional in nature such as fraud, forgery, all of which are subject to the Indian penal code. The misuse of computer has also given birth to a gamut of new age crimes that are addressed by the information technology Act 2000.

**CHECKING CYBER CRIMES UNDER INFORMATION TECHNOLOGY ACT:**

The information technology Act 2000 which is amended by IT Act 2008 check the issue which is directly related with cyber crimes or E-mail crimes, or computer crimes. When a criminal commit the crime by using internet as the sources of target or as a tool then such type of crimes is called cyber crime.

The information technology Act 2000 provides strict punishment for cyber crimes such as imprisonment up to 10 years and also file upto 1 crore.

**MAIN FEATURES OF THE INFORMATION TECHNOLOGY ACT, 2000:**

India has enacted the information technology Act in the year, 2000 based on the modern law on electronic commerce adopted by the United Nations commission on international Trade Law. Main features of the information technology Act, 2000 are as follows:

·      The Act provides for regulation of certifying Authorities. This Act also empowers the certifying Authority to issue Digital signature Certificate.

·      The Act provides for establishment of cyber Appellate Tribunal.

·      The act completely bars the jurisdiction of civil court.

·      Breach of confidential and privacy.

·      Fraud

·      Publishing digital signature certificate falsely.

·      Misrepresentation.

·      The Act also provides for confiscation of any computer, computer system, floppies, compact Discs, tap drives or any other accessories related in the commission of the offence.

·      The Act also provides powers to control and state Govt. to frame rules and regulations for effective implementation of the Act.

This Act consists of 94 sections with 4 schedules. There are 13 chapters that deal with preliminary aspects, digital signature, security of electronic records, penalties, electronic governance, offences, adjudication etc.

Relevant provision of the Indian penal code have been amended in accordance with the schedule appended with IT Act. Following activities have been made punishable.

·      Destruction of electronic records to prevent its production as evidence in court is punishable.

·      Counterfeiting electronic records is made punishable.

·      Fabricating false evidence by making fictitious entry in electronic book or record is made punishable.

·      Whoever being a public servant prepares in correct electronic records in discharges of his officials duty, is liable for a punishment up to three years.

·      Forgery by making false electronic records is also an offence.

Topic-Doctrinal approach

Doctrinal legal research methodology, also called "black letter" methodology, **focuses on the letter of the law rather than the law in action**. Using this method, a researcher composes a descriptive and detailed analysis of legal rules found in primary sources (cases, statutes, or regulations)

Topic-Consensual approach

A consensual definition allows future research to be aligned and it facilitates the interpretation and comparison of existing research. The findings suggest that the routine activity approach can be applied to the digital world.

Topic-Real Approach

**the law regarding Information-technology including computers and the internet**. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce

topic-Cyber Ethics

Cyberethics is a branch of computer technology behavior that defines the best practices that must be adopted by a user when he uses the computer system. In simple terms, cyberethics refers to the basic ethics and etiquette that must be followed while using a computer system. Ethics, in general, refers to propagating good behavior, similarly by cyber ethics we refer to propagating good behavior online that is not harsh or rude. Cyberethics governs rules that individuals must be polite and responsible when they use the internet. Cyberethics aim to protect the moral, financial, social behavior of individuals. Cyberethics engages the users to use the internet safely and use technology responsibly and sensibly. Cyberethics empathizes the behavior that must be adopted while using cyber technology.

Some of the breaches of cyberethics are listed below:

* **Cyber Bullying:**[Cyberbullying](https://www.geeksforgeeks.org/what-is-cyber-bullying-definition-types-effects-laws/) is a form of bullying carried out via internet technology such as social media where individuals are mocked on their physical appearance, lifestyle, preferences, etc. The teenage generation or say youngsters are the major victims of this form of cyber ethic breach. Cyberbullying affects the emotional ethics of individuals and can cause mental disturbance to individuals.
* **Hacking:**Stealing a user’s personal or organizational information without authorized permission is not considered a good practice. It is one of the riskiest cyber breaches to data leak. Data leak includes passing of sensitive information such as passwords, bank details of the user to a third-party user who is not authorized to access the information.
* **Copywriting:**Claiming of another individual as one’s own is another type of cyber ethic breach that must be eradicated. Never engage in copywriting another person’s content or document and claim as it is your own. It leads to a serious problem called plagiarism, which is a punishable offense and considered a legal crime. It is always advisable to follow general cyberethics, while using the internet or say any kind of technology. A proper code of conduct must be followed while using cyber technology. Cyberethics if not used wisely can lead to serious situations. Social and legal laws are defined to use cyber technology wisely. In extreme cases, legal action can be taken if there is a violation of cyber ethics.

### ****Cyber Ethics focuses on the following:****

**1. Privacy:**

* The content that is available on the internet should not hurt any moral, emotional, or personal ethics of individuals.
* Users should have the right to protect any information which they don’t want to share openly.
* Private information like user’s contact details, address, security-related information like bank details, credit card/debit card details, are all included in basic cyber ethics of user privacy and must not be breached in any case.
* Any breach of privacy is theft/fraud of user identity and user personal information, which is punishable as per the rules of law.
* **2. IPR:**
* [IPR](https://www.geeksforgeeks.org/intellectual-property-rights/)stands for Intellectual Property Rights.
* IPR defines that the owners have the complete right to the content that is posted on the internet.
* The entire content is solely a belonging of the originator and no individual is allowed to claim that content published by the original creator as its own.
* Unauthorized distribution of someone else’s work should never be adopted as it’s ethically incorrect to not give creation and monetary benefits to the creator of the work.

**3. Security:**

* [Security](https://www.geeksforgeeks.org/cyber-security-types-and-importance/) on the internet is the most basic ethical right that every user must be accessible.
* Users of the internet should feel safe while they surf the net.
* Security, in general means only authorized users to have access to the content on the computer.
* And confidential information is safe, without any risk of loss of information/content.

**4. Accuracy:**

* The content available on the internet is accessed by billions of users.
* If there is no reliability of the information that is posted online, then it would mislead the masses.
* Cyberethics assert the importance of posting content on the internet that is correct in all aspects.
* Users trust the content of the internet and rely heavily on the internet for facts, therefore it is highly needed that the asked information is correct and reliable.

Best policies that individuals must adopt while using the internet or any kind of technology should include the following:

* Being Polite and not using harsh words.
* Avoid clicking on unknown links.
* Wisely opening Emails from known senders only.
* Not mocking anyone on Social Media.
* Not copying any individual’s work and claiming it as their own. Always cite that you have used someone else’s work.
* Be careful and research before installing any free software.
* Never intrude on another person’s privacy.
* Don’t contribute to any malpractice that can lead to the leak of data of an individual or organization.
* Never engage in Cyberbullying.
* Never compromise with the safety of your system. Always install an anti-virus on your system.

MEANING OF IPR(INTELLECTUAL PROPERTY RIGHTS)

**Intellectual property rights are the rights given to persons over the innovative work creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time.**

MEANING OF PAPENT

A patent is **an exclusive right granted for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem**.

Meaning of copyright

the legal right to be the only person who may print, copy, perform, etc. a piece of original work, such as a book, a song or a computer program.this is **original work authorship.**

**TOPIC-Evolution of computer technology**

Generations are:

1. First Generation Computer (1940-1956)
2. Second Generation Computer (1956-1963)
3. Third Generation Computer(1964-1971)
4. Fourth Generation Computer(1971-Present)
5. Fifth Generation Computer(Present and Beyond)

## 1. FIRST GENERATION COMPUTER: Vacuum Tubes (1940-1956)

The first generation of computers is characterized by the use of “Vacuum tubes” and it was developed in 1904 by the British engineer **“John Ambrose Fleming”**. A vacuum tube is an electronic device that is used to control the flow of electric current in a vacuum. It is used in CRT(Cathode Ray Tube) Tv, Radio, etc.

## 2. SECOND GENERATION COMPUTER: Transistors (1956-1963)

The second generation of computers is characterized by the use of “transistors” and it was developed in 1947 by three American physicists **“John Bardeen, Walter Brattain, and William Shockley”**.

## 3. THIRD GENERATION COMPUTER: [Integrated Circuits](https://computerstudypoint.com/what-is-integrated-circuit-and-its-types/) (1964-1971)

The third generation of computers is characterized by the use of [“Integrated Circuits”](https://computerstudypoint.com/what-is-integrated-circuit-and-its-types/) it was developed in 1958 by “Jack Kilby”. The integrated circuit is a set of electronic circuits on small flat pieces of semiconductor that is normally known as silicon. The transistors were miniaturized and placed on silicon chips which are called semiconductors, which drastically increased the efficiency and speed of the computers.

## 4. FOURTH GENERATION OF COMPUTER: Microprocessor (1971-Present)

The fourth generation of computers is characterized by the use of “Microprocessor”. It was invented in the 1970s and It is developed by four inventors named are **“Marcian Hoff, Masatoshi Shima, Federico Faggin, and**Stanley major”. The first microprocessor named was the **“Intel 4004”** CPU, it was the first microprocessor that was invented.

.5. FIFTH GENERATION OF COMPUTERS (Present and beyond)

These generations of computers were based on **AI**(Artificial Intelligence) technology. Artificial technology is the branch of computer science concerned with making computers behave like humans and allowing the computer to take its own decision currently, no computers exhibit full artificial intelligence (that is, are able to simulate human behavior).

**TOPIC-emergence of cyber space**

**The term cyberspace was first used by the American-Canadian author William Gibson in 1982** in a story published in Omni magazine and then in his book Neuromancer. In this science-fiction novel, Gibson described cyberspace as the creation of a computer network in a world filled with artificially intelligent beings.

**CyberspaceCyberspace mainly refers to the computer which is a virtual network and is a medium electronically designed to help online communications to occur. This facilitates easy and accessible communications to occur across the world. The whole Cyberspace is composed of large computer networks which have many sub-networks. These follow the TCP or IP protocol. The TCP (Transmission Control Protocol) is a standard for communications that allows the application programs and other computing devices to exchange data and messages over a Cyber network. These are designed to send data across the internet which then makes sure that the sent data are successfully delivered over the networks. It is the standards that are mostly used to define the rules of the internet and are defined by the Internet Engineering Task Force or IETF. It is a very commonly used protocol and it ensures that there is an end-to-end delivery of data. On the other hand, Internet Protocol or IP is the protocol or method that involves sending data from one device to another using the internet. Each and every device has an IP address that is unique to it and this gives it its identity. The IP address enables communication and exchange of data to other devices across the internet. It defines how devices and their applications will exchange packages of data with each other and connected networks.  All the transfer occurs through either of the Internet Protocol Suite or protocols i.e. either TCP or IP. Cyberspace is that space in which users share information, interact with each other; engage in discussions or social media platforms, and many other activities. This concept was introduced by William Gibson in his book ‘Neuromancer’ which was done in 1894. Thus, this term is still widely used among everyone as it is rapidly growing and used for various purposes by an individual.**

**Topic-Cyber Jurisdiction**

Cyber Jurisdiction or Jurisdiction in Cyber Space- In simple terms, is **the extension of principles of international jurisdiction into the cyberspace**. Cyberspace has no physical (national) boundaries. It is an ever-growing exponential and dynamic space.

There are three types of cyber jurisdiction recognized in international law, namely-

* **Personal Jurisdiction** – It is a type of jurisdiction where the court can pass judgments on particular parties and persons. In the case of *Pennoyer v. Neff****[[3]](https://lawbhoomi.com/jurisdictional-aspects-in-cyber-law-and-information-technology-act/" \l "_ftn3)****,*The Supreme Court of the US observed that the Due process enshrined in the constitution of the US constrains the personal jurisdiction upon its implication on the non-resident, hence there is no direct jurisdiction on the non-residents. However, this restraint was curbed over by the minimum contact theory which allowed the jurisdiction over the non-residents as well.
* **Subject-matter jurisdiction** – It is a type of jurisdiction where the court can hear and decide specific cases that include a particular subject matter. If the specific subject matter is of one court but the plaintiff had sued in any other court then the plea will be rejected and the plaintiff will have to file the case in the court which is related to that matter. For instance, a complaint regarding a consumer good should be filed in the district consumer forum rather than district court as district consumer forums specifically look at consumer related cases. In the same manner, all environmental-related cases are tried in NGT rather than a district court.
* **Pecuniary Jurisdiction** – This type of jurisdiction mainly deals with monetary matters. The value of the suit should not exceed the pecuniary jurisdiction. There are various limits set for a court that can try a case of certain value beyond which it is tried in different courts. For example, district consumer forum looks at the matter not exceeding 20 lakh rupees, State consumer dispute redressal commission which has pecuniary jurisdiction of more than 20 lakh rupees but not exceeding 1 crore, National consumer dispute redressal commission which has pecuniary jurisdiction involving cases of more than 1 crore rupees in India. It is dependent upon the claim made in proceedings and is structured in hierarchical order.

**Topic-Hierarchy of courts,**

The three levels of judiciary in India are divided as follows; - **District, that is, District and Sessions Courts, State, that is, High Courts, and the Supreme Court at the top**.

**TOPIC-Civil and criminal jurisdictions**

The jurisdiction of the court in case of cyber crime committed by out state offender having impact within the territory of local court is not useful till the time offender is not within the jurisdiction of any local court. In such cases the extradition is the option to bring the offender within the territory of India.

**TOPIC-Cyberspace-Web space**

Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

In the common IT lexicon, any system that has a significant user base or even a well-designed interface can be thought to be “cyberspace.”

One way to talk about cyberspace is related to the use of the global Internet for diverse purposes, from commerce to entertainment. Wherever stakeholders set up virtual meeting spaces, we see the cyberspace existing. Wherever the Internet is used, you could say, that creates a cyberspace. The prolific use of both desktop computers and smartphones to access the Internet means that, in a practical (yet somewhat theoretical) sense, the cyberspace is growing.

Another prime example of cyberspace is the online gaming platforms advertised as massive online player ecosystems. These large communities, playing all together, create their own cyberspace worlds that exist only in the digital realm, and not in the physical world, sometimes nicknamed the “meatspace.”

To really consider what cyberspace means and what it is, consider what happens when thousands of people, who may have gathered together in physical rooms in the past to play a game, do it instead by each looking into a device from remote locations.

**TOPIC- Web hosting and web Development agreement**

An important first step for any web-based business is the creation of a website that looks good and

is easy to use. Roadblocks to navigation and transaction must be avoided, but so must legal errors.

This short article attempts to summarize several of the most important issues faced by a company

seeking to establish a web presence, change its web site, and have its site hosted. Don't ignore

these basic business and legal issues that must be dealt with when negotiating website development

and hosting agreements

An important first step for any web-based business is the creation of a website that looks good and

is easy to use. Roadblocks to navigation and transaction must be avoided, but so must legal errors.

This short article attempts to summarize several of the most important issues faced by a company

seeking to establish a web presence, change its web site, and have its site hosted. Don't ignore

these basic business and legal issues that must be dealt with when negotiating website development

and hostin

An important first step for any web-based business is the creation of a website that looks good and

is easy to use. Roadblocks to navigation and transaction must be avoided, but so must legal errors.

This short article attempts to summarize several of the most important issues faced by a company

seeking to establish a web presence, change its web site, and have its site hosted. Don't ignore

these basic business and legal issues that must be dealt with when negotiating website development

and hostin

**Introduction.**

An important first step for any web-based business is the creation of a website that looks good and is easy to use. Roadblocks to navigation and transaction must be avoided, but so must legal errors. This short article attempts to summarize several of the most important issues faced by a company seeking to establish a web presence, change its web site, and have its site hosted. Don't ignore these basic business and legal issues that must be dealt with when negotiating website development and hosting agreements.

**Basic Items to Include in a Web Site Development Agreement**

* **Look and Feel Clause.** The agreement should include a detailed, written description of both what the web site will look like and how the web site will function and perform. Although this sounds simplistic, many of these relationships turn sour when multiple change orders and the related increases in development costs start flying back and forth between customer and developer. The further you digress from this approach, the more risk you assume in higher development costs and not getting a web site that accomplishes your objectives. Any changes to the description that occur during the development process should be put in writing.
* **Responsibilities Clause.** The agreement should include a detailed description of each parties' responsibilities during the development process. The agreement should specify who will do what. What is left unsaid or unwritten can often cause disputes later on in the development process. The agreement should either state that the customer has no role in the development process or spell-out in detail what obligations the customer has in such regard.
* **Development Schedule.** The agreement should contain a detailed development schedule tied to periodic payments for interim deliverables. The agreement should have a start date and an end date for the developer's work. An initial payment to cover development costs is typical, but the customer should retain at least 30% of the total development cost until it is determined that the entire website is complete and conforms to the description included as part of the agreement. This acceptance test by the customer is a critical part of the development process. The further you stray from this disciplined approach, the greater risk you assume that the website will not be completed on time and within budget.
* **Ownership Clause.** The agreement must address the issue of who owns the finished website and its underlying work product. This issue raises a classic conflict between the customer's desire to preserve the uniqueness of its site and the developer's desire to recycle as much of the work product as possible for other customers. One approach is to protect the truly unique elements of the site by means such as (a) not allowing any reuse of such elements by the developer for any of its customers for a period of time or (b) prohibiting the developer from making these elements available to any competitor of the customer.
* **Intellectual Property Clause.** The agreement should protect the customer from unauthorized uses of intellectual property by the developer. The developer must warrant that it either owns or is authorized to use the tools and technology it utilizes to create the website. This is increasingly important if the developer is providing any kind of content for the website. Furthermore, the developer should be required to indemnify and hold the customer harmless from any liability arising out of a breach of this warranty. Exposure for this risk should be shifted entirely to the developer to the fullest extent possible.
* **Developer's Post Completion Obligations.** The agreement should describe any post-completion obligations of the developer. Provisions for on-going maintenance and support by the developer should be addressed. Similarly, the developer's obligation to provided enhancements to the site to address things like changes in browser technology should be addressed as well.

The above points is just a summary and does not begin to touch upon some other issues that frequently arise. However, including the above-mentioned 6 points in the web site development agreement is a good first step and should reduce a significant portion of the risk in these transactions.

**Things to Consider Before Choosing Your Web Host.**

* **Select a reputable and dependable web host provider.** The old cliché "you get what you pay for" generally holds true in this area as in most. Saving some money by dealing with an industry newcomer may seem prudent, but service and dependability problems can quickly turn those savings into lost customer relationships. Check around and research which provider suits your needs.
* **The Agreement should define the services to be provided by the web host.** A typical menu of services would include things like domain name registration, content management, backup and data recovery services, Internet connection management, server maintenance, and promotional obligations. The agreement should make clear who is responsible for registering domain names. If registered by the provider, there should be an obligation to transfer the domain name to the customer upon any termination of the agreement. Promotional obligations may include things like having the provider register your website with a variety of search engines. Customers typically demand complete control over the content that is posted on their web site, but should insist upon a commitment from the provider to post new content within a reasonable period of time to keep the web site looking fresh and up-to-date. The agreement should address who will answer customer support calls from people using your web site.
* **The Agreement should provide for a meaningful service level commitment from the web host.** For web-only businesses, your web site is the only exposure your customers have to your business. It is customary to cover service level issues such as how long it takes the server to respond when someone is trying to access the website; how long it takes for users to download content; how many users may access and use the website at the same time; and how much scheduled and unscheduled downtime the provider's servers will experience. Access to mirror servers and back-up connections to multiple Internet service providers can help prevent significant downtime incidents. The agreement should also address what obligations the provider has to make disaster recovery services available in the event of a prolonged period of downtime.
* **Security should be a key concern and addressed in the agreement.** The web host should have systems and procedures in place to prevent unauthorized access to the information posted on and collected through your website. The agreement should obligate the provider to maintain adequate security for the term of the agreement and thereafter impose financial implications for any breach of this obligation. It is also important to make sure that the level of security provided by your web host is consistent with the commitments you make to your customers regarding the security of your website.
* **Privacy Protection and Your Privacy Policy.** An understandable privacy policy should be posted on your web site. This policy should describe the types of information that will be collected through your web site and how that information will be used. It is important to make sure that your web host understands and agrees to respect these commitments.
* **Maintain your ability to get out of a relationship that has gone bad. Resist the temptation to sign up for a long-term contract at a lower price.** Preserve your ability to change providers by agreeing to a shorter contract term with well-defined termination rights. Backstop these rights with a commitment from the hosting provider to offer an adequate level of transition assistance if you decide to move to a new hosting provider, even if you have to pay a premium for such service. Any significant downtime experienced in the changeover could be catastrophic to your business, and the agreement should address that concern by exposing the web host to significant damages if it fails to perform its transition commitments.

**Conclusion.**

Keeping these issues in mind when deciding with whom to host your web site will help you avoid problems that can seriously damage your business

**TOPIC- Legal and Technological Significance of domain Names**

**Domain Name is significantly more than an Internet Address, for it moreover perceives the Internet site to the people who accomplish it**, similar as a man's name recognizes a particular individual, or as more relevant to reserve banter, a Company's name recognizes a specific Company.Domain names were **intended to perform a technical function in a manner that was convenient to human users of the Internet**. They were intended to provide addresses for computers that were easy to remember and to identify without the need to resort to the underlying IP numeric address.

**Meaning of Domain Name**

Domain names are necessary pieces of organizations having any internet-based business movement. Since the business exercises on the Internet are expanding each day, the convenience and motivation behind domain names can’t be overlooked.Nowadays, domain names are names of sites of various elements, yet fill in as business identifiers and advertisers. Some might allude to domain names as the internet-based counterparts of brand names. Domain names are easy to understand types of internet tends to normally used to track down sites.

Domain names are made according to the techniques and rules of the ***Domain Name System (DNS)***, and the names enlisted in the DNS are domain names. A domain name is a character of one’s business on the web. Each web server requires a DNS server to make an interpretation of domain names into ***Internet Protocol (IP) addresses***.

Since Domain Names are not difficult to utilize and recollect that, they have become business identifiers. Initially a domain names intention was to go about as a location for PCs on the web. The Internet has, regardless, made from a simple means to convey to a strategy for carrying on business.

With the development of business on the Internet, a Domain Name is moreover used as a recognizable proof of such organizations. In short, a domain name isn’t just for giving a location to an Internet Communication yet in addition is a location for a particular website. There is a creating weight on brand name proprietors to get the privileges over the domain name for their association.

A huge piece of the associations individuals actually notices the ***“.com”*** domain is the most befitting and all good for business. Due to north of 15 million ***“.com” “.organization”*** and ***“.net”*** names are as of now classified and as a rule the domain name of an organization’s decision is now taken, organizations wouldn’t fret spending single amount add up to purchase a domain name from an outsider.

Domain Name is significantly more than an Internet Address, for it moreover perceives the Internet site to the people who accomplish it, similar as a man’s name recognizes a particular individual, or as more relevant to reserve banter, a Company’s name recognizes a specific Company.

**Functions of Domain Name**

Domain name fills the very roles as that of a brand name. A domain name serves the very capacities online that a brand name performs disconnected in transactions and exchanges. A brand name is a realistic signifier of the organization item or administration, while the domain name is a guide of the organization on the internet and the virtual picture of the business. An enrolled and secured brand name and the domain name offers the accompanying advantages:

* A brand name secures and advances the brand name, while an enrolled domain name ensures unapproved use by any substance or individual.
* Brand name upholds the presumptive worth of a calling or business, while a domain name builds the contact worth of the business from any remote spot of the world.
* A brand name makes an item or administration conspicuous on the lookout, while a domain name can convey the help or item to clients around the world.

The enrolled owners of a brand name get the selective right to utilize the imprint in regards to the labor and products. It serves to recognize the organization items from those of their rivals in exchange. In this manner, a brand name and domain name serve similar capacity as business identifiers.

An all-around ensured domain name is useful for the security and productivity of a business, very much like a globally ensured brand name. In this manner, enlistment of both the brand name and domain name is fundamental.

Be that as it may, the methodology of getting a domain name includes no assessment of whether it is proficient or unmistakable of separating itself, in contrast to brand names. Illustrative words can be enrolled as domain names.

A few organizations use their enrolled brand names as domain names. In this way, when a domain name is picked, the holder can apply to get brand name security for the domain name to keep any outsider from utilizing the name. Without a trace of a specific law overseeing domain names, the Trademark Law applies for something similar.

**Domain Names in India**

Picking a Domain Name is probably the most start and fundamental development of a Company or relationship towards setting up a qualification in the internet. Domain names look like names to a site comparative as names are to individuals, through which the association and PCs know who the owner of a particular site is or who has control over the resources.

The enlistment of Domain Names is ending up being progressively more critical for an association to be set up. There are countless people glancing through the net and using the web search instrument to track down associations and their things. To make it more clear for customers to notice a particular association, the domain name should resemble the work that is being done by the Company.

The protection of domain name in India has been in some way or another, a remarkable one, on the grounds that the Courts of India have been more understanding towards giving legitimate security to domain name as that to mark names.

Domain names resemble brand name, and are not straightforward areas, it is prepared for tantamount safeguard and affirmation comparable as the brand name. To make it considerably more comprehended, this piece of the article will look at a couple of fundamental cases that are picked by Indian Courts recalling a definitive goal to approve the above explanation.

By virtue of ***Tata Sons Ltd. v. Manukosuri and Others* the Hon’ble Court** held that domain names ought to be permitted confirmation comparative as the brand name. Brand name law applies to the exercises or activities that are done on the web, and the fundamental truth is that the various up-and-comers have not enlisted their domain names.

For the most part, in India, the capture begins when an individual gets a domain name chose with the Registering Authority, if generally speaking ends up being the Trade Name of someone else. There is no system in the Registry to find out if a Domain Name has adequately been taken. It has been seen through a case **Minerals Ltd. v. Pramod Borse** and Another that the courts law emphasis on the assumption for the party to have a particular domain name.

A singular objective is irrefutably important to see. Accepting an individual had wiped out assumptions while getting a name that at this point has been taken and should have been mischievous, then, the court will make this a ground for order.

Including a nonexclusive name or an engraving as a domain name may be permitted protection. Regardless of the way that using two regular terms along in light of a particular objective may be infringement. For example, **“Aaj”** and**“Tak”** may be traditional terms and may not be stored by any individual or association yet both of them together would oblige confirmation as a brand name.

A practically identical discernment had been made by the High Court of Kerala with respect to the words **“Pen”** and **“Books”**, but a mix of both the words have been yielded affirmation under the Trademark Law.

In the hour of 2005, India opened up the **“.in”** country code, permitting limitless second-level determinations under “. in.” and tremendous enrollments under facilitated zones which have been existing, for example, “. co.in” and ‘. org.in’.

With India’s full scale public outcome making at a speed of more than 8%, and a headway shower in the nation’s warily adroit lively individuals, there was a rivalry to get space names in the “.in” locale. This open door was additionally misused by cyber squatters.

To deal with the battles from opportunities holders, in 2005 the “.in” Registry organized the “.in” Domain Dispute Resolution Policy (INDRP) according to the Uniform Domain Name Dispute Resolution Policy. One of the essential protests under the INDRP was recorded in 2006.

From this point forward, more than 300 fights have been recorded and practically settled under the INDRP. It isn’t just new brand proprietors -, for example, Google, Dell and Disney – that have suitably gained domain names from cybersquatters under the INDRP. Indian relationship, for example, Airtel and Pantaloons, have in like way utilized this system to hold pariah back from utilizing domain names.

**Legal Framework for Domain Name in Law**

Any Person who views at that as an enrolled domain name which conflicts with his freedoms or interests might record a Complaint to the .IN Registry on the going with premises:

* The Registrant’s domain name is undefined or confusingly indistinct from a name or a brand name in which the Complainant has honors.
* The Registrant has no opportunities or interests in regard of the domain name;
* The Registrant’s domain name has been chosen or is being utilized in a malafide way.

In cases when such debates emerge and a Complainant documents an objection to the .IN Registry in consistence with the Rules and Regulations, the Registrant is needed to go through Arbitration continuing. The Registry keeps a rundown of Arbitrators from which the **.IN** Registry delegates an Arbitrator settle the said debate. This rundown containing the Arbitrators are distributed online by the .IN Registry on their site: [www.registry.in](http://www.registry.in/).

The Arbitrator should lead the Arbitration Proceedings according to the ***Arbitration and Conciliation Act 1996***. During the procedure on the off chance that the Arbitrator discovers any of the accompanying conditions relying upon the proof accumulated will show the Registrants right to the domain name:

(a) Before any notification to the Registrant of the inquiry, the Registrant’s use of, or apparent plans to use, the domain name or a name connecting with the domain name in regards to giving labor and products.;

(b) The Registrant (as an individual, business, or other affiliation) has been customarily known by the domain name, paying little mind to the likelihood that the Registrant has obtained no brand name.

(c) The Registrant is making a veritable sensible use of the domain name, with no objective for business benefit to delude or divert purchasers or utilize the brand name with malafide expectation.

The cure opens to a Complainant’s agreeable with any system before an Arbitrator may be limited to requiring the scratch-off of the Registrant’s domain name or the trading of the Registrant’s domain name enlistment to the Complainant’s Cost as may be viewed as fit may similarly be allowed by the Arbitrator.

The documentation of an issue under the UDRP doesn’t keep either party from introducing a contention under the steady gaze of a court for a goal either prior or as per the finishing of systems before the Administrative Panel.

If an Administrative Panel picks that the domain name enlistment should be dissolved or traded, there is a time of 10 working days conceded wherein the documentation of the claim should be shipped off the concerned Service Provider. No further move will be made by the Service Provider until it gets:

* Reasonable evidence of a goal of the discussion between the gatherings;
* Sufficient show that the case has been removed or withdrawn;
* A request duplicate of the Hon’ble Court excusing the claim or a request that has been passed for killing the Domain Name or moving something similar.

**TOPIC- Internet as a tool for global access.**

**When the Internet was first created, its design was based on the idea that it would be a global cyberspace, free of borders and any sort of filter. But over time, certain governments reluctant towards granting freedom of information as we know it have developed effective techniques to censor the web when it interests them. And states such as China, Russia or India defend a model of national sovereignty over the Internet, which safeguards these sorts of restrictive measures.**

The most radical way of controlling the Internet used by some governments is to cut off certain area’s access to it, pure and simple. During frenzied times, such as elections or when there are protests, some governments are quick to apply this blackout strategy. According to the organization [Access Now](https://www.accessnow.org/election-handbook-fight-back-internet-shutdowns/), which fights for the protection of freedom of information and for the right of citizens to Internet access, in 2020 there were 155 cuts in 29 countries.

**Internet blackouts**

The first place in the ranking for this type of censorship is held by India, with 109 Internet cut incidents throughout parts of the country in 2020. India might be proud of being “the largest democracy in the world”, but Hindu nationalist Narendra Modi’s government and some states have no objection to depriving their citizens of Internet access “for security reasons.” As such, when in 2019 the central government decided to revoke Kashmir’s autonomy, it also applied an Internet blockade in the territory that lasted 213 days. There were to be no opportunities for organized resistance.**Internet outages often target mobile networks, which is the medium most used by most people**

Also, in Myanmar, two and a half months post the military coup last February, the junta imposed an almost complete Internet shutdown during night hours. Then fixed-line connectivity was restored, but not wireless broadband Internet.

The outages often focus on mobile Internet service, which is the cheapest and most efficient means of accessing the Internet for most people. This allows companies, government offices, educational centers and other institutions with fixed network connections to continue to operate over the Internet, while individual users are left without means of communicating. The Indian government resorted to this tactic during the farmers’ protests in New Delhi last February, disconnecting mobile broadband for hours to prevent protesters from transmitting messages over the data network.

**Social networks and messaging blocking**

Other times, to prevent people from sharing information or calling for demonstrations, access to networks such as Facebook, Twitter, WhatsApp or Telegram is blocked. Without implementing a complete blockade, governments can slow down the operation of these networks, making it almost impossible to share images or videos or communicate quickly. This sort of slowdown can also be used as a form of punishment operation, like the one that Russia applied to Twitter last March for not removing content deemed “illicit” by the Russian regulator.

In Russia, there is increasing pressure on social networks for fear that they may become channels for anti-government discussion and means for mobilizing action, as occurred after the arrest and conviction of opposition leader Alexei Navalny. To prevent this, the Duma passed a law last year that gives authorities greater powers to block access to Western social networks and to impose fines if they don’t remove content considered illegal under Russian law.

In India, the government is also attentive to what’s published on social networks, and when it doesn’t like something, it reacts. According to Twitter, in the first half of 2020, there were more than 2,700 official requests to remove content, and last February, during the farmers’ protests, the government demanded 250 accounts be blocked, including those of influential journalists critical of the government.

**Xi Jinping’s government maintains that “within Chinese territory, the Internet is under the jurisdiction of Chinese sovereignty”**

Twitter is also totally blocked for citizens of China, North Korea and Iran. Other governments, such as those of Turkey, Egypt or Cuba, have suspended or slowed down the service during times of protests or social unrest.

In Hong Kong, the government has not only imprisoned opposition leaders, applying the security law to them. Chief executive Carrie Lam has also said that the government is preparing a law to fight against “fake news”, which has increased during the protest movements and the pandemic. She, in particular, has put the spotlight on social media, accusing it of being inundated with fake news and hate speech.

**National cyber sovereignty**

Beyond episodic cases of censorship, the most significant change in cyberspace regulation is the tendency to assert “national sovereignty” over what was originally conceived as a global, non-governmental network. The Chinese government is exemplary of this practice, which, in a 2010 White Paper already maintained that “within Chinese territory, the Internet is under the jurisdiction of Chinese sovereignty.” And President Xi Jinping has defended that “the right of each country to choose its own cyber-governance model must be respected.”

The model chosen by the Chinese regime has given the government authority over what comes in from outside the country and control within the country. Those who hoped that the Internet would inevitably give way to a climate of greater freedom and democratization in China have been sorely disappointed. Rather, China’s technological might has served to accentuate the government’s control over Internet users.

Against the Silicon Valley giants, China has its own champions: Alibaba in e-commerce, search engine Baidu, and Tencent as a leading multinational tech company for video games and other apps such as WeChat. But on the Chinese Internet, you don’t chat about serious things without the government’s surveillance. An entire army of censors is on the lookout to quickly locate and delete negative opinions and sensitive information. In addition, the government somehow “subcontracts” the monitoring and control of information to the Internet giants, by making them responsible for what’s published on their platforms. Hence, these Chinese companies have hundreds of thousands of moderators devoted to online censorship and surveillance.

**Holding big tech accountable**

In a way, the Chinese model is also being imitated in Western countries at the request of governments or from pressure from public opinion. The platforms, which initially maintained that they were neutral concerning the content that circulated on them, are thus forced to have a plethora of moderators.

The defense of national sovereignty against foreign companies is not a specifically Chinese trait. Trump’s restrictions on Huawei, claiming that the company could transmit confidential data to the Chinese government, and the restrictions placed on [TikTok](https://www.aceprensa.com/cultura/redes-sociales/tiktok-la-nueva-red-social-que-triunfa-entre-los-adolescentes/" \t "_blank), show that the U.S. is wary of threats that actions of Chinese companies on American soil could pose to national security.

The dispute between China and the U.S. hasn’t disappeared under the Biden Administration. Tencent is negotiating with the U.S. Foreign Investment Committee to maintain its stake in American video game companies. Tencent owns Riot Games, as well as 40% of Epic Games, the creator of [Fortnite](https://www.aceprensa.com/resenas-videojuegos/fortnite/" \t "_blank). The Committee is investigating whether the handling of users’ personal data by these two companies could pose “a threat to national security.”

**Controllable infrastructures**

Following in the footsteps of China’s model, some states, such as Russia and Iran, are working to create national Internet access infrastructures, with services essentially hosted on national territory and, therefore, more controllable. This allows for easier and more precise censorship, limiting the economic consequences of network outages. As NGO Access Now’s Melody Patry [tells Le Monde](https://www.lemonde.fr/international/article/2021/04/07/controle-d-internet-la-tendance-inquietante-des-coupures-du-reseau-par-les-etats_6075888_3210.html): “If, for example, the Internet is accessed through increasingly local infrastructures, network disconnects can target specific social networks such as Twitter and Facebook, while simultaneously keeping government websites and official information sites controlled by the State up and running.”

Along these lines, Putin signed a “sovereign Internet” bill, which passed in 2019, allowing Russian Internet to operate independently from the World Wide Web in the event of an emergency or foreign threat, a maneuver that only reinforces the government’s control over the network.

The desire of authoritarian governments to censor information is nothing new. What is unprecedented is that the Internet, which was born as a global instrument for sharing information, has undergone processes of balkanization disguised as means to safeguard national sovereignty.