

LAW AND TECHNOLOGY IN INDIA

By- Alice Chouhan

B.A. LL. B (Hons.) III Semester, School of Law DAVV, Indore

ABSTRACT

Since the existence of human civilization there have been many cultural and traditional changes. Every alteration and change leads to new invention and one among them is technology. In India around 480 million people are using internet. So, it is important to make people aware about the advantages and disadvantages of the technology. According to Stephane Nappo – Our future world will have to find equilibrium in the te

chnology pendulum swing. Technology is the branch of knowledge that deals with the use and creation of techniques and its relation with society environment and life, whereas the law is official rules and regulations of the country that says what the people may or may not do. Both law and technology enhance the life of the people. The Government of India introduced the INFORMATIVE TECHNOLOGY ACT 2000 to make people aware about how technology functions and how it can be misused.

Think Lawgically
Grow Lawjustifiably

INFORMATION TECHNOLOGY ACT 2000 (IT ACT)

This Act provides legal framework for means of electronic data and others means of electronic communications which involves electronic filling of documents and use of alternative paper-based methods of communications. Information Technology Act was enacted in the year 2000 for prevention and control of cyber-crimes. This Act is based on the UNCITRAL MODEL law on e-commerce to create a uniform environment regulating for e-commerce. The original Act contained 94 sections placed under 13 chapters and 4 schedules. The law is applicable in India. The IT Act is not a panel statue. All the cyber-crimes are covered in this Act as well as in the Indian penal code (IPC). This Act was amended various section of IPC and the Indian Evidence Act, 1872 covering various crimes under it. With the increase in the use of the internet, there is also an increase in the number of cyber-crimes.

It contains various sections, which are as follows –

SECTION 65 - Tampering with computer source documents. Punishment –Imprisonment upto 3 years or with fine upto Rs 2,00,000.

SECTION 66 A – Publishing offensive, false or threatening information. Punishment- Imprisonment upto 3 years with fine.

SECTION 66 “ac” – Hacking with a computer system. Punishment- Imprisonment upto 3 years or fine upto Rs 3,00,000.

SECTION 66 B – Receiving stolen computers or communication devices. Punishment - Imprisonment upto 3 years or fine upto Rs 1,00,000.

SECTION 66 C “ac” – Using the password of another person. Punishment - Imprisonment upto 3 years or fine upto Rs 100000.

SECTION 66 D “ac” – Cheating using a computer resource. Punishment - Imprisonment upto 3 years or fine upto Rs 100000 .

SECTION 66 E “ac” – Publishing private images of others. Punishment - Imprisonment upto 3 years or fine upto Rs 2,00,000.

SECTION 66 F “ac” – Act of cyber terrorism. Punishment – Imprisonment of LIFE.

SECTION 67 – Publishing information which is obscene in the electronic form. Punishment - Imprisonment upto 7 years or fine upto Rs 10,00,000.

SECTION 67 B “ac” – Publishing child porn or predated children online. Punishment - Imprisonment upto 5 years or fine upto Rs 10,00,000.

SECTION 68 – Failure / refusal to comply with orders. Punishment - Imprisonment upto 3 years or fine upto Rs 200000.

SECTION 69 - Failure / refusal to decrypt data. Punishment - Imprisonment upto 5 years or fine upto Rs 2,00,000.

SECTION 70 – Securing access to a protected system. Punishment - Imprisonment upto 10 years with fine.

SECTION 71 “ac” – Misrepresentation. Punishment - Imprisonment upto 3 years or fine upto Rs 1,00,000.

DATA PROTECTION

The IT ACT which was introduced in year 2000 does not specify any provision for data protection. THE GOVERNMENT OF INDIA INTRODUCE A SEPARATE BILL CALLED “PERSONAL DATA PROTECTION ACT 2006” which is still pending in the parliament. So, the government introduced IT ACT in two sections which address data protection to great extent and which gives rise to certain key considerations for the sector.

CYBER CRIME

It is an unlawful act done by means of a computer or other electronics devices with increase in use of technology. Since everyone is dependent on internet it increases the risk of cyber-crime.

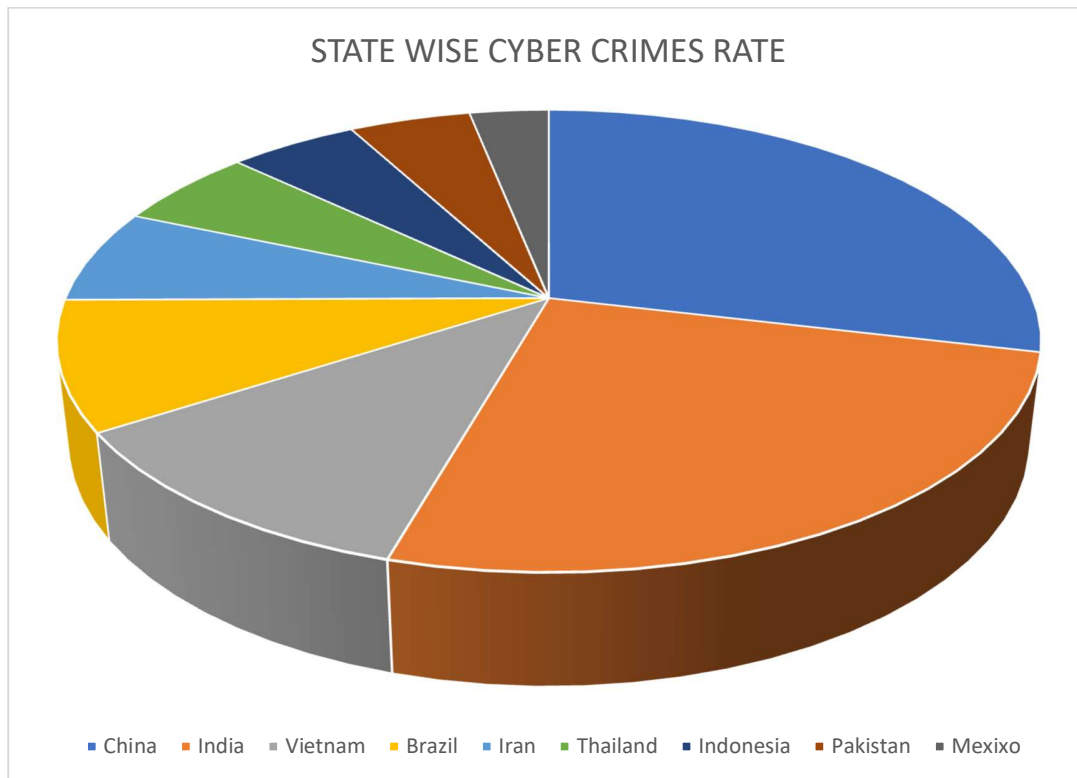
According to NCRB data cybercrimes rose 19 times and cyber crime on the whole arose nine times in India. Cyber crimes in India are registered under the INFORMATION TECHNOLOGY ACT, State level legislation and the IPC. Cyber Crime are categorised as cyber terrorism, cyber stalking, unauthorised access to electronic devices, child pornography, forgery, Fake calls, Hacking, Blackmailing and sharing fake news sharing on social media.

In India the cyber crime rate is 0.43 which is almost double in 2017 according to survey released by national crime record bureau (NCRB).

State wise cyber crime (2018) list is -

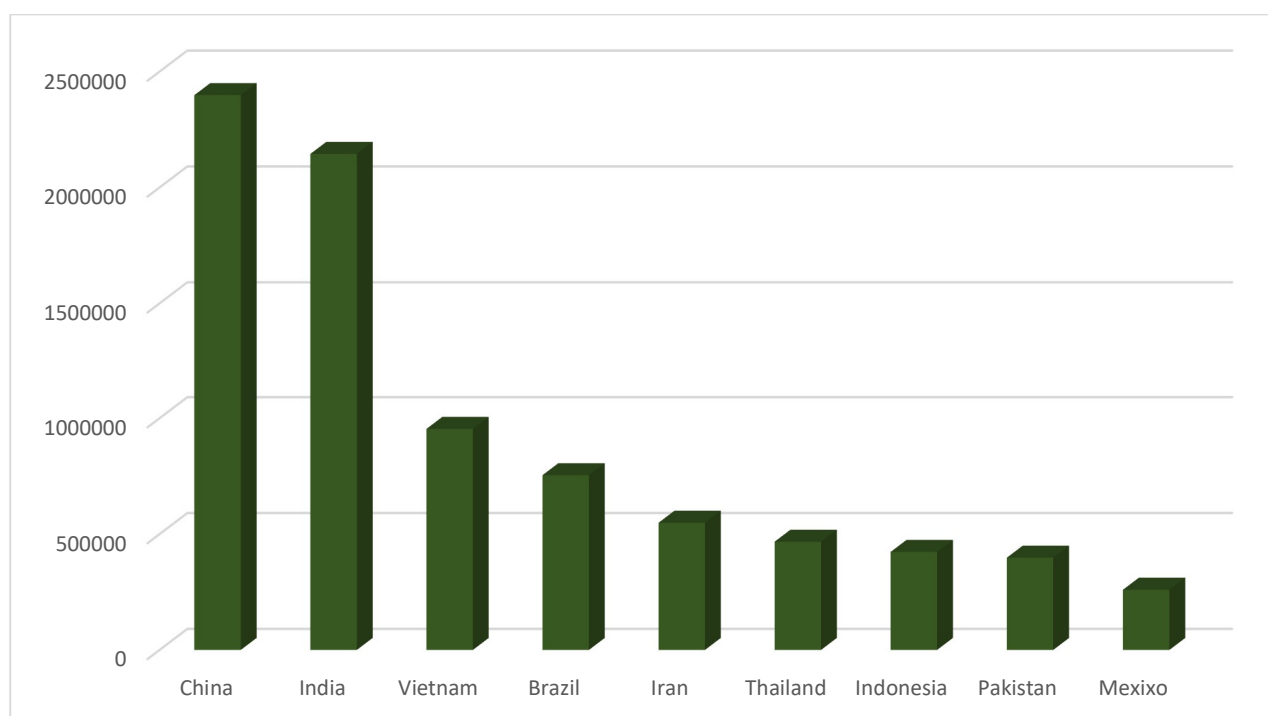
STATE -	CASES -
Uttar Pradesh	6280
Karnataka	5839
Maharashtra	3511
Assam	2022
Telangana	1207
Rajasthan	1104
Madhya Pradesh	740
Gujarat	702
Haryana	418

So users of internet should be aware of the cyber-crime and should have a unique password and make use of the anti-virus software.



CYBER CRIME DURING PANDEMIC

The spread of novel coronavirus pandemic across the world creates fear in mind of people. This period of social distancing, wearing masks and staying at homes. Everyone is sitting at their homes in this lockdown and trying to get information related to COVID 19 to remain safe. In this period, misinformation also leads to the already existing dark elements of the society. In this period of COVID 19, cyber crime increases at a high rate. There are many fake apps and fake domain name websites which give fake information to create fear among the people. Nowadays, the concept prevailing in society is WORK FROM HOME, which means that people are working from their homes by means of various electronic devices. Earlier the number of people using internet was 4.57 billion, but, due to this lockdown, internet consumption rose by 13% and THAT MEANS CYBER CRIMES HAS ALSO INCREASED BY 86% IN INDIA BETWEEN APRIL AND MARCH.



CYBER CRIMES IN DIFFERENT COUNTRIES

By the means of various online meeting apps, people are working from their homes. Some of the apps are fake which access the data of a person by accessing their IP address and some websites contain cookies which also steal personal information.

Many apps which claim that they can give information related to coronavirus and trace infected person but they actually trace personal information and access to their device. Many web sites target private citizens and violate their personal information. Most important is the PM cares fund established by prime minister office. At least half of the fake versions of the websites developed

which take away the money from the people by means of fraud. Related to this many complains received by home ministry.

But this is only the disadvantages of technology, there are many advantages of technology. People can make better use of technology only if they are aware and make use of it properly after reading all terms and conditions. During this pandemic the internet helps the people in many ways –

- Teachers are able to take online classes and interact with the students. This reduces the hindrance in studies.
- Teachers can take online assignment and online test of the student.
- It also helps in tracing infected people.
- Big and small organisations alike have all their employees working on online mode.
- People can do online shopping which reduces crowd in the market and hence it reduces the infection.
- Nowadays people can also access online medical facilities by consulting their doctors.
- Online hearing of cases is going on in courts to avoid delay in justice. On April 6th the Supreme Court by using its power provided for under Article 142 of the constitution, issued certain directions related to the functioning of courts through video conferencing during this pandemic situation. There are virtual court hearings which means no physical court room for hearing. There is also the concept of e-filing which makes urgent hearing possible through virtual conference. But because 90% of the advocates and judges are unaware of the technology the Bar Council of India (BCI) has opposed the virtual hearing process.

So, people must be aware of the technology to make better use of it. As now half of our work is done with internet

AWARENESS AMONG PEOPLE

In India only a few people are aware about the Information and Technology laws. The IT Act does provide effective legal provision but systematic and proper implementation is needed at wider range. Government should create awareness among the people by various camps. Some of the tips which people must be aware of are –

- **KEEP STRONG PASSWORD-** Users should keep different passwords for different websites and password should be at least of ten digits which must be combination of upper case, lowercase and symbols.
- **SOFTWARE UPDATED –** Cybercriminals usually known exploits software to gain access to your system so users must update their software frequently.
- **USE FULL SERVICE INTERNET SECURITYSITES –** Users should access websites which are safe, free from cookies and viruses.
- **MANAGE SOCIAL MEDIA SETTINGS –** Now a days we can see that more than half of population is on different social media platforms and therefore the users should keep their personal and private information locked down.
- **USE OF ANTI – VIRUS SOFTWARE -** Anti – virus software helps to protect your computer against malware and cybercriminals. It seeks to block or remove malware as quickly as possible.
- **TAKE MEASURES TO PROTECT YOURSELF AGAINST IDENTITY THEFT -** It is important to guard your personal information over internet. A VPN (Virtual Private Network) can help to protect the data online, especially when accessing the internet on public Wi-Fi. In the absence of awareness among the people fake news, rumours, posting hated materials become very common. Many posts on social media and many comments go on unreported because only due to absence of awareness among the people.

CONCLUSION

Many efforts are being made nationally and internationally against cyber crime. The Indian police has started special cyber cells across the country and have started educating people so that they can have knowledge and they can protect themselves against such crimes. Nowadays cyber law and IT Act are being taught in colleges and schools for creating awareness among the students. By setting a strong password, updating software, managing social media settings, securing data by installing antivirus software, installing firewalls and by educating children about it we can reduce cyber crimes. Many governmental and private agencies like the CIA, the FBI and the state police are working to detect hackers and to protect people as well as their data. People should also be aware and cooperate with the government.

REFERENCES

Websites

- www.wikipedia.com
- www.barandbench.com
- <http://www.latestlaws.com/library/legal-document>
- <http://www.legalservices.com/article/ITact/1136>
- www.bitly.com
- www.thehindu/survey/cybercrime