Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 4, 1279-1287

An Analysis of Cyber Crime with Special Reference to Cyber Stalking

Ms.Sakshi
Research Scholar, K.R. Mangalam University, Gurugram, Haryana 122103, India
Sakshidudeja59@gmail.com

Dr. Archana Vashishth
Assistant Professor, K.R. Mangalam University, Gurugram, Haryana 122103,
Indiaarchana.vashisth@krmangalam.edu.in

Dr.Teena
Assistant Professor, GDGoenkaUniversity, Gurugram, Haryana 122103, India
teena444parmar@gmail.com

Abstract

As we are all aware that the internet and mobile phones have entirely turned the physical world into a virtual one. The Covid 19 pandemic also gives this virtual world a new ray of hope. Everyone now falls under the umbrella of the internet, whether they are school-aged children, adults, or senior citizens. Everyone is using social media or other internet-based platforms to share their precious time. However, in this virtual environment, anyone can disguise or personate his identity in order to commit crime and easily hide. India is advancing toward a digital India, but there are few laws and technological tools in place to address the issue that is arising as a result of this virtual virus. Cybercrime is defined as any criminal behaviour that involves the use of a computer as a tool, target, or weapon. There are number of cyber crime and cyber stalking is one of them. Cyber stalking refers to following someone using a computer and everything related to a computer that can instill terror in the victim's mind. This study will analyse the meaning and typology of cyber crime. The purpose of this article is to investigate the number of cases increasing in India from 2012-2020. In addition, this research will also look into the meaning, type and reason of cyber stalking. The Indian legal system as well as judicial decision will also be explored in this article.

Key words: *cyber crime, Computer, Technology, Cyber Stalking, IT Act 2000*

Purpose of Research:

- To study the meaningand typologyof cyber crime.
- To explore the growing number of cases of cybercrime.
- To understand the meaning, type and reason of cyber stalking.
- To examine the legal provisions of Indian legal system.

.

Methodology:

The study is doctrinal in nature. The present work titled as "An Analysis of Cyber Crime with special Reference to Cyber stalking" will be based on primary as well as secondary data. The sources of data collection are report of NCRB, articles, books, case laws etc.

Introduction:

It's almost hard to imagine a world without technology. We all use technology for work, shopping, leisure, and other purposes. On the one hand, technology provides convenience by saving time and supplying everything we require, but it also has a darker side, which is the formation of a new sort of crime known as computer crime or cyber crime.

A cyber crime is one in which a computer is used as a target, instrument, or other means of committing a crime. Almost all cybercrime focuses on an individual's, corporation's, society's, or government's information. Cybercrime is the cyber world's newest and arguably most difficult concern. To commit such crimes, criminals use technology. One of these is cyber stalking, which is when someone is followed through communication technology. Cyber stalking occurs when a stalker makes repeated attempts to contact someone else with the intent of influencing the victim's life or instilling fear in him. The traditional stalker has been supplanted by a cyber-stalker. In addition, stalkers can now hide their identities thanks to advances in information technology, which allows offenders to remain peacefully indoors while committing crimes anonymously and at a low cost.

While cyber stalking is based on the same harassment concepts as traditional stalking, the victims are mostly found online. The most frequent methods of attempted cyber stalking are emails, the internet, chat rooms, and the developing social networks such as Facebook. Several researches have discovered that.Cyber stalking victims can be both male and female.

The term "cybercrime" does not have a clear definition under Indian law. In reality, even after being amended by the Information Technology (Amendment) Act 2008, the Indian Penal Code does not utilise the phrase "cybercrime" at any time.

Meaning of Cyber Crime:

Cybercrime is an offence involving a computer, computer network, electronics, and electronic communication, as well as information methods, in which the computer is utilised as a tool, a target, or both.

"Cyber Crime" can be defined as any criminal conduct involving electronic communications or information systems, including any device or the Internet, or both or both of them. In brief, "Cyber Crime" refers to offences or crimes committed via electronic communications or information technologies. The term cyber refers to the computer-modeled information space in which various items or information in the form of symbols and images exist. As a result, the place where computer programs operate and data processing takes place.[1]

The term "cyber" comes from the phrase "cybernetics," which means science of communication and control over machines and people. Cyberspace is a new horizon intended for information and communication between human being from all over the world that is controlled by machines. As a result, cybercrime refers to crimes performed in cyberspace involving equipment or devices, as well as crimes involving cyber technology. Information technology and internet commerce are frequently utilised to aid or perpetrate criminal activity. Hacking, terrorism, fraud, unlawful gambling, cyber stalking, cyber theft, forgery, and cyber pornography are all examples of cyber crime in a broader sense.

Classification of Cyber Crime:

Cybercrime classification is a difficult endeavor since it is a new type of crime with an ever-increasing and developing problem.

Cybercrime can be categorised in a number of ways.One method is to divide the computer into five categories:

1. Cyber Crime against individuals:

The term "crimes against the individual" refers to criminal offences that are committed against an individual's will, such as bodily harm, threat of bodily harm, harassment, kidnapping, and stalking, etc. However, in the context of cyber crime, this category can include cyber stalking, distributing pornography, trafficking, cyber bullying, child soliciting, and abuse. Such cybercrime has a negative impact on an individual's psyche and the psychology of the younger generation. The following are some of them:

- **Cyber-stalking**: Cyber stalking is a crime in which an individual or a group of individuals uses a digital device such as the internet or other communication tools to follow another person. Cyber stalking is a criminal act that includes a computer or computer-related technology such as the internet. Cyber stalking is usually motivated by vengeance, hatred, or envy. Cyber

[1] JyotiRatan, *Cyber Laws & Information Technology* 62 (Bharat Law House, Delhi,6thedn., 2017)

stalking instills fear in the victim's mind by unwanted or threatening activities.

- **Cyber defamation:** Cyber defamation is an act in which an offender insults or defames another person using electronic means in the cyber realm, with the intent to harm that person's reputation. Cyber defamation can take the form of both written and oral communication. Defamation can be regarded a civil as well as a criminal offence in India, hence the Indian legal system provides legal redress to the victims.
- **Email spoofing:** The victim of email spoofing received the falsified email from someone or somewhere other than the legitimate source. The fundamental goal of email spoofing is to get the recipient to open, respond to, and interact with the message. For instance, a spoof email that purports to be from a well-known shopping website and requests personal information such as a password or credit card number. Alternatively, a faked email may contain a link that, if opened, installs malware on the recipient's device.
- **Spamming:** Spamming is when someone sends an unwanted mailor message to a large group of people for the purpose of commercial advertising, non-commercial evangelising, or any other offensive goal.

2. Cyber Crime against the Society:

If a crime is done with intention of causing harm via using cyber means to the society at large or number of the people.[2]

- **Forgery**: It is defined as the formation of a false document, signature, money, or revenue stamp etc.

3. Cyber Crime against Property:

Cybercrime against all sorts of property is the second category of cybercrime. As international trade grows, firms and consumers are increasingly adopting computers to create, transfer, and retain information in electronic form rather than conventional paper documents. Certain offences have a direct impact on a person's property. Some of the examples are:

- **Software piracy**: In the instance of software piracy, the offender has the ability to duplicate the software without authorization.
- **Copyright infringement:** It is characterised as a breach of an individual's or organization's copyright. In this scenario, the person has unauthorizedly copyrighted the material of another person who owns the copyright to such work, such as music, software, and so on.
- **Trademark infringement**: It is described as the unlawful use of a service mark or trademark.

4. Cyber Crime against Organization:

Certain offences are committed by a group of people who use the internet to threaten a firm, a company, or a group of people. These cybercrimes are known as cybercrimes against Organization. Here are a few examples:

- **Email bombing**: It’s a type of Internet abuse in which someone sends a large number of emails sent to a single email address in order to flood the mailbox or server that holds the email address.
- **DOS attack:** In this attack, the attacker floods the servers, systems or networks with traffic in order to overpower the victim resources and make it infeasible or problematic for the users to use them.”[3]

Other cyber crimes against organizations includeSalami attack, logical bombs, Torjan horses, data tampering, and so on.

5.Cyber Crime againstGovernment:

When an offender's act targets not only a single person or group of people, but also the international government, it is classified as cyber crime against government. Cybercrime against the government can take the form of a cyber

[2] Harpreet Singh Dalla& Ms. Geeta, “Cyber Crime – A Threat to Persons, Property, Government and Societies” 3*ARCSSE* (2013).

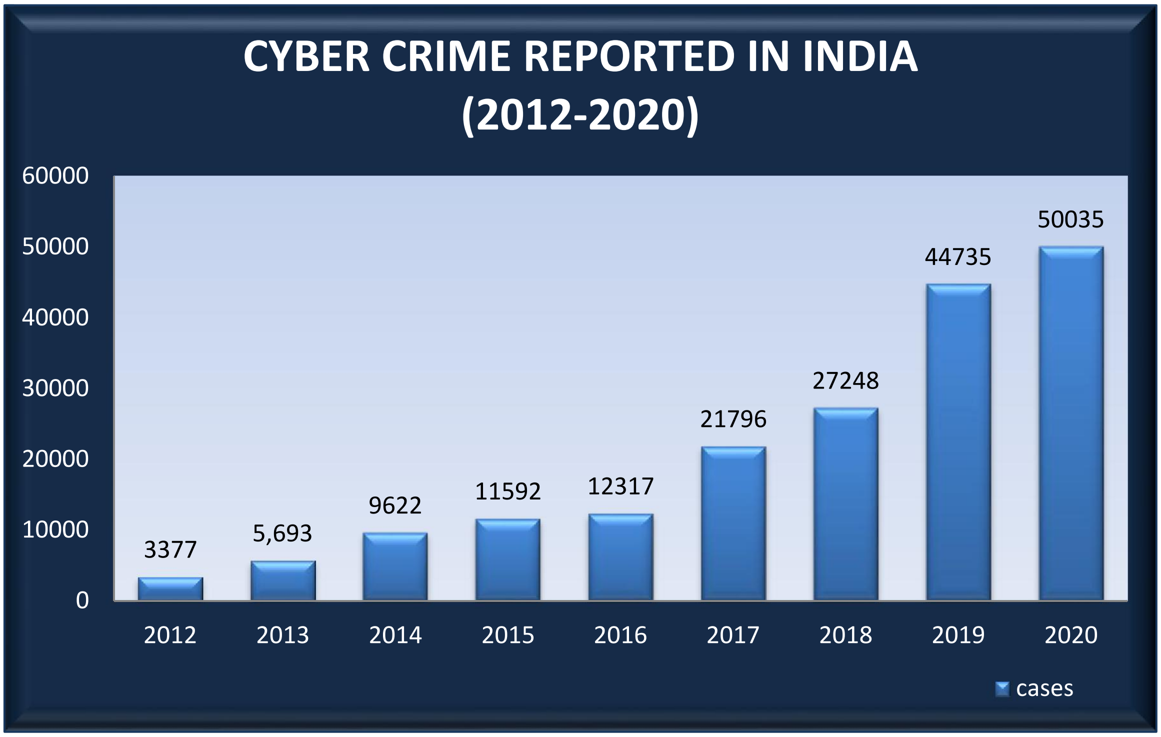
[3] AnimeshSarmah, RoshmiSarmah and AmlanJyotiBaruah, “A brief study on Cyber Crime and Cyber Law’s of India” 4 *IRJET*1635 (2017)

attack on a government website, military website, or cyber terrorism etc.

- **Cyber Terrorism-** Issue of Cyber terrorism concern both domestically and globally. Terrorist attacks on the Internet include distributed denial of service attacks, hate emails and hate websites, and attacks on sensitive computer networks, etc. Cyber terrorism poses a danger to the country's security and dignity.

Analysis of Cybercrimes in India:
According to the latest NCRB data, a total of 50, 035 cases of cybercrime were registered in India in 2020.

Total number of cyber crimes reported in India from 2012-2020.[4]



(Source: - www.Statista.com visited on- 15 Jan 2022)

[4] https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece

Meaning of Cyber stalking:

Cyber stalking is a crime in which a person or a group of people uses a digital device such as the internet or other communication tools to harass another person. It entails engaging in a pattern of behaviour that involves sending or causing to be sent words, images, or language to a specific person via mail or electronic communication, causing that person significant emotional distress and for no valid purpose.

Bocij, Griffiths and McFarlane: Hedefines cyber stalking as "a group of behaviour in which an individual/s or the whole organisations uses information and communications technology to harass one or more individuals.[5]

According to Fisher, B.S., F.T. Cullen, and M.G.Turner*: "*Cyber stalking involves the use of technology (most often, the Internet!) to make someone else afraid or concerned about their safety.[6]

According to Brenner: "In a sense, cyber stalking and cyber harassment are lineal descendants of the obscene or annoying telephone call offenses that were created roughly a century ago, to address harms resulting from the misuse of a nineteenth century technology".[7]

According to Baer: "Cyber stalking in particular is composed of words alone and therefore stands more distinctly as apart as a crime of accumulation".[8]

According to Ellison and Akdeniz : "the term cyber stalking as online harassment, which may include various digitally harassing behaviors, including sending junk mails, computer viruses, impersonating the victim, etc.".[9]

Types of Cyber Stalking:

1. **E-mail Stalking**: One of the most common forms of modern days stalking includes unsolicited emails in the form of hate/provoking messages, obscene/vulgar content, threats, and more.[10] This also includes the monitoring of the acts of the victim to check his/her usage on the computer to send viruses and malwares through email junk files in order to earn easy money by inducing the victims to pay a hefty sum to clean their systems off all the malwares.
2. **Internet Stalking**: A little too far from physical stalking, this form specifically associates with the acts wherein a stalker can literally set up his base thousands of miles away from the victim and still succeed with his ill-motives. Some of the acts includes monitoring of the social media accounts and check ins by the victim or cat fishing in which a fake profile is created to approach victims as happened in the case of Megan Meier.[11] A few more acts include hijacking of victim's webcam, tracking victim's location through communication and information devices.[12] There are also

[5] Cyber Stalking: Challenges In Regulating Cyberstalking At The Cyber Space, AravinthBalakrishnan http://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyber-space.html

[6] Fisher, B.S., F.T. Cullen, and M.G. Turner, "Being pursued: Stalking victimization in a national study of college women",1 Criminology & Public Policy 259, (2002).

[7] DebaratiHalder,"Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws
in India from Restorative Justice and Therapeutic Jurisprudential Perspectives",*TEMIDA*107 (2015)

[8] Ibid

[9] Supra note 5 p.108

[10] Supra note 4.

[11] Karen L. Paullet, Daniel R. Rota, Thomas T. Swan, "Cyberstalking: An Exploratory Study Of Students At A Mid-Atlantic University" 10 *Issues in Information Systems* 641(2009).

[12] What is Cyberstalking, Jatin Sharma, 15 April 2020

some instances which have proved that a huge number of internet stalking happening currently takes place more on a public dimension rather than private in order to slander and endanger the victims.[13]

3. **Computer Stalking**: Although it is a form of Internet Stalking, but the nature of it and it's gradual widespread throughout the globe makes it a separate category. It is more of a peer to peer, i.e., person to person type of stalking where the stalker gets access to the victim's computer simply by connecting and syncing his own computer to the victim's with the help of internet which makes it possible for the hacker/stalker to use his own computer as the controller for the victim's system and the only way out of this is to disconnect the victim computer from the internet and then completely relinquishing the current internet address which is not an easy task for a layperson.[14]

Reason behind Cyber Stalking:

1. **Jealousy**: Jealousy can be ainfluential motivation for stalking, particularly when it involves ex-lovers and present partners.
2. **Erotomania:** Erotomania is a sort of stalking belief in which the stalker believes the victim, who is usually a stranger or well-known person, is in love with him. It always entails having a sexual attraction to someone.
3. **Obsession and attraction**: Obsession and attraction could be another reason for stalking. The stalker may be sexually or mentally attracted to the victim
4. **Sexual harassment**:Cyber stalking is said to be mostly motivated by sexual harassment. This is due to the fact that the internet reflects actual life.
5. **Revenge and hatred**: Even when the victim is not the source of the stalker's feelings of hatred and revenge, he or she remains the stalker's target. The stalker appears to find the internet to be the most convenient medium for expressing his hatred and vengeance.

Legal provisions of cyber stalking:

Section 354D of the IPC contains provisions relating to cyber stalking. Prior to the Criminal Amendment Act of 2013, there was no express law relating to cyber stalking, however the Amendment Act has added the legal provisions of this offence.

This section can be used to punish a man who follows a woman or tries to contact her in any way, whether physically or through the internet. Stalking imposes a penalty of up to 3 years in imprisonment and a fine for the first offence and up to 5 years in imprisonment and a fine for the second offence. Aside from that the rules under Sections 499, 507, 503, 509,292 of the IPC can also attract cyber stalking.

"Punishment for sending offensive messages through communication services, etc." is covered by Section 66A of the IT Act 2000. Any person, male or female, who sends an offensive message through a communication medium that causes fear, annoyance, hurt, insult, or other injury can be sentenced to up to three years in imprisonment under this section. This section was removed after the case of Shreyasinghal vs. U.O.I.

Under Section 67 of the Act, a stalker who sends or uploads any obscene content to the victim via electronic media faces a five-year prison sentence and a fine of Rs. one lakh. They will be punished to ten years in prison and a fine of Rs. 2 lakh if the incidence occurs again. Section 67A has created a new category called "material containing sexually explicit activity." For the first offence, publishing, transmitting, or encouraging the transmission of such material is punishable by up to five years in jail and a fine, and for the second offence, up to seven years in prison and a fine. Aside from that, this offence is addressed in sections 67B and 66E of the IT Act 2000.

Cases related to Cyber Crime:

RituKohli Case:

"The Manish Kathuria case was the first reported incidence of cyber-stalking in India, and it was the basis for the revision to the IT

https://www.lawyered.in/legal-disrupt/articles/what-is-cyberstalking/

[13] Supra, note 4.

[14] Ibid.

Act. It featured the stalking of a woman called RituKohli. Kathuria stalked Kohli on a chat service, verbally attacked her, and then distributed her phone number to a lot of individuals. Later, he began chatting on the website "www.mirc.com" using Kohli's identity. As a result, she began to receive over forty obscene phone calls at strange hours of the night for three consecutive days. This situation compelled her to contact the Delhi Police Department. The IP addresses were located and Kathuria was arrested under Section 509 of the Indian Penal Code as soon as the complaint was filed. Because the IT Act had not yet come into effect when the complaint was submitted, it was not used in this case. While there is no record of any following proceedings, this case prompted Indian legislators to recognise the necessity for cyber-stalking legislation. Even then, it was only in 2008 that Section 66-A was introduced. As a result, cases are now being reported under this section rather than Section 509 of the Indian Penal Code."[15]

The Bank NSP Case:

"One of the most well-known cybercrime incidents is the Bank NSP case, in which a bank management trainee was engaged to be married.. Using the corporate computers, the pair exchanged several emails. After they broke up, the girl made up fake email addresses "indianbarassociations" and sent emails to the boy's international clients. She did this on the bank's computer. The boy's business lost a lot of customers, therefore took the bank to court. . The bank was found responsible for emails sent through its system."[16]

Parliament Attack Case:

"This case was handled by the Hyderabad Bureau of Police Research and Development. The terrorist who attacked the Parliament was found with a laptop. The laptop taken from the two terrorists who were gunned down on the 13th of December 2001 while the Parliament was under siege was sent to the BPRD's Computer Forensics Division. The laptop contained several proofs that affirmed the two terrorists' motives, including a Ministry of Home sticker that they had created on the laptop and affixed to their ambassador car to gain access to Parliament House, as well as a fake ID card with a Government of India emblem and seal that one of the two terrorists was carrying. The emblems (of the three lions) were meticulously scanned, and a seal was crafted with care, complete with a Jammu and Kashmir residential address. However, meticulous examination revealed that everything was forged and created on the laptop."[17]

StateofTamilNaduv.SuhasKatti:

"This case was the first in India to be decided under Section 67 of the Information Technology Act. Several indecent, calumniator, and vexing messages were posted on a Yahoo messaging cluster about the victim, who is currently divorced. Messages of this nature result in phone calls to the sufferer. On filing a single FIR, the perpetrator, who was formerly a family member of the victim, was arrested and found guilty of the crimes listed in IPC Sections 469, 509, and IT Act Section 67."[18]

WilhelmusWeijdeveldv.India:

"This was considered a primary instance under Section 67B of the Act. Wilhelmus, a Dutch national, came to India as a tourist in 1980 and started an orphanage. He was handcuffed in 2002 after receiving a tip from INTERPOL that he was using to upload pornographic content. It was subsequently discovered that a Dutch national had also sexually abused five orphaned boys in the institution."[19]

StateofTamilNaduv.Dr.L.Prakash:

"This is a landmark case in which the perpetrator, a well-known Tamil Nadu doctor, was imprisoned for creating pornographic recordings with his patients and publishing photographs and videos on the internet.The arraignment for was based on many IPC

[15] https://www.legalindia.com/tag/ritu-kohli-case/

[16] https://www.cyberralegalservices.com/detail-casestudies.php> accessed 15 January 2021

[17] Avnish Bajaj vs. State (N.C.T.) Of Delhi ,2005 Cri LJ 364 (DLT).

[18] http://www.pslaw.in/category-page/110-state-of-tamil-nadu-v-suhas-katti.html

[19] https://www.khaleejtimes.com/article/20110527/ARTICLE/305279912/1028

provisions, including the Immoral Traffic (Prevention) Act of 1956 and the Women (Prohibition) Act of 1986. In light of the gravity of the offence, the doctor was sentenced to life in prison under the Immoral Traffic (Prevention) Act of 1956."[20]

Conclusion:

It is accurately argued that if we want to bring change to our society in response to the current crisis, we must overcome the outmoded model of dealing with the situation and construct a new, efficient, and well-organized one. Cybercrime is a relatively new form of criminal activity that has recently attracted the attention of our legislators and judiciary. Cybercrime is a serious offence that has both physical and mental consequences. Psychological anguish, fear for one's safety, shock and disbelief, anxiety, and nightmares are all possible consequences of cybercrime.Cybercrime has the potential to instill terror in the victim's mind. In most cases, the perpetrator's purpose is to annoy, threaten, or profit economically, like in traditional crime, but now the offender uses a social media platform to carry out this type of crime. Many countries, including India, have legislation dealing with cyber crime. The IT Act, 2000, and the I.P.C deal with this form of crime.

References:

1. Jyoti Ratan, *Cyber Laws & Information Technology* 62 (Bharat Law House, Delhi,6thedn., 2017)
2. Harpreet Singh Dalla& Ms. Geeta, "Cyber Crime – A Threat to Persons, Property, Government and Societies" 3*ARCSSE* (2013).
3. AnimeshSarmah, RoshmiSarmah and AmlanJyotiBaruah, "A brief study on Cyber Crime and Cyber Law's of India" *IRJET*1635 (2017)
4. https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake news-on-social-media-data/article36480525.ece
5. Cyber Stalking: Challenges In Regulating Cyber stalking At The Cyber Space, Aravinth Balakrishnan,http://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyber-space.html
6. Fisher, B.S., F.T. Cullen, and M.G. Turner, "Being pursued: Stalking victimization in a national study of college women", 1 Criminology & Public Policy 259, (2002).
7. DebaratiHalder,"Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Lawsin India from Restorative Justice and Therapeutic Jurisprudential Perspectives",*TEMIDA*107 (2015)
8. Ibid
9. Supra note 5 p.108
10. Supra note 4.
11. Karen L. Paullet, Daniel R. Rota, Thomas T. Swan, "Cyberstalking: An Exploratory Study Of Students At A Mid-Atlantic University" 10 *Issues in Information Systems* 641(2009).
12. What is Cyberstalking, Jatin Sharma, 15 April 2020 https://www.lawyered.in/legal-disrupt/articles/what-is-cyberstalking/
13. Supra, note 4.
14. Ibid.
15. https://www.legalindia.com/tag/ritu-kohli-case/
16. https://www.cyberralegalservices.com/detail-casestudies.php> accessed 15 January 2021
17. Avnish Bajaj vs. State (N.C.T.) Of Delhi ,2005 Cri LJ 364 (DLT).
18. http://www.pslaw.in/category-page/110-state-of-tamil-nadu-v-suhas-katti.html
19. https://www.khaleejtimes.com/article/20110527/ARTICLE/305279912/1028
20. State of Tamil Nadu v.Dr.L.Prakash, 2002Cri LJ 2596 (SC).
21. Kumar, S. (2022). Strategic management of carbon footprint using carbon collectible non-fungible tokens (NFTS) on blockchain. Academy of Strategic Management Journal, 21(S3), 1-10

[20] StateofTamilNaduv.Dr.L.Prakash, 2002CriLJ2596(SC).

22. Kumar, S. (2021). Review of geothermal energy as an alternate energy source for Bitcoin mining. Journal of Economics and Economic Education Research, 23(1), 1-12
23. Dr. Naveen Nandal, Dr. AarushiKataria, Dr. Meenakshi Dhingra. (2020). Measuring Innovation: Challenges and Best Practices. International Journal of Advanced Science and Technology, 29(5s), 1275 - 1285.
24. Nandal, N. Impact of product innovation on the financial performance of the selected organizations: A study in indian context. Psychol. Educ. J. 2021, 58, 5152–5163.