PANCHAKOTesSAYS
ISSN : 0976-4968
Vol-13, No.-2, Nov 2022

Cyber Security and Human Rights

Dr. Chandan Bandyopadhyay [1*]

[1*] Associate Professor, Department of Economics, Asansol Girls' College, Asansol, West Bengal, India.
Email Id: chban_econ70@yahoo.com

Abstract

Internet is widely used by the world population. It is used in every sphere of life from education to medical practices to financial transactions to communication etc. In doing all these with the help of the internet there may be some sort of disturbances or obstacles appear which will hamper not only the user&#39;s device but also the user&#39;s personal identity, private documents, privacy and also it may cost you a sum of money. This is known as 'cyber crime'. Cyber security or IT security refers to the practice of ensuring the integrity, confidentiality, and availability of information. Human Rights are the basic rights which each and every human being in the world has. Substantive provisions of certain cybercrime laws, particularly those that are Internet content-related such as disrespect for authority, insults, defamation of the head of state, and obscenity or pornographic material, may unduly restrict the exercise of certain human rights (UNODC, 2013, p. xxi and 114-115).

KEYWORDS: Cyber crime, Cyber security, Human Rights, UDHR, Hackers, Virus

INTRODUCTION

Internet is used worldwide by the world population. Its usage has beneficial effects on our life. From education to banking, finance, communication, office work etc. everything is dependent on the internet. It helps in searching information, doing research works, playing games, making payments, doing office related day to day work, communicating with doctors, with friends. The list is not exhaustive, one can add anything from his/her domain to get the facility. India had around 687.6 million Internet Users in January 2020 as per Digital India's Report and from this we can estimate the reach and growth of Cyber Space in India.

It is used by the population of different age, caste and creed, religion. Even kids are playing with the help of the internet; actually now-a-days they enjoy the most in this domain. People are eager to connect themselves with the internet as soon as possible as their day starts. A country's economy will be more developed with the increase in internet usage, i.e., a developed country has more internet users compared to the lesser developed country.

Cyber space is the term used for specifying the space or domain where internet facility is available and used. It consists of working with an internet interface, connecting or communicating with people through emails, social media like facebook, twitter, instagram etc. different payment modules like internet banking, UPI, mobile apps for different banks. It helps in doing and/or completing the job faster.

Cyber space is a virtual space which is created with the help of the Internet. This space is not tangible and does not have a real existence. The communication of messages in this space can only be done from one system to another system with the help of the internet. The cyber space provides for effective communication so that messages reach from one part to another part of the real world through this virtual world. Cyberspace can also be used as a place of business and for expansion of business, playing virtual games, using artistic skills and for social interaction.

In doing all these with the help of the internet there may be some sort of disturbances or obstacles appear which will hamper not only the user's device but also the user's personal identity, private documents, privacy and also it may cost you a sum of money. This is known as ‘cyber crime’. In general cybercrime may be defined as “Any unlawful act where a computer or communication device or computer network is used to commit or facilitate the commission of crime”.

DIFFERENT TYPES OF CYBER CRIME

Computer Virus: It enters the user's computer and damages/alters files/data and replicates themselves. It can also damage the device.

Worms: They make copies of themselves again and again on the local drive, network shares, etc. and can also damage the whole networking system.

Trojan: It is not a virus. It looks like a genuine application and is a destructive program. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.

Ransomware: It is a type of computer malware that encrypts the files, storage media on devices like desktops, Laptops, Mobile phones etc. The victim is asked to pay the demanded ransom to get his device decrypted.

Child sexually abusive material (CSAM): refers to material containing sexual image in any form, of a child who is abused or sexually exploited.

Cyber Bullying/Stalking/Grooming: These are forms of harassment through the use of electronic communication by a person to follow or attempt to contact. Communication devices such as computers, mobile phone, laptop, etc. are used in bullying or stalking. Cyber Grooming is when a person builds an online relationship with a young person and tricks or pressures him/ her into doing sexual act.

Online Job Fraud: It is an attempt to defraud people who are in need of employment by giving them a false hope/ promise of better employment with higher wages.

Financial fraud: There are many types of financial fraud activities. Phishing is one such type of fraud. It steals personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source. Credit card (or debit card) fraud involves an unauthorized use of another's credit or debit card information for the purpose of purchases or withdrawing funds from it. Cryptocurrency is a digital currency. People are investing in cryptocurrency like investing in stock markets. Cryptojacking is the unauthorized use of computing resources to mine cryptocurrencies.

Online Drug Trafficking: It is a crime of selling, transporting, or illegally importing unlawful controlled substances, such as heroin, cocaine, marijuana, or other illegal drugs using electronic means.

Espionage: It is the act or practice of obtaining data and information without the permission and knowledge of the owner. (National Cyber Crime Reporting Portal).

CYBER SECURITY

Cyber security or IT security refers to the practice of ensuring the integrity, confidentiality, and availability of information. It consists of an evolving set of tools, risk management approaches, technologies, training, and best practices designed to protect networks, devices, programs, and data from attacks or unauthorized access.

Some common cyber security were:

Network Security: It guards against unauthorized intrusion of your internal networks due to malicious intent and also secure networks by protecting infrastructure and inhibiting access to it.

Cloud Security: It protects and monitors the data in your cloud resources. Cloud providers are constantly creating and implementing new security tools to help enterprise users better secure their data.

Antivirus: It protects the data by scanning known threats in the computer.

LAWS

Cybercrime is a growing concern to the World community. The evolving cybercrime landscape and skills gaps are also a significant challenge for law enforcement agencies and prosecutors. 156 countries (80 per cent) have enacted cybercrime legislation, however the pattern varies by region, as Europe has the highest adopted the legislation more than 90 percent but Africa has adopted only 72 per cent. The role of international law in the cyber context has gained increasing prominence. The Budapest Convention on Cybercrime(2001) is the first international agreement to address internet and computer related crime (cyber crime) taking into consideration national laws. The UN General Assembly’s First Committee on Disarmament and International Security, the G20, the European Union, ASEAN, and the OAS have affirmed that existing international law applies to the use of information and communication technologies (ICTs) by states.

In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. In 2000 the UN GA adopted a resolution on combating the criminal misuse of information technology. In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology. In 1997, G8 released a Ministers' Communiqué that includes an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment. The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cybersecurity issues. In 2003, the Geneva Declaration of Principles and the Geneva Plan of Action were released, which highlights the importance of measures in the fight against cybercrime. In India the act for controlling the cyber crime is The Information Telecommunication Act of 2000, amended in 2008.

THE CONCEPT OF HUMAN RIGHTS

Human Rights are the basic rights which each and every human being in the world has. These rights are provided and guaranteed to all human beings irrespective of caste, creed, gender and colour. Human Rights are inherent rights and these rights cannot be taken in any circumstances. The first legal document that talked about human rights was the Universal Declaration of Human Rights (UDHR) and this document was also adopted by the UN General Assembly on 10th December 1948. UDHR is still considered as the parent document or the constitution of Human Rights, and it refers to all the treaties and conventions which are related to the concept of Human Rights. Some of the rights included in Human rights are Right to privacy, Freedom of Expression and Religion, right to be free and equal, freedom from torture or inhumane treatment etc.

Substantive provisions of certain cybercrime laws, particularly those that are Internet content-related such as disrespect for authority, insults, defamation of the head of state, and obscenity or pornographic material, may unduly restrict the exercise of certain human rights (UNODC, 2013, p. xxi and 114-115). Procedural provisions of cybercrime laws enabling the use of tools and tactics during cybercrime investigations that facilitate the interception of communications and electronic surveillance may also unjustifiably restrict the exercise of human rights, such as privacy (UNODC, 2013, p. 121) .The United Nations Human Rights Council has repeatedly affirmed that the "same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice"

The state and local administrations often restrict internet facility accessible to individuals for internal safety, integrity, peace and harmony. But the state and the government do not have the power to restrict the access of the internet to its citizens. The Supreme Court in its recent judgement in a case lodged when the internet facility was curbed in the State of Jammu and Kashmir, has held that the right of access to the internet is a fundamental right under Article 19 (1)(a) of the Constitution of India and had directed the administration of the State of Jammu and Kashmir to review the orders of curbing the internet and restore the internet facility in the state. Moreover, in 2016, the United Nations Human Rights Council passed a resolution condemning the practice of preventing and/or disrupting individuals' access to the Internet. Kerala became the first state of India in 2017 which has declared that access to the Internet is a basic human right. As a result, the government of Kerala has provided free internet connections to the persons belonging to poor families and at a marginalised rate to the others. Through this the government would provide easy access to both governmental and non-governmental services in Kerala. The people using social media are prone to the risk of human rights violations. The unique user ID which is provided by the social media is easily accessible to the other users of the social media. Such easy accessibility often leads to invasion of the human right of privacy of the individuals, which is not only a human right but also a fundamental right.

CONCLUSION

So cyber crime is a crime happened in the cyber space. It is the virtual world where this type of crime is done. This crime disturbs our life financially, mentally. By cyber bullying or stalking our mental health is disturbed. By trapping in different financial fraud activities our financial health is curbed. Children are mostly fond of playing online games. So they are prone to being under the scanner of cyber crime. Child pornography is a heinous act and this is one of a serious cyber crime. Viruses, worms, malwares are used to steal files and data from our devices. Hackers hack the official system of any company and can steal important information, thereby demanding a ransom from the company. Hackers may also enter into the main system of internal and external security of any country and thereby the sovereignty and the security of that country may be at stake.

India has formulated some specialised as well as general laws for the purpose of dealing with the cybercrimes. The Information Technology Act, 2000 is the specialised law of India which deals which the cyber crimes in the cyberworld. Apart from this, The Indian Penal Code, Code of Criminal Procedure, Companies Act and the Evidence Act also punishes the culprits which are involved in cybercrime. However to protect against cybercrime the Governments enacted laws which may restrict human rights. For example, disruption of internet facility by the State due to security reasons or to maintain peace deprives the citizens of the fundamental as well as human rights.

REFERENCES:

i. Kondo T, Katsenga NN, Zvidzayi T: Cybercrime and human rights: A case for the due process of internet criminals, Forensic Research & Criminology International Journal, Volume 6 Issue 2 - 2018

ii. National Cyber Crime Reporting Portal (India)

iii. NCRB Report

iv. https://www.coe.int/en/web/cybercrime/the-budapest-convention

v. https://en.wikipedia.org/wiki/International_cybercrime#cite_note-Weiping_Chang-1