FIXING LIABILITIES FOR TECHNOLOGY IN CYBER CRIMES – A CRITICAL ANALYSIS

Written by ***Priyesh Pathak***

LL.M. (2022-2023), Hidayatullah National Law University, Raipur, India

DOI: doi.org/10.55662/JLSR.2023.9101

ABSTRACT

The meaning of cybercrime, its concept and types are covered in this research. It further deals with the liability in cybercrimes and whether the liability can be fixed to technology. By the late 1970s, the idea of 'crime by computer' had become a serious problem that called for new criminal laws, but technology's constant growth and continuous penetration into the legal system had not yet had the same destructive impact as it does now. The word 'cyber' has a technological connotation. Cybercrime is the term used to describe crimes committed in this digital age. They are non-violent, bloodless crimes committed by computer users who have a solid understanding of how computer systems work and use intricate, technical techniques. There isn't a single, accepted definition of cybercrime. The most common cybercrimes are click jacking, spyware, email fraud, social media fraud, banking fraud, ransomware assaults, cyber espionage, etc. There are many different sorts of cybercrimes. 'Cyberspace Liability' refers to the issues over liabilities incurred when communicating or conducting business online. The existing legal framework does not explicitly hold technology accountable for any cybercrimes that may be committed. The user, service provider, and person are largely responsible. There is currently no law that makes it possible for technology to be held accountable for cybercrime.

INTRODUCTION

A route toward technical splendor and sophistication had been taken in the advancement of computers, and along with it, the perception and method of crime had also altered. By the late 1970s, the idea of "crime by computer" had grown to be a serious problem that called for new criminal codes, although technology's ongoing development and pervasive penetration into the legal system hadn't yet had the exact catastrophic impact as it has today. Machines are associated with the word "cyber." Cybercrime is the name given to crimes committed in the current digital era. They are non-violent, bloodless crimes committed by computer users who are skilled in using computer systems and who adhere to intricate, technical procedures. There is no unified, accepted definition of cybercrime. Cybercrime is the illegal use of information and communication technology (ICT) to either attack networks, systems, data, websites, or technology, or to facilitate criminal activity. Because it "knows no physical or geographic constraints and can be carried out faster, more readily, and with less effort," cybercrime differs from traditional crime. Cybercrimes occur in a variety of forms, but the most common ones include click jacking, malware, email fraud, social media fraud, banking fraud, ransomware assaults, cyber espionage, and identity theft. The most prevalent ones are discussed in the further chapters. Cybercrime is defined as unlawful behaviour carried out online or through a computer or other electronic device. Cybercrime is the illegal activity of using a computer to access information without authorization. Cybersecurity offers the in-depth understanding of how to thwart or recover from intrusions. "Cyberspace Liability" is the umbrella term used to describe the risks associated with communicating or doing business online. Examples of such threats include email and the Internet. The use of internet communication tools can lead to charges of invasions of privacy, theft or infringement of intellectual property, defamation, workplace discrimination, and contravening obscenity laws. When a cybercrime is perpetrated, the technology is not explicitly held accountable under the present legal framework. Individuals, service providers, and users are primarily held responsible. There is currently no law that makes it possible to hold technology responsible for cybercrime. But as technology advances, especially in the field of artificial intelligence where self-developing technologies are used that are capable of performing tasks without any operator of the technology, it raises the question of whether the inventor of that technology would be held accountable for the technology itself in the event of a crime. The Internet has been used by intelligent individuals

to carry out evil deeds, sometimes for their own financial gain. As a result, cyber rules now come into play and are essential for everyone. In India and throughout the world, people are using computers more and more, thus cyber laws must be updated and enhanced frequently to stay current.

REVIEW OF LITERATURE

Lipinsky, Dmitry A., Konstantin N. Evdokimov, and Aleksandra A. Musatkina. "Regulation of criminal responsibility for cyber crimes in countries with different legal systems." ***Perspectives on the use of New Information and Communication Technology (ICT) in the Modern Economy. Springer, Cham,*** **2017.** This paper describes the criminal laws of Russia and other nations that establish liability for the committing of crimes involving computers. Studying of criminal laws from the Russian Federation and other nations that govern responsibility for the occurrence of cybercrimes is the cognitive objective. A broad result was drawn about a tendency for national criminal law systems to converge in terms of who is accountable for computer information crimes. It specifically manifests itself in the commonalities of corpus delicti and the presence of crimes that are identical in origin and content but differ only in name.

Chowbe, Vijaykumar Shrikrushna. "The Concept of Cyber-Crime: Nature & Scope." ***Available at SSRN 1766238*** **(2011).** The notion of "cyber crime" has been attempted in this paper. From a legal perspective, the study touches on a number of different issues. This paper has studied the operational strategy for combating cybercrime and its likely challenges in the conventional system, which is dependent on several norms that are difficult to manage and seldom respected in cyberspace. These assessments have the goal of determining whether the legal system can function alongside such technologically advanced crime.

Kirpichnikov, Danila, et al. , "Criminal Liability of the Artificial Intelligence." ***E3S Web of Conferences. Vol. 159*****. EDP Sciences, 2020.** This paper clarifies how artificial intelligence's capacity for self-improvement and competition with human intelligence—two traits that put it on a level with people—can be achieved. Given that AI is likely to be acknowledged as a topic of law in the future, the researcher seeks to ascertain in this respect if

it is conceivable to apply criminal culpability to AI. The author draws the following conclusion after doing various analyses and using examples: In addition to having the potential to change its conduct when subjected to coercion, AI is inherently capable of becoming criminally liable.

Viano, Emilio C. "Cybercrime: Definition, typology, and criminalization." ***Cybercrime, Organized Crime, and Societal Responses.*** **Springer, Cham, 2017. 3-22.** This paper examines the topic of cybercrime and provides a comprehensive analysis of the fundamental concept, legal tenets, and remedies to this evolving criminal justice reality. The concept of cybercrime, the legal rights guaranteed by ICT and cybercrime legislation, and other topics are all addressed methodically. It goes into great detail about how widespread criminality is, especially with regard to preparing & possessing. It does centre on the problem of the difficulties and constraints of criminal law. It closes by analysing the legal requirements raised by the globalisation of cybercrime, a feature of this kind of crimes, and then looks ahead to future developments.

SCOPE OF STUDY

The study mainly focuses on whether liability can be fixed on technology in Cybercrimes or not. It studies the meaning and concept of Cybercrimes. This study discusses types of Cybercrimes. It also provides a description of Liabilities in Cybercrimes. At last, the conclusion and findings of the research is described.

WHAT ARE CYBER CRIMES? - CONCEPT AND MEANING

Through the midst of the twentieth century, the infusion of technology had already begun to rip holes in the foundation of the legal system. The development of computers had followed a path toward technological brilliance and complexity, and along with it, the image and mode of crime had also changed. The concept "crime by computer" had become a significant issue by the late 1970's, necessitating new criminal regulations,[i] but technology's persistent advancement and persistent intrusion into the realm of law had not yet had the same devastating effect as it has now. The term spread through the years to have the current evasive and nebulous

character of crime and to describe the stature of cybercrimes. The area of computer law could be traced back to 1960, when IBM and 7[ii] other firms controlled the market for huge mainframe computers, collectively referred to by Douglas W. Jones as "Snow White and the Seven Dwarfs." The first legal article on computer law by Roy N. Freed, which describes "the awakening of the legal mind to the importance and relevance of computers," was published this year.[iii] The term "cyber" is related to machine. Cybernetics is described as "the science of communication and automated control system in both machines and living things" as in Concise Oxford English Dictionary. In 1982, science fiction writer William Gibson used the phrase "cyberspace" for the first time in his book Neuromancer. By then, the term had already become commonly adopted. As a result, the phrase "cyber crime" may indeed be traced to the early 1980s, when the Internet's dimensions first began to open up to new possibilities, and "The Worm of the 88"[iv] is likely the first cyber crime to have been officially reported. The stage was prepared for the new breed of crimes referred to as "cyber crimes".

The concept of cybercrime can be divided into four phases. The first phase is generally called the discovery period which is from 1946 to 1976 and here in this period the main focus is on understanding by explaining computer abuse. The second phase is regarded as the criminalisation period. During this period from 1977 to 1988, it was focused on correcting numerous flaws in criminal law. The third phase is regarded as the hacker's phase. This five year period is shown as intensive law is enforced and efforts were made to identify or to impose sanctions towards hackers and crackers. The fourth phase is the current one, and it is generally referred to as the censorship period. The existing priority of attention has been focused on reducing computer users' access to several "dangerous" systems commonly available over the Internet, such as collections of sexually explicit writings, pornographic images, and information on violence and terrorism. This is due to the Internet's rapid expansion. Those who discovered that huge quantities of wealth could be produced by sale instead of sharing quickly transformed this selfless environment. A sophisticated computer scam that had been committed the year before at the Flagler Dog Track in Hialeah prompted the State of Florida to create the first computer crime legislation in 1978.

The crimes of this digital age are referred to as cyber crime. They are crimes which are bloodless, non-violent, and are carried out by computer persons who are well acknowledged with the operation of computer systems and follow technical and complex methods. Majority

of cyber crimes committed by a number of accomplices called “outsiders and insiders” who work for internet service companies and providers. They are involved in the majority of cyber crimes. *Modus operandi*[v] on which cyber crime is committed is primarily consisting of illegal interference in computer systems and networks. This illegal interference may further be classified into various heads. There is no definition of "cyber-crimes" in any law or regulation. Terminology for everything having to do with computers, information technology, the internet, and virtual reality is "cyber." It follows that "cyber-crimes" are crimes using computers, information technology, the internet, and virtual reality.

Cybercrime does not have a single, agreed definition. Applying information and communication technology (ICT) to either attack network, systems, data, websites, or technology or to assist a crime, cybercrime is an unlawful practice. Cybercrime is distinct from traditional crime in that it "knows no physical or geographic limits and can be carried out more quickly, more easily, and with less effort."[vi] According to Europol (2018), there are 2 types of cybercrime: cyber-dependent crimes and cyber-enabled crimes, or "traditional crimes made easier by the Internet and digital technologies." Cyber-dependent crimes are defined as "any crime that can only be committed using computers, computer networks, or other forms of information communication technology."[vii] The main distinction between these types of cybercrime is how ICT is used in the crime—whether as the intended victim of the crime or as a component of the perpetrator's method of operation.[viii] This cybercrime adversely impacts the "confidentiality, integrity, and/or availability of computer data or systems where ICT is the intended target."[ix] The "CIA Triad" is a set of values that includes availability, integrity, and confidentiality.[x] A typical crime (such fraud and theft, for example) that has been made easier in some manner by the Internet and digital technology is considered a cybercrime when ICT is used as part of the modus operandi.

The working definition for computer-related crime or computer crime adopted by the Organization for Economic Co-operation and Development (OECD) is as follows: "Computer abuse is considered as any illegal, unethical, or unauthorised behaviour relating to the automatic processing and transmission of data."[xi]

Almost all of the aforementioned definitions of cybercrime are missing certain essential information. While just a handful of these mentions the Net, all of them make a mention to

computers. The Internet has created cybercrime. If a definition of cybercrime makes no mention to the Internet, it is insufficient and inappropriate. Moreover, it's noteworthy that the Information Technology Act of 2000 does not define computer or cybercrime either. Even the most important cyber laws in the U.S.A.[xii] and the U.K.[xiii] doesn't define cybercrime. The phrase "computer-related offences" is used in India's Information Technology Act, 2008, where a substantial number of cybercrimes have been added to the list of crimes already recognised as criminal acts.[xiv]

TYPES OF CYBERCRIMES

There are many various types of cybercrimes; the most prevalent ones are click jacking, spyware, email fraud, social media fraud, banking fraud, ransomware attacks, cyber espionage, and identity theft. The most common cyber crimes are discussed below:

- **Malware** - It is a term that consists of a broad range of cyber attacks. For example, warms, viruses, Trojans. It can be simply understood as a computer code written to steal data or cause damage on a computer.

- **Phishing** - It merely means obtaining a request from the third party to access the information. The phishing emails generally consist of a link and the person opens and click on the link will have to provide information relating to personal data. Recent years these emails have become more complex in nature and it is very difficult to distinguish between genuine and fraudulent ones for the user. The steps which are involved in phishing consist of preparation, setting up, to attack, access the information, and does the fraud.

- **Denial of Services (DoS) and Distributed Denial of Service (DDoS) attack** - A denial of service attack, it merely focuses on disrupting the network services. The attacker transmits a huge amount of data traffic through the network system and the operating system becomes overloaded and that led to dysfunctioning of that system. The disturb denial of service attack is the most common one. Here attacker sends huge traffic by using several machines and computers that led to overload the system.

- **Child Pornography and Cyber Grooming -** The term "child sexually abusive material" (CSAM) describes anything that includes pornographic pictures of molested or sexually exploited children in any format. According to Section 67(B) of the Information Technology Act, "it is illegal for posting or sending in electronic form material showing minors in the sexually explicit act, etc." Whenever an individual develops an online contact with a youngster and mislead or forces him / her into performing a sexual act, this is known as "cyber grooming."

- **Cyber bullying and Cyber stalking -** Cyberbullying is a type of exploitation or intimidation committed via computer systems, cell phones, laptops, or other electronic or communication equipment. Cyberstalking is the practise of using "electronic communication by a person to follow a person," or making numerous attempts to get in touch with someone to nurture a personal relationship despite a blatant lack of interest on their part. Cyberstalking also includes "monitoring the internet, email, or any other form of electronic communication."

- **Online Sextortion -** Online sextortion happens when a victim is threatened with having sensitive and personal information distributed via an electronic means if she/he does not offer sexually explicit photographs, money, or special favors.

- **Data Breach and Cyber Squatting -** A situation when data is obtained without authority is known as a data breach. The action of registration, utilising, or trading in a domain name with the purpose of generating revenue from the reputation of a "brand that belongs to another person" is known as cybersquatting.

- **Hacking -** Hacking is the effort to "gain access to a computer's internal private or system or network." In essence, it refers to illegal access to or manipulation of computer network safety mechanisms with malicious purposes.

- **Drug Trafficking Online -** Online drug trafficking involves the illicit sale, transportation, or importation of unauthorized illegal substances including heroin, cocaine, marijuana, or other illegal narcotics through digital mode.

These are the some of the cybercrimes which are commonly observed. Around 4.5 million cybercrimes, India had the largest number in the world in 2020.[xv] Cybercrime is defined as illegal activity carried out while utilising a computer or another electronic gadget that is online. The unlawful act of gaining unauthorized access to computer is known as cybercrime. The detailed grasp about how to stop or recuperate from cyberattacks is provided by cyber security.

LIABILITIES IN CYBERSPACE

The liabilities concerns incurred by conversing or conducting business online are referred to as "Cyberspace Liability." The Internet and email are examples of potential risks. Internet communication tools may give rise to complaints of privacy rights violations, theft or infringement of intellectual property, defamation, workplace discrimination, and breaking obscenity laws. The several liabilities which are prevailing by current legislation are –

Liability of the internet service provider - Internet service providers serve as intermediaries, information carriers, and digital representations of telecommunications firms. Internet service providers not only provide services to consumers but also to big businesses by connecting their networks directly to the Internet. Network Access Points are used to link Internet Service Providers to one another (NAPs). These ISPs have regulatory liability, especially in the US and UK. However, their position is somewhat different, and in these countries, they are subject to fulfill the regulatory compliances. The liability of internet service providers in the regard of failure of communication also there. The liability also arises in case of negligence. Also, the famous case of ***Donghue versus Stevenson***[xvi] is a classic example where the house of lords decided the liability in case of negligent act. In the case of ***Rylands versus Fletcher***[xvii] the strict liability principle arising here also in case of third-party access and computer related viruses entering the system then the owner of antivirus could be made liable. In ***Shreya Singhal v. Union of India,*** the Supreme Court ruled that "if an intermediary looks for exemption under Section 79, IT Act, then it must promptly delete harmful content whenever it is demanded by a court order or by a direction of the government."[xviii] In ***Swami Ramdev v. Facebook Inc***., the Delhi High Court was posed the following question: "whether Internet intermediaries, like as Facebook, Google, YouTube, and Twitter, were required to delete unlawful information when ordered to do so by the government, or if they were required to do so internationally. According

to the court, because the information was posted 'from India' and made publicly accessible, it must be removed 'worldwide' and not only from India when a court or government orders its removal. The court's conclusion is supported by the language of Section 79(3)(b) when combined with Section 2 of the IT Act's definitions of computer resource, computer system, and computer network." Computer networks are included in the term "computer resource," therefore it refers to the full, worldwide network.[xix]

Liability of ISPs under copyright law - A new Directive, known as Directive EU 2019/790 Copyright in the Digital Single Market, was created by the European Union. The Directives intends to establish exceptions to the copyright laws, to enhance licencing procedures, to guarantee greater access to material, and to establish a successful copyright market.[xx] India also grants ISPs a great deal of latitude and a safe zone, according to the restrictions outlined in the aforementioned section. If the ISP can demonstrate they had no knowledge of the infringement or that reasonable care was taken to prevent such activities, Section 79 releases them from responsibility. It is necessary to make clearer about India's view on service providers' culpability for copyright infringement.

Liability of online intermediaries and their components - Online intermediaries are unwitting participants in online transactions and do not already have a legal connection to other participants.[xxi] The largest group in the class of entities subject to responsibility is the online intermediaries.[xxii] The liability of online intermediaries and their components are there if any online intermediaries distribute or publish defamatory material, in the matter of obscenity there online intermediaries would be liable. The liability of employers' vests in vicarious liability or in criminal cases the criminal liability arises.

Corporate liability - Despite possessing a number of rights to its name, a corporation frequently has legal obligations placed upon it. Both civil and criminal consequences are applicable. A firm is accountable for any crimes it commits under the Information Technology Act as well. A firm is liable for the offences it commits, according to Section 85 of the Act. The major purpose of Section 85 is to "limit the company's liability to the IT Act, 2000 regulations exclusively." Although the section's limits have not yet been shown, like several other aspects of the Act, it is clear that an amendment is essential.

Can Technology be made liable in Cybercrimes?

In the above discussion, the observations can be made that the liabilities in cyberspace is limited to the internet service providers or individual or the corporate who are involved in committing the cybercrime, such as infringement of intellectual property laws, defamation, discrimination in the online medium, Breaking any legislation, cyber bullying, cyber, stalking, online, fraud, child pornography, phishing, Or any other similar cyber offences. By observing all the instances, it can be said that the current legal system does not clearly make the technology liable if any cyber crime is committed. The liability primarily imposed on the individual, the service provider, the user. There is no legislation till now which has a provision where the technology can be made liable in the cyber crime. However, the development of technology and especially in the area of artificial intelligence where the self developing technologies are used which are capable of doing the things of their own without any operator of the technology so there is a big question arises whether The creator of that technology would be liable for the technology itself would be made liable in case of commission of crime. The legislation regarding artificial intelligence which has been passed in various countries lacks the information regarding the same. Recently in the news there was a robot that broke the finger of a boy while playing chess.[xxiii] In that type of scenario who would be made liable, there is a big question. The development of automatic self driving cars or self driving vehicles, in case of miss happening or accident by the automated driven vehicle there is the question whether the owner of that vehicle would be liable or the manufacture of that vehicle would be liable or the vehicle itself would be made liable, these are the areas where the legislators and the technocrats together can think and uplift the legislation considering these things. In the commission of cybercrime, if the automated technology itself violates the intellectual property rights or commit, any other form of cyber crimes such as defaming, someone or posting such obscene material, so whether it can be made liable. These are the certain issues regarding fixing the liability to the technology. Till now the user, the creator, the developers have been made liable in many decided cases, but the technology itself to be made liable that day yet to be seen.

Also, there is a question, if in any case the technology would be made liable so what would be the punishment? The legislators while framing the new laws where in future the artificial

intelligence and the self developing technologies would be developed too much. These questions must be kept in mind while framing any laws.

CONCLUSION

In this paper I have discussed the meaning of Cybercrimes, its types and the liabilities in case of commission of cybercrime. The crimes of this digital age are referred to as cyber crime. Cybercrime is distinct from traditional crime in that it "knows no physical or geographic limits and can be carried out more quickly, more easily, and with less effort." Cybercrime is defined as "illegal activity carried out while utilising a computer or another electronic gadget that is online." There are many various types of cybercrimes; the most prevalent ones are click jacking, spyware, email fraud, social media fraud, banking fraud, ransomware attacks, cyber espionage, and identity theft. The liabilities concerns incurred by conversing or conducting business online are referred to as "Cyberspace Liability." The Internet and email are examples of potential risks. Internet communication tools may give rise to complaints of privacy rights violations, theft or infringement of intellectual property, defamation, workplace discrimination, and breaking obscenity laws. Considering every situation, it may be concluded that the existing legal framework does not expressly hold technology accountable for any cybercrimes that may be perpetrated. The user, service provider, and person are largely responsible. There is currently no law that makes it possible for technology to be held accountable for cybercrime. The question of whether the inventor of that technology would be held accountable for the technology itself in the event of a crime, however, is raised by the development of technology, particularly in the field of artificial intelligence where self-developing technologies are employed that are capable of performing tasks without any operator of the technology. Intellectual people have turned the Internet into a tool for wicked activities, which they occasionally use for monetary advantage. Cyber laws therefore enter the picture at this time and are crucial for every person. Some actions are categorised as dark actions that aren't subject to legal regulation since cyberspace is a very challenging area to manage. Considering people relying more and more on computers, both in India and throughout the world, cyber laws need to be updated & improved on a regular basis to keep ahead. As a result of the epidemic, it has also resulted in a considerable rise in the number of remote employees, which has raised the requirement for security controls. Lawmakers must take additional steps to be one point ahead

of the scammers in order to take measures towards them when they appear. If politicians, internet service providers, banks, online retailers, and other intermediaries cooperate, it may be stopped. Nevertheless, the decision to take role in the fight over cybercrime rests entirely with the users. The only option for the development of online security and resiliency to occur is by taking into account these players' activities and making sure they adhere to the rules of cyber world. There is also need to think whether if automated technology commits offence itself so there is no law where the technologies could be made liable, as the further advancement of technology, there is a possibility in future where the liability could be fixed on technology involved in cybercrimes.

ENDNOTES

[i] Richard C. Hollinger, "Computer Crime" in Clifton D. Bryant (Ed.), *Encyclopedia of Criminology and Deviant Behavior*, Vol. II (Brunner-Routledge, Taylor & Francis Group 2000) 76–81.
[ii] Seven Companies often referred to as BUNCH which stood for Burroughs, Univac, NCR, Control Data, Honeywell, plus GE and Xerox.
[iii] Roy N. Freed, "A Lawyer's Guide Through the Computer Maze", *The Practical Lawyer, (*November 1960).
[iv] On 1-11-1988, a malicious program called the "Internet Worm appeared and disabled about 6000 of the total Internet hosts." Herbert. A. Bloch, "Theory into Practice". What is Crime? The example against the Environment. *Crime in America*, Philosophical Library, Inc. 15 East 40th Street New York 1961, 9.
[v] *Modus operandi* is a Latin phrase meaning "mode of operating" or "operating method".
[vi] Cybercrime in brief, Module 1: Introduction to Cybercrime, E4J University Module Series: Cybercrime , First published in May 2019, updated in February 2020. Accessed on : https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html
[vii] McGuire and Dowling, 2013, p. 4; Europol, 2018, p. 15
[viii] UNODC, 2013, p. 15
[ix] UNODC, 2013
[x] Rouse, 2014
[xi] Suresh T. Vishwanathan, "The Criminal Aspect in Cyber Law" in The Indian Cyber Law (Bharat Law House (P) Ltd. 2001) 81.
[xii] In the US, "different Acts are passed which are computer crime specific."
[xiii] The Computer Misuse Act, 1990 became a law on 29-8-1990. The Act introduced "three new categories of offences: unauthorised access to computer material, unauthorised access with intent to commit a further offence and unauthorised modification." Ian Walden, Chap 9 "Computer Crime" in Chris Reed (Ed.), Computer *Law* (3rd Edn., Oxford University Press 2003).
[xiv] By virtue of S. 32, IT (Amendment) Act, 2008, new S. 66 is substituted and new S. 6(A–F) is inserted in the IT Act, 2000.
[xv] Shivani Shinde & Neha Alawadhi, "India becomes favourite destination for cyber criminals amid Covid-19", *Business Standard*, Last Updated at April 6, 2021 23:45 IST. Accessed on : Friday, October 7, 2022 | 02:17 PM IST , https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.html
[xvi] *1932 AC 562*
[xvii] *(1868) LR 3 HL 330 (HL).*
[xviii] *Shreya Singhal v. Union of India, (2015) 5 SCC 1*
[xix] *Swami Ramdev v. Facebook, 2019 SCC OnLine Del 10701*
[xx] .EUR-Lex: Access to European Union Law. Initial date of creation 11-8-2019,

[xxi] Chris Reed, Chap 2 "From Each According to His Ability: Actors and Activities in the Internet World" in Internet Law: Text and Materials (Cambridge University Press, 2004; Universal Law Publishing, First Indian Reprint 2005) 89.

[xxii] *Ibid*

[xxiii] Sounak Mukhopadhyay, "AI gone wrong? Chess robot breaks child's finger at Russia tournament",*Mint,* Updated: 24 Jul 2022, 08:39 PM IST. Accessed on : Friday, October 7, 2022 | 02:59 PM. https://www.livemint.com/news/world/ai-gone-wrong-chess-robot-breaks-child-s-finger-at-russia-tournament-11658674872366.html