IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"Unveiling The Legal Framework: A Comprehensive Analysis Of Cyber Law In The Digital Age"

Shriya Rajput

Law Student (B.com. LL.B)

Amity Law School, Lucknow

ABSTRACT:-

In this research paper, we delve into the realm of cyber law, exploring its crucial role in addressing the challenges posed by cybercrimes. We examine the legal framework established to combat cyber threats and protect individuals, organizations, and society as a whole. Through an inspection of case studies and legislative developments, we explore the methodologies employed in studying cyber law and the enforcement mechanisms used to prosecute offenders.

This research sheds light on the evolving nature of cybercrimes and the difficulty involved in investigating and prosecuting such offenses like cyberbullying. We also discuss the challenges faced by legal systems worldwide in keeping pace with rapidly advancing technology. Additionally, we examine the role of international cooperation and collaboration in combating cyber threats, emphasizing the need for a merged approach.

By understanding the methodologies used in studying cyber law, we gain insights into the legal strategies employed to prevent and mitigate cybercrimes. This research paper aims to contribute to the broader understanding of cyber crime cyber law, and its implications for individuals, businesses, and governments in the digital era."

KEYWORDS: Cyber threats, cybercrime, cyberlaw, cyberbullying, digital era

INTRODUCTION:-

Cyber law is super important in today's digital age. With the rapid advancement of technology and the widespread use of internet been truly remarkable, cyber law plays a crucial role in protecting individual and organization form various threats. It help in safeguard online privacy, ensure our digital transaction and protect intellectual property rights. Cyber law also addresses cybercrime such as hacking, identify theft, and online fraud. Another challenges is the jurisdictional aspect of cyber law. Since the internet knows no boundaries, it can be difficult to determine which law apply in cross border cases. It sets of guideline for

responsible online behavior and help to establish a safe and secure digital environment for everyone. So, it's navigated and protected ourselves in the digital world. India is one of the few countries which has enacted the IT Act 2000 to deal with issues pertaining to cyber-crimes in order to protect the women from exploitation by vicious predators and provide them support so that they can fight back against all wrongdoings. Many institutions have taken up the issues pertaining to cybercrime in order to raise awareness for the safety of women but still a steep increase has been observed in this area, which poses a negative impact on the development of the nation.

WHAT IS THE CYBER LAW ?

Cyber law refers to the legal regulations and protection related to the internet and digital technology. It includes area such as online privacy, intellectual property, cybercrime, and internet governance. These laws are in place to protect individuals and organizations from cyber threats, ensure the security of online transaction and safeguard digital assets. Cyber law helps regulate online behavior, prevent cyber bulling and address problem related to hacking, data breaching, and online fraud. Its's crucial to understand by these law to ensure a safe and secure online environment for everyone.

Cyber law can diversify countries due to differences in legal systems, cultural norms, and technological advancements. Each country may have its own set of laws and regulations to address cyber-related issues. Some countries may have more comprehensive cyber laws that cover a wide range of topics, while others may have less developed or specific laws. Additionally, international cooperation and agreements play a role in addressing cross-border cybercrimes and establishing common standards. It's important to be aware of the specific cyber laws in your country to understand your rights and responsibilities when it comes to online activities.

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

CYBER CRIME:-

Cybercrime is the dark side of the digital era. It encompasses various illegal activities committed using computers and the internet. These include hacking, identity theft, online fraud, spreading malware, phishing, and cyberbullying. Cybercriminals exploit vulnerabilities in systems and networks to gain unauthorized access, steal sensitive information, or cause abuse. They employ sophisticated techniques to deceive and manipulate unsuspecting individuals. To protect ourselves, we must stay vigilant, practice good cybersecurity habits, and be cautious of potential threats. By staying informed and taking necessary precautions, we can navigate the digital landscape cautiously and securely.

To understand cyber law we have to need more focus of the crime which is refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web.

TYPES OF CYBER CRIME :-

1. CYBERSTALKING

   Now days, most popular committed crime is cyberstalking. It is defined as the use of email, direct messaging or other electronic means to harass, scare, or threaten someone with physical harm. And it can come in various forms, such as bullying, sexual harassment, or other unwelcome attention around your life and activities.

   While each cyber stalkers case is different, a look of recent cases reveals that cyber stalkers commonly engage in identity theft and other criminal behaviour. That's because many cyber stalkers use a blend of online and physical harassment and intimidation such as:

   - Tracking someone's online activity or physical location
   - Making death threats or other overt threats of violence.
   - Blackmailing a victim using personal information or photos.
   - Sending threatening doctors photos or deepfakes of the victim or their family.
   - Destroying or manipulation data by sending virus to a victim device.

   Some cyber stalkers use technology to get information such as a physical address and mail threatening physical items to a victim or even show up at their home.

   The offender for committing this offence charged for breach of privacy and confidentiality under section 67 of the IT Act, 2008 (Amendment). Also, section 79 (Word, gesture or act intended to insult modesty of woman) and 329(criminal trespass) of BNS are also applicable for the same.

2. CYBER PORNOGRAPHY

It is an act by using cyberspace to create, display, distribute, import, or publish offensive materials relates to children who are engaged in sexual acts with other.

According to IT Amendment Act 2008 "crime of pornography under section 67-A, whoever publishes and transmits or causes to be a published and transmitted in the electronic form any material which contains sexually explicit act or conduct punishable with imprisonment upto 5 years and fine upto 10 lakhs. Section 329 (criminal trespass) / 295 (Whoever sells, lets to hire, distributes, exhibits or circulates to any child any such obscene object) /296 (obscene act)/356 (criminal defamation) and 351(criminal intimidation) of BNS, 2023 are applicable and victim can file a complaint near the Police Station where the crime has been committed or where he/she came to know about crime.

3. CYBER MORPHING

Morphing is altering or changing the pictures of the person using morphing tools available online. Young girls and women usually fall prey at the hands of the online criminals, who use their photographs posted online and misuse these images by changing the pictures. Due to the lack of awareness among the users the

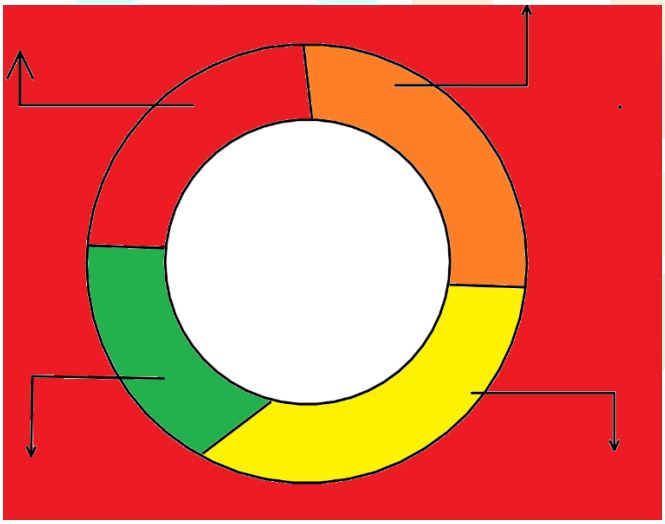
criminals are encouraged to commit such heinous crimes. Cyber morphing or Cyber obscenity is punishable under section 43 and 66 of Information Act 2000.

4. ACCOUNTING FRAUD

Online **fraud** refers to fraudulent activities such as identity theft and financial **fraud** that are committed by using the internet. A fraudulent online transaction in one's bank account, debit or credit card could be because of e-mail spoofing, phishing or it could have been an act committed by cloning one's card. If you a fraud related to net banking or ATM transactions, or any other online transaction happens, you have to raise a complaint.

Victim of Online Banking, then you have legal recourse under the provisions of Section 43 of the Information Technology Act, 2000 which deals with Unauthorised Access along with legal recourse against the Bank under Section 43A of the Information Technology Act for failure to protect your sensitive information and passwords, with claim for compensation upto Rs. 5 Crores.

CYBERSTALKING **ACCOUNTING FRAUD**



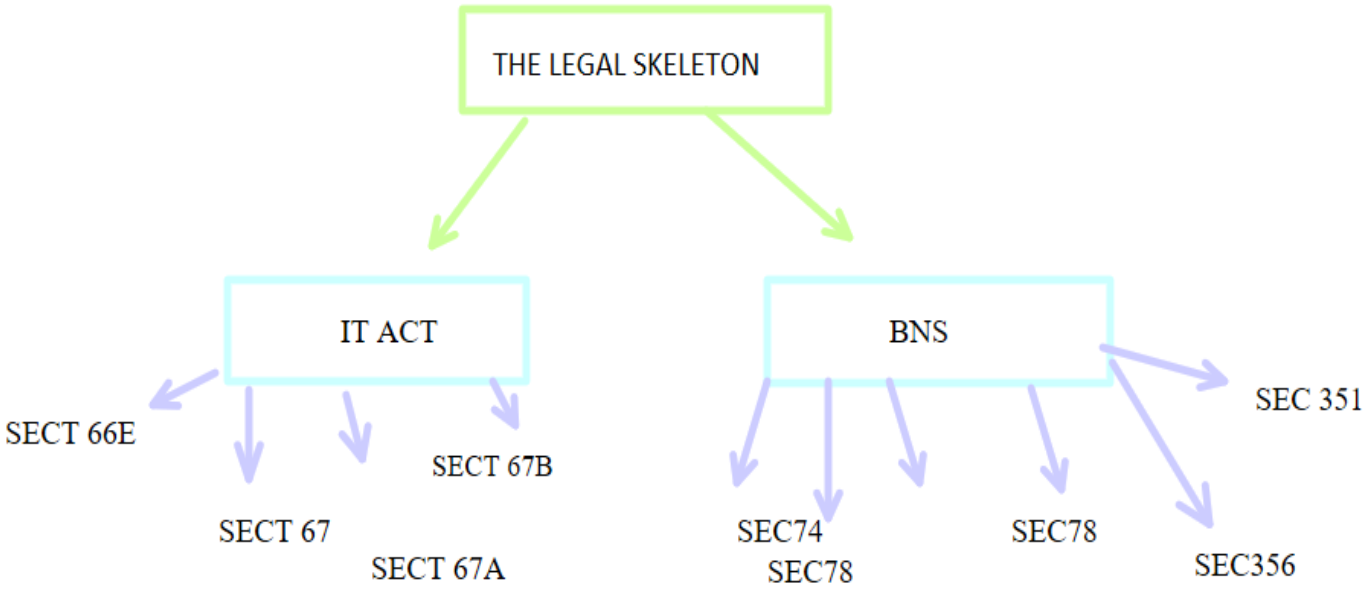
CYBER MORPHING **CYBER PRONOGRAPHY**

THE LEGAL SKELETON:-

There are various illegal activities that take place online, such as hacking, cyber fraud, distributing illegal content, and even organized cybercrime networks. It's important to stay vigilant and protect ourselves from falling victim to these activities. Always remember to practice good online habits, like using strong passwords, being cautious with sharing personal information, and avoiding suspicious websites or links. At present there is some specific law that deals with cyber-crime against women. Other laws which can be used in the specific case, most women are not aware of. Women does not know about their rights or that such rights exist.

There are many laws in statues and regulations which penalises cyber-crime Bharatiya Nyaya Sanhita 2023. But the majority of the laws belong to the and the Information technology Act (IT Act),(Amendment) 2008. These law are general for prescribes punishment for the same.

Both IT Act and BNS are complementary to each other on cyber-crime against women. The below mentioned table analysed the given law of the cyber offences.



Act	Clause	Details of the offence this provision addresses
IT Act	Section 66E	The capture and electronic transmission of images of private parts of a person, without his/her consent.
	Section 67	The publishing or transmission of obscene material in electronic form.
	Section 67A	The publishing or transmission of sexually explicit content in electronic form.
	Section 67B	The electronic publishing or transmission of material in electronic form that depicts children in obscene or indecent or sexually explicit manner.
BNS	Section 75 (3)	Sexual harassment, including by showing pornography against the will of a woman
	Section 74	Voyeurism, including watching or capturing the image of a woman engaging in a private act in circumstances where she would have a reasonable expectation of not being observed; and dissemination of images of a woman engaging in a private act under circumstances where she has agree to the capture of images but not to their dissemination.
	Section 78	Following a woman, contacting/ attempting to contact her to foster personal interaction repeatedly despite a clear indication of disinterest by such woman, or monitoring the use by a woman of the Internet, email, or any other form of electronic communication

	Section 356	Criminal Defamation that leads to reputational harm
	Section 351	Criminal intimidation by anonymous communication
	Section 78	Word, gesture, act or exhibition of an object intended to insult the modesty of a woman.

LATEST CASES:-

1. The Honourable Mr. Justice V. Bharathidasan.
2. Smti. Jyoti Bezbarua Goswami and 2ors.V. The State of Assam and 6 ors.
3. Dr. Biswajit Lenka V. Union of India and Others.

LANDMARK JUDGEMENTS:-

1. Avnish Bajaj vs State, famously known as Bazee.com case (2005)

Avnish Bajaj, the CEO of Bazee.com was arrested under Section 67 of the IT Act for the broadcasting of cyber pornography. Someone else had sold copies of a CD containing pornographic material through the bazee.com website.

2. **K. Ramajayam V. The Inspector Of Police**
   The DVR is an electronic record within in the meaning of Section 2(t) of the Information Technology Act, 2000, as it stores data in electronic form and is also capable of output.

3. **A. Shankar vs State Rep. [2010]**
   The petitioner had secured access unauthorisedly to the protected system of the Legal Advisor.

CONCLUSION:-

In conclusion, cyber law is a analytical aspect of digital world. It obey to protect individual, organization, from the danger and challenges posed by the ever-expanding digital landscape. By establishing regulations and guidelines, cyber law helps safeguard privacy, combat cybercrime, and promote responsible online behaviour. As technology continues to advance, the importance of cyber law will only expand. It is essential for individuals and businesses to stay informed about the newest blossoming in cyber law to ensure a secure and thriving digital environment for all. Let's embrace the opportunities of the digital world while upholding the principles of cyber law.

SUGGESTIONS:-

1. Use strong and unique passwords for all your online accounts.

2. Be cautious while sharing personal information online, especially on social media.

3. Keep your devices and software updated with the latest security patches.

4. Be wary of suspicious emails, messages, or links, and avoid clicking on them.

5. Enable two-factor authentication whenever possible for an extra layer of security.

6. Regularly back up your important data to prevent loss in case of an attack.

7. Install reputable antivirus software and keep it up to date.

8. Be mindful of the websites you visit and only download files from trusted sources.

9. Educate yourself about common online scams and techniques used by cybercriminals.

10. Finally, trust your instincts and if something feels off, it's better to be safe than sorry.

11. The government should make more rigid rules to apply on the Internet Service Providers (ISPs) as they have the entire record of the data that is accuses by the users surfing on the web. Also, in case of any suspicious activities a report should be made by them in order to prevent crimes at an early stage.

Remember, staying informed and practicing good cybersecurity habits can go a long way in protecting yourself from cybercrime. Stay safe and enjoy your time online.

REFERENCE:-

1. Researchgate.net/profile/Shailendra-Giri-3/publication/338986738_Cyber_Crime_Cyber_threat_Cyber_Security_Strategies_and_Cyber_Law_in_Nepal/links/5e36ebc392851c7f7f17a07d/Cyber-Crime-Cyber-threat-Cyber-Security-Strategies-and-Cyber-Law-in-Nepal.pdf
2. Adv. Prashant Mali, *IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 1*
3. https://ijlmh.com/paper/a-study-on-cyber-crime-and-its-legal-framework-in-india/
4. **https://www.bajajfinserv.in/insurance/online-fraud-and-types-of-online-fraud**
5. jstor.org/stable/23249823
6. Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering, August Vol 5, Issue8. [https://www.ijarcsse.com/docs/papers/Volume_5/8_Augu st2015/V5I8-0156.pdf]
7. Slide share.

8. https://infosecawareness.in/cyber-laws-of-india#:~:text=To%20regulate%20such%20activities%20that,attempt%20to%20safeguard%20the%20cyberspace
9. Live law.in