JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER CRIME AND RELEVANT LAWS: A REVIEW

Rishi Gupta
Research Scholar, Law Department
OPJS University, Churu, Rajasthan

Dr. Ravi Tyagi (Guide)
Associate Professor, Law Department
OPJS University, Churu, Rajasthan

ABSTRACT:

At present, the whole world including India has become highly dependent on the world of internet which has become the backbone of the rapidly changing society. Like always, this time too this important change has a very bright face on the one hand and on the other hand those who distort its face are also present all over the world today. Where we are doing the biggest things very easily through the world of the internet, on the other hand in this world of the internet, many people do burglary in different ways to people and big organizations and sometimes even to a country. By trapping even, the government in their net, they are cheating them a lot. Thus, if we see, we find that with the use of the internet all over the world, where we have benefited, on the other hand, many types of crimes have also spread through its use, which we call cyber-crime in the world of internet. know. Today a large population in India is connected to the social network and to further innovate and accelerate it, the dissemination of 5G networking across India has been started from October 1, 2022 by the current Prime Minister Narendra Modi[1]. His government does not want to limit this facility only to the urban areas of India, but is constantly striving to connect the remote rural areas of India with it. Due to the lack of information in this rapidly expanding Internet world in India and being in countries outside the main servers of the Internet, there is a lot of difficulty in getting to the root of the crimes related to it.

This paper is focused on analysis of different cyber-crime and associated securities and its major role in the media and government of India.

KEYWORDS:

Internet, Cyber Crime, 5G, Hackers, Online Security, I.T. Act, 2000.

OBJECTIVES:

The following three main goals have been kept in mind while writing this research paper:

1. To raise awareness about the crimes and illegal activities taking place in the world of internet, especially the scams and frauds done using the internet by creating an understanding and reaching out to them.

2. A meaningful effort to bring awareness about the laws made to bring cyber-crime under control.

3. To make recommendations for preventive measures in addition to cyber laws to protect the users of cyberspace.

INTRODUCTION:

Most of the work in the whole world including India was completed through paper. In 1837, the important invention of computer was done by English mathematician and inventor Charles Babbage[2], whose sophisticated form has had a significant impact in taking the whole world on the path of progress today and which continues to attain new dimensions continuously. Simply put, a computer is a mechanism that procedures info as directed by the user. Currently, information is exchanged between different networks by connecting computers to the Internet. Internet technology is also used for online transactions beyond online transactions. Therefore, its safety is a major concern. Various types of breaches in this security have given rise to 'cyber-crime'. Thus, we can define cyber-crime as crimes committed using computer networks. In simple words, cyber-crimes are crimes that are based on electronic information systems. A cybercriminal uses a variety of devices to access the personal information of others, the privacy of people's businesses and the governments of countries. Selling people's personal data without the consent of their owners is also a type of cyber-crime. Such criminals are called 'hackers' and these crimes are known as electronic crime or e-crime, or cyber-crime or hi-tech crime or digital crime etc.

Currently, cybercrime has seriously harmed people, businesses and governments of several nations and their intelligence agencies all over the world too. Many efforts have been made globally to stop these internet related crimes. For this purpose, the introduction of cyber legislation in India. An attempt to frame cyber laws by clarifying cyberspace cyber-crimes, digital and electronic signatures, data security and privacy, etc., came in the form of the Information Technology (IT) Act, 2000[3] by India. This legislation was adopted in accordance with the UN model.

BUDAPEST CONVENTION:

This is the first international treaty to harmonize the laws of different countries and to detect and combat cybercrime through the internet through technological advancement through mutual cooperation. It was signed on November 23, 2001 in Budapest, the largest city on the banks of the Danube River in Hungary, and presented to various nations for its approval and came into force on July 1, 2004. This convention based on cybercrime is known as 'Budapest Convention[4].'

Article 32B of the Convention allows cross-border access to data and that is why India has not yet signed the treaty for the protection of national sovereignty.

WHAT IS CYBER CRIME:

The first credit for introducing the term 'cyber-crime' was given to Sussman and Heuston in 1995[5]. Cybercrime cannot be limited by any one definition. It has been regarded as a collection of acts and conduct. The offenses under this are based on physical objects and systems that adversely affect computer data or systems.

According to Anderson & Gardner, "Cyber-crimes are 'criminal acts' implemented through the use of computers or other forms of electronic communication."[6]

K. Jaishankar and Debarati Halder additional explain cybercrime from a gender viewpoint and defined “cybercrime against women” as “Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones”.[7]

If we put in humble arguments, the acts declared culpable by the I T Act, 2000 are considered as 'cyber-crimes'. In 2008, the Information Technology Act, 2008[8] was passed by making some amendments in this act. Now it has been given an even wider scope by including areas such as online e-commerce, digital signatures, profitable dealings etc.

Thus, 'cybercrime' is such a malicious crime in which illegal intrusion into the secret information of a person or organization or government and security agencies through the Internet with the help of electronic communication systems, and many tools, earns unethical profit.

CLASSIFICATION OF CYBER CRIME:

1. ONLINE STALKING:

It is one of the crimes that is perpetrated the most frequently in the contemporary world. It entails tracking someone's whereabouts and sneakily chasing them. It entails obtaining information that might be used to threaten or harass a person. Although a cyber stalker doesn't directly threaten a victim physically because they stalk them online, it can be difficult to identify them because of the anonymity of their online activities, consequently this offence is more common than actual stalking.

Children and females who are stalked by males and mature marauders for retaliation, erotic tyranny, and ego are among the main targets of cyber stalking. Because most victims are not familiar with internet usage guidelines and user privacy, cyber stalking has become an increasingly common form of crime. Since cyberstalking is not yet covered by India's existing cyber laws, the person who committed this offense may be charged in IT Act, 72 Sec. for breach of privacy and confidentiality. Sections 441 and 509 of the IPC are also relevant here.

2. INTERNET PORNOGRAPHY:

It poses a serious risk to the safety of women and children since it entails posting or sending pornographic content online that can be promptly replicated on a variety of other technological devices. It alludes to how sexual content is portrayed online.

According to Adv. P. Mali[9], Pornography is any written, visual or audio content that degrades or depicts sexual behavior to one or more of the participants in such a way as to endorse the degradation. It also includes the sexually clear graphics, images or arguments. It does not change how demeaning such behavior is that the victim chose to be hurt, abused, or exposed to duress. About half of all sites on the net include adult content, including nude content, images and photos of females that are harmful to women's integrity.

Anyone who issues and conveys, or reasons to be printed and conveyed in electric format, any content that comprises clearly sexual acts or dealings is guilty of the crime of pornography under Section 67-A of the IT Amendment Act of 2008, which states that. In addition, the Indian Penal Code[10], 1860's Sections 292/293/294, 500/506, and 509 are relevant, and a victim may lodge a complaint close to the police department wherever the lawbreaking was perpetrated or wherever he first learned of the incident. If the offense is proven, the accused may be declared to have received their 1st conviction and face up to 5 years in prison and a mulct of 10 lakh rupees. The maximum sentence for a 2nd conviction is 7 years in prison and a mulct of 10 lakh rupees.

3. CYBER-MORPHING:

It is an illegal act when the real image is altered by an unwarranted operator or someone using a false identity. Female users' photos are copied from their profiles and edited before being uploaded for sexual reasons by bogus accounts on several websites. The users' lack of understanding is what encourages crooks to perpetrate such horrible actions. Sections 43 and 66 of the Information Act of 2000 criminalise cyber-morphing and cyber-obscenity.

4. ONLINE BULLYING:

Cyberbullying is when someone uses the internet to send, upload, or share damaging or misleading content using digital devices such as computers, tablets, laptops, and mobile phones in order to disgrace or humiliate somebody in public. Info can be swapped online and is accessible to many persons through social media platforms, online gaming groups, online forums, and SMS. Being relentless and lasting, cyberbullying has the potential to damage both the victim's and the perpetrators' online reputations.

5. SPOOFING AND IMPERSONATION IN EMAIL:

One of the most frequent cybercrimes is this one. Its beginnings can be seen in the sending of email. Today, this type of crime is so prevalent that it is quite challenging to determine whether e-mail that is got is actually coming from the intended despatcher. Most often, e-mail hoaxing is applied to illegally get private info and secluded photographs from females, which are then applied to extortion them. Research claims that since 2016, 2phishing attacks have increased by 280%. According to Avanan research, around 4% of the emails that a person receives are fake e-mails. In the Guj. Ambuja Ex. Case[11], the fifty-one years old cybercriminal constructed a phony email ID and engaged in a "cyber relationship" with an Abu Dhabi-based businessman in order to extort Rs 96 lakh from him.

Sec. 66-D of the I. T. Amend. Act of 2008 and Sections 465, 417, and 419 of the I. P. C. of 1860 both make email spoofing a crime. With the consent of the court where the prosecution of the offense is pending, it is a cognizable, 2bailable, and compoundable offense that may be tried through any judge.

6. ONLINE HARASSMENT:

It's a kind of on-line ferocity that occurs on communal broadcasting sites where users have the freedom to express themselves. Persons that speak out and believe otherwise from the prevalent society standards are frequently the targets of online harassers. Females who are the targets of cyberbullies are represented in this section. "Women who are vocal online, especially on topics that have traditionally been relegated to 'male expertise' like religion or politics, or about women's experiences, including those of sexuality, menstruation, or speaking out about patriarchy, are subjected to a vicious form of trolling," according to a report by Digital Hifazat[12].

The victims of social media bullying suffer both physical and emotional health effects. The most frequent components of trolling are rebuke, hatred language, and unpleasant remarks. The utmost frequent effects of troll are mental health issues and self-censorship.

SOCIAL MEDIA'S ROLE:

1. The public that often uses social networking sites is not aware of the risks associated with cybercrime. Due to the concentration of social networking companies' servers in other nations, concerns have been raised about the potential exploitation of personal data in these nations.
2. Because people publish their personal information on a variety of social networking sites, hackers can easily break into these accounts and utilise the information they steal.
3. Hackers use social networking sites to defraud individuals online.
4. Security agencies have also discovered that numerous internet currency transfer apps are used to finance terrorists and anti-national elements.
5. Through numerous online games, cybercriminals urge kids to commit crimes.

GOVERNMENT'S ROLE:

1. The Indian government passed the Information Technology Act, 2000 and the I. P. C.
2. The Act's provisions are adequate for fully addressing cybercrimes. Hacking and cybercrimes are covered in sections 43, 43A, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 70, 72, 72A, and 74 of the Information Technology Act 2000.
3. The government established the "National Critical Information Infrastructure Protection Center (NCIIPC)[13]" to protect highly sensitive data as part of the "National Cyber Security Policy, 2013" that it announced.
4. This has a clause that allows for fines or imprisonment for 2 years to life.
5. The government has started the "Information Security Education and Awareness" project to develop human resources in the field of information security at all levels (ISEA)[14].
6. The government established the "Computer Emergency Response Team (CERT-In)[15]," which serves as a national model agency for computer security.
7. The nation has also established a "Cyber Swachhata Kendra[16]" to combat cybercrimes in a coordinated and efficient manner. It is a component of the Ministry of Electronics and Information Technology's Digital India Programme for the Indian government.
8. In order to embrace best practices for information exchange and cyber security, India is working with nations including the US, the UK, and China.
9. The "Indian Cyber Crime Co-ordination Centre- I 4 C" has been established to facilitate interagency coordination.

INDIAN CYBER CRIME COORDINATION CENTRE:

The Ministry of Home Affairs (MHA) launched the Indian Cyber Crime Coordination Centre[17] (I 4 C) in an effort to tackle cybercrime in the nation in a coordinated and efficient way. The plan's term is from 2018 to 2020, and an investment of Rs. 415.86 billion is suggested. India-wide implementation of this Programme. To more effectively combat cybercrime and execute I 4 C, the approach is broken down into seven key components. These 7 elements are as follows:

1. NATIONAL-CYBERCRIME-THREAT-ANALYTICS-UNIT:

It will be accomplished via a NCTAU, which will offer a stage for laws implementation officials, individuals from the commercial subdivision, academic institutions, and investigate groups to collaborate while analysing every piece of the cybercrime jigsaw.

Additionally, the Threat Analytics Unit must organise regular interactions on certain cybercrime-related subjects and generate reports on cybercrime threat information.

Establish a multi-stakeholder framework where law enforcement professionals and business leaders may interact.

2. NATIONAL-CYBERCRIME-REPORTING:

To form expert investigation teams, this unit will collaborate with currently operational investigative components at the national and federal heights along with specialists from many fields.

will be able to react in real time to a threat from cybercrime that is always evolving.

Will be able to work with partners to look into online and online-enabled crime.

3. PLATFORM-FOR-JOINT-CYBERCRIME-INVESTIGATION-TEAM:

The goal of it is to coordinate and lead intellect-led act in contradiction of significant cyber-crime intimidations and goals. It will make it easier to jointly identify, priorities, plan for, and start multijurisdictional countermeasures against cybercrime.

4. NATIONAL-CYBERCRIME-FORENSIC-LABORATORY-ECOSYSTEM:

Owing to modern digital skill and methodologies, cybercrime is now the subject of forensic examination and investigation.

Create a facility to aid the investigating process. For the purpose of examination and investigative efforts to stay up by novel technological breakthroughs, utilising a whole novel type of cyber-crime may possess been perpetrated, NCFL[18] and the related CFSL[19] must be well-furnished and operated.

5. NATIONAL-CYBERCRIME-TRAINING-CENTER:

This will be established with an emphasis on standardising the course curriculum for cybercrimes, impact containment, and investigations, and providing hands-on training in cyber-crime discovery, suppression, and commentary in fake cyber surroundings.

creating a huge exposed connected sequence that will be provided using a cloud-built exercise system. The National-Cybercrime-Training-Center will concentrate on developing a Cyber-Range for enhanced imitation and exercise on cyberattacks and such cybercrimes' examination also.

6. CYBERCRIME-ECOSYSTEM-MANAGEMENT-UNIT:

Create ecosystems that enable academics, business, and government to collaborate in order to study cybercrime, create standard operating procedures, mitigate its effects, and respond to it. Support the development of all ecosystem elements aimed at combating cybercrime.

7. NATIONAL-CYBER RESEARCH-AND-INNOVATION-CENTER:

Keep trace of new technology advances and foresee possible weaknesses that fraudsters may exploit. To make use of the power and knowledge of all participants, whether they are from the academic or business worlds or intergovernmental organisations. Form strategic alliances with all of these organisations to do cutting-edge research and innovation on cybercrimes, impact containment, and investigations.

THE FRAMEWORK OF LAW:

The Internet has two distinctive characteristics. First of all, it is not restricted to a certain area and a cybercriminal can carry out their crime from anywhere in the earth. The 2nd distinctive quality is, this gives its users secrecy, which has benefits and drawbacks of its own. It's a blessing for those who use anonymity to voice their opinions to the world, but it's a curse for those who use anonymity to commit crimes. As a result, these qualities present difficulties for both enforcing the law and preventing crime. There isn't a specific statute dealing with cybercrime against women as of right now. The majority of women are unaware of other laws that may apply in the particular situation. Women are unaware of their rights or even that they exist.

Cybercrime is punishable by a number of laws found in statutes and regulations. The Information Technology Act (IT Act), 2000, and the Indian Penal Code (IPC), however, make up the majority of the laws. The I. P. C. is India's general-criminal-code, which outlines crimes and their associated penalties. IPC, which has been legally modified and wisely construed to apply to cybercriminals, deals with laws and punishments pertaining to the physical world. The IT Act, on the other hand, is a specific code that deals with the usage of technique and crimes done with it. The IT Amendment Act, which includes some offences relating to the internet realm, was passed in 2008. Regarding cybercrime against women, the IT Act and IPC are complementary. the below-listed. Now below details display the regulations that a cybercriminal who harms women can be held accountable for. The gaps in the aforementioned laws are then examined: -

IT ACT 2000 - SECTION 66E:

Under the above section, if a person takes a photo of someone's private parts and publish it, then that one can be punished with imprisonment of up to 3 years or a fine of up to 2 lakhs or both.

IT ACT 2000 - SECTION 67:

As per the above section whoever publishes clear sexual material in electronic form or by means of which appeals to carnal interest or tends to corrupt, shall be punished with imprisonment of either description for a term which may extend to 3 years, and with fine of which may extend to 5 lakhs. Repeated offense can lead to imprisonment up to 5 years and fine up to 10 lakhs.

IT ACT 2000 - SECTION 67A:

Under the above section, if anyone electrically publishes any material related to sexual acts, that one can be imprisoned for up to 5 years and fined up to 10 lakhs. Repeated offense can lead to imprisonment up to 7 years and fine up to 10 lakhs.

IT ACT 2000 - SECTION 67B:

Under the above section, if anyone electrically publishes any material related to depiction of children sexual acts, that one can be imprisoned for up to 5 years and fined up to 10 lakhs. Repeated offense can lead to imprisonment up to 7 years and fine up to 10 lakhs.

IPC 1860 - SECTION 354 A:

Under this section, whoever offers to have sex without desire or solicits grace to have sex or shows a woman with obscene literature against her will, can be imprisoned for up to 3 years or fine or both and if that one makes sexual remarks, then the one can be imprisoned for up to 1 years or fine or both.

IPC 1860 - SECTION 354 C:

Under this section, if anyone takes or disseminates photographs of private time of woman, then the one will be guilty of imprisonment from 1 to 3 years and fine too. If convicted again for the same, imprisonment of 3 to 7 years and fine will have to be given.

IPC 1860 - SECTION 354D:

In this, if anyone follows a woman without any legal reason or keep an eye on her through electronic means, then that one will be guilty of imprisonment up to 3 years and fine. On re-conviction shall be punishable with imprisonment which extend to 5 years and with fine.

IPC 1860 - SECTION 499 & 500:

Whoever will harm the person's reputation by stigma with the intention of harming a person, he can be punished with plain imprisonment or fine or both that can be extended for 2 years.

IPC 1860 - SECTION 507:

Under this section, if anyone makes threats or conceals any such person by means of unknown communication, that one will be guilty of imprisonment up to 2 years.

Although this clause is gender-neutral, women who are threatened by online trolls whose identities are frequently anonymous could use it to their advantage.

IPC 1860 - SECTION 509:

Under this section, whoever intentionally utters or makes any sound or gesture or exhibits any object to insult and interfere with the secrecy of a lady, will be guilty of imprisonment up to 2 years with fine.

Although this clause doesn't specifically include online sexual harassment and abuse, it may be used in those situations.

All of the above important provisions address the provisions relating to online violence against women.

A GAP IN THE CURRENT LEGAL PROVISION:

Online verbal abuse that is not sexual in nature is not adequately addressed. Sections 499 and 507 applies to personal issues, do not apply to general sexist remarks. Furthermore, doxing that doesn't involve the exchange of explicit material or intimidation is excluded. The act of doxing by hacking does not specifically comprise in I. T. Act Sec. 66.

IPC Sections 499 and 507 and IT Act Section 66 regard connected harassment, spoken misuse, and pony-trekking for doxing as private, remote criminalities. The fact that this act of violence is being performed against a woman just because she is a woman must be noted. The abuse of women is based on their sexual orientation and caste, as can be seen from the past.

Violence as physical injury, as opposed to interference with physical honesty and individual self-sufficiency, as definite through the additional provisions of the I. P. C. and I. T. Act is an exemption under IT Act-Sec. 66E and IPC-Sections 354C & 354D. Additionally, these sections only address "physical privacy" rather than "informational privacy." It should be noted that although while Section 509 of the IPC mentions "Privacy," it only does so in relation to ladies' diffidence. Erotic ferocity is mostly seen from the perspective of upholding community politeness by reducing offensiveness and defending ladies' diffidence.

Furthermore, it is evident that it may be revoked at any time. When sexual assault and the urge to control how sexuality is ratified and represented are coupled, gender norms that priorities preserving women's sexuality over their physical integrity or personal information are reinforced. The IT Act's Sections 7214 and 43 when taken along with Section 66-15 constitute an economic offence rather than a social or gender offence.

The law does not recognise gender-based psychological abuse against women outside of the context of the family. The dissemination of peculiar info by a violation of confidentiality that is not sensual in character constitutes psychological harm that has not been acknowledged.

Furthermore, regulations like the 2005 PWDV Act[20], which addresses incidents of psychological abuse in the home and intimate relationships, do not address cybercrime with regard to women.

PROPOSALS:

1. It's a tough to work on net deprived of revealing any individual information; as a result, one should be careful about it on net.
2. One should be careful about fraudulent e-mails and specially for those which request personal information shouldn't be replied to. Email addresses should also be protected.
3. one should be aware about the privacy settings on sites when participating in online activities and to avoid shady websites that are used to steal personal information.
4. The fight against harassment and abuse must be understood as a part of a larger campaign that addresses online offences against women. Since it is essentially a people-centered concern, broader initiatives should be launched.
5. It's important to keep up with the rate of change. The majority of internet crimes occur as a result of consumers' ignorance and lack of understanding, making custody up by technical variations a problem that essentially be resolved.
6. To encourage ladies' management and policymaking in civilization, media, clubs, associations, and women's media networks must work together.
7. Emphatic and masterful connected due diligence, nursing, and broadcasting should be done to combat ferocity and cyber-crime.
8. Women oriented e-portal should run to solve their issues anonymously deprived of having to worry about being stigmatised by calling the police. Additionally, it is important to maintain the criminal database so that law enforcement may use it.
9. There must be an education system by which women can get best knowledge about networks.
10. There must be some educational programs on burning issues about net uses to increase public understanding of net usage.
11. The administration must enact severer regulations on Internet-Service-Providers, as they keep the data that internet users accuse of being misused. Additionally, in order to stop crimes before they start, they should report any suspicious activity.

CONCLUSION:

"The law is not the only way to solve problems." Despite a solid legal foundation and despite their silence, victims still do not receive justice. Cybercrime against women serves as a stark reminder of what actually occurs in the real world. The distinction between the offline and online worlds is fading. Because the offenders believe it to be a much simpler method with less penalties, cybercrime occurs. With millions of users on internet sites, the complaint processes have also lost their effectiveness.

For instance, in the recent incident involving the Delhi-based boy's locker room, a group of adolescent males posted images of underage girls and objectified them by making disparaging comments about them in group chat on Instagram and Snapchat. The group was exposed after a female uploaded screenshot of the discussions. Women spoke up across the nation, but it was clear that they were not startled. The society's acceptance of the objectification of women is the primary cause. As additional incidents of male objectification are revealed daily, women have come to accept this mindset. Years have passed, yet women continue to live in terror of stepping outside on their own in the actual cosmos. In actuality, the internet world, which she could access from the protection of her house, has also become dangerous. Long-term steps must be implemented to address cybercrime against women in order to resolve this issue.

With the advancement of information technology, it is imperative that society and cultural standards change. There must be mandatory actions done. Actions like promoting digital literacy, improving data security, giving women and girls access to technology and most importantly passing laws that expressly address cybercrime, particularly as it relates to women.

REFERENCES:

1. https://teqip.in/jio-5g-launch-date-in-india.html
2. https://en.wikipedia.org/wiki/Charles_Babbage
3. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
4. https://www.coe.int/en/web/cybercrime/the-budapest-convention
5.https://www.intolegalworld.com/article?title=cyber-crime-in-india
6.https://www.researchgate.net/publication/350107577_Cyber_Crimes_and_Cyber_Laws_in_India_An_Overview Cyber Crimes and Cyber Laws in India: An Overview, Pallavi Kapila (Assistant Professor), January 2020
In book: Contemporary Issues and Challenges in the Society (pp.36-48) Edition: 2020
Publisher: New Era International Imprint
7.DEBRATI HALDER & K. JAISHANKAR, CYBER CRIMES AGAINST WOMEN IN INDIA © 2021.
International Journal of Law Management & Humanities
[ISSN 2581-5369]495 [Vol. 4 Iss 2; 493]
8.https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf
9.Adv. Prashant Mali, IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 1
10. https://legislative.gov.in/sites/default/files/A1860-45.pdf
11.Gujarat Abuja's Executive case

Case of Cyber Extortion, INDIA FORENSIC, (Jan 20, 2021), http://www.indiaforensic.com/cyberextortion.htm
12.Trolls Target Women: Dealing with Online Violence, THE CITIZEN, (Jan 21, 2021), https://www.thecitizen.in/index.php/en/NewsDetail/index/7/17330/Trolls-Target-Women-Dealing-with-Online-Violence
13.https://nciipc.gov.in/
14.https://isea.gov.in/
15.https://cert-in.org.in/
16.https://www.csk.gov.in/
17.https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme
18.https://cybersecureindia.in/tag/national-cyber-crime-forensic-laboratory-ncfl/
19.https://cfslhyd.gov.in/
20.https://indiankanoon.org/doc/542601/