Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 608-620

Evaluation of cybercrime and its punishment: A study of effectiveness of current laws and regulations

[1]Esha Agrawal, [2]Tithi Verma
[1]LLM Student, [2]Assistant Professor
[1,2]Department of Law, Kalinga University Raipur C.G.
[1]eshaagrawal501@gmail.com, [2]tithi.verma@kalingauniversity.ac.in

Abstract: -
With the rise of advanced technology, especially Artificial Intelligence (AI), our dependence on machines is growing rapidly. However, as we rely more on technology, the risk of cyber-crimes also increases. These are crimes carried out using digital platforms and networks, and to deal with them, we have Cyber Laws in place. These laws define the punishments and rules related to online offenses.

India has experienced several cyber-attacks in the past and continues to face such threats even today. Like everything else, technology also has both positive and negative sides. While it brings many benefits, if it falls into the wrong hands, it can cause serious harm to society and humanity. This is why it is important to use technology responsibly and ensure proper legal measures are in place to prevent misuse.As technology becomes an essential part of our daily lives, cyber-crimes have become a major concern for individuals, businesses, and governments. The growing use of digital platforms has led to an increase in the number and complexity of cyber-related offenses. This paper focuses on analyzing different types of cyber-crimes such as hacking, identity theft, online financial fraud, cyber bullying, and data breaches.

Keywords: Cybercrime, Information technology act, Unauthorized access, Cyber-attacks, dark web.

Introduction: -

India has seen significant growth over the past few decades, especially with the rise of globalization and advancements in technology. As more people gained access to computers, smartphones, and the internet, the use of digital tools has become a part of everyday life. However, this rapid digital shift has also led to a rise in cybercrime—criminal activities carried out using the internet. These crimes not only affect individuals and government systems but also pose a threat to society and future generations. Cybercrime is a global issue, with almost no country completely safe from it. To tackle and prevent such digital threats in India, a specific set of laws was introduced, known as the Information Technology Act, 2000. This law provides a framework for handling cyber-related offenses and ensuring digital safety.

Cyber Crime and Cyber Law:-

“Cyber Crime” can be defined as any malefactor or other offences where electronic communications or information systems, including any device or the Internet or both or more of them are Involved.

“Cyber law” cis defined as the legal issues that are related to utilize of communications technology, concretely "cyberspace", i.e. the Internet. It is an endeavor to integrate the challenges presented by human action on the Internet with legacy system of laws applicable to the physical world.

Cyber Crime: -

Sussman and Heuston first proposed the term “Cyber Crime” in the year 1995. Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or conducts. These acts are based on the material offence object that affects the computer data or systems. These are the illegal acts where a digital device or information system is a tool or a target or it can be the combination of both. The cybercrime is also known as electronic crimes, computer-related crimes, e-crime, high technology crime, information age crime etc. In simple term we can describe “Cyber Crime” are the offences or crimes that takes place over electronic communications or information systems. These types of crimes are basically the illegal activities in which a computer and a network are involved. Due of the development of the internet, the volumes of the cybercrime activities are also increasing because when committing a crime there is no longer a need for the physical present of the criminal. The unusual characteristic of cybercrime is that the victim and the offender may never come into direct contact. Cybercriminals often opt to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution.

History of cyber crime :-

History of Cyber Crime The first Cyber Crime was recorded within the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage’s analytical engine is considered as the time of present day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that the new technology cannot be utilized in the future.

Definition of cyber crime :

The ‘Oxford dictionary’ meaning of ‘cyber’ is forming words relates to electronic communication network and virtual reality.

The term “cyber- crime” has not defined in “The Information Technology Act, 2ooo”[1]. ‘cyber-crime’ can be described as crimes committed with the computer or through the computer in cyberspace and may include damaging the computer or the computer networks, committing theft of computer data, computer software, unlawful access to computer data, blackmailing, credit card frauds, stock transfer, electronic fund transfers and e-commerce frauds, hacking by theft of information, passwords, credit card numbers from the internet, giving threats, committing defamation, extortion, intimation, etc. through emails, exposure of pornographic material, illegal gambling, pirated software, stolen data besides cyber stalking and espionage.

Importance of cyber crime :-

Cyber law plays a very important role in this new epoch of technology. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, but each action and each reaction in Cyberspace has some legal and Cyber legal views

Areas of cyber law:

The crucial areas of cyber law include the following:

1) **Intellectual Property:** Cyber law helps protect the ownership rights of creative work online. It ensures that things like music, videos, software, and written content aren't copied or used without permission.
2) **Scams and Frauds**: Cyber laws are used to catch and punish people who commit online scams. These include fake emails, phishing, and other tactics used to trick people into giving away money or personal info.
3) **Data Protection**: With so much personal and customer data stored online, cyber law plays a vital role in keeping that information private and safe. It ensures companies handle data responsibly and securely.
4) **Online Harassment**: Cyber laws address issues like bullying, stalking, or threats that happen over the internet. There are legal rules in place to punish people who harass others online.
5) **Trade Secrets:**Businesses rely on cyber law to keep their sensitive information—like formulas, strategies, or customer lists—safe from being leaked or stolen by competitors or hackers.

Categories of cybercrime:

in general, there are utmost categories of cybercrime:

[1] The Act was enacted by Parliament in the Fifty-first Year of the Republic of India.

1) **Cybercrime against Individuals :** Cybercrime against a person refers to illegal activities carried out online that directly impact an individual's personal life. These crimes can cause emotional, financial, or social harm. Examples include stealing someone's identity to commit fraud, spreading false information to damage someone's reputation (defamation), online scams, or sharing illegal and harmful content like child pornography. These crimes invade a person's privacy and can seriously affect their mental well-being and daily routine.

•**Email spoofing**: This technique is a forgery of an email header. This means that the message appears to have received from someone or somewhere other than the genuine or actual source. These tactics are usually usedin spam campaigns or in phishing, because people are probably going to open an electronic mail or an email when they think that the email has been sent by a legitimate source.

• **Spamming**: Email spam which is otherwise called as junk email. It is unsought mass message sent through email. The uses of spam have become popular in the mid 1990s and it is a problem faced by most email users now a days. Recipient's email addresses are obtained by spam bots, which are automated programs that crawls the internet in search of email addresses. The spammers use spam bots to create email distribution lists. With the expectation of receiving a few number of respond a spammer typically sends an email to millions of email addresses.

•**Cyber defamation**: Cyber defamation means the harm that is brought on the reputation of an individual in the eyes of other individual through the cyber space . The purpose of making defamatory statement is to bring down the reputation of the individual.

Kalandi Charan Lenka vs State of Odisha :[2]

In this case, the victim received indecent texts on her mobile device, followed by offensive messages to her father's phone from an unidentified number. These messages caused significant mental distress to the victim.

Additionally, her character was defamed through written letters sent to her father in 2015 and 2016, containing sexual remarks. Furthermore, a false Facebook account was created in her name, posting modified naked photos, with the intention of offending her modesty.

[2] The Orissa High Court in the case of Kalandi Charan Lenka v. State of Odisha [BLAPL No. 7596 of 2016 decided on16.01.2017] held that ...

Rajiv Dinesh Gadkari vs Smt. Nilangi Rajiv Gadkari :[3]

After the appellant requested a consent divorce, the respondent's wife was harassed with filthy images and text posted on the appellant's website. She filed a defamation case under the IT Act, leading to the offence being recorded against him. The respondent sought restitution of items and maintenance of Rs. 75,000 per month.

The appellant created obscene content for her profiles on various websites, including posting photos taken during her visit to Hawaii Island. She had to alert web hosting companies to remove the content

•**IRC Crime (Internet Relay Chat):**IRC servers allow the people around the world to come together under a single platform which is sometime called as rooms and they chat to each other. ¬Cyber Criminals basically uses it for meeting

¬Hacker uses it for discussing their techniques.

¬Paedophiles use it to allure small children.

A few reasons behind IRC Crime:¬Chat to win ones confidence and later starts to harass sexually, and then blackmail people for ransom, and if the victim denied paying the amount, criminal starts threatening to upload victim's nude photographs or video on the internet.

¬A few are paedophiles, they harass children for their own benefits

. ¬A few uses IRC by offering fake jobs and sometime fake lottery and earns money

2) **Cybercrime against property**: This type of crime targets property, including things like computer networks and electronic devices. It can involve both physical items (like hardware) and non-physical ones (like data or digital content). For example, illegally using someone's copyrighted work or violating intellectual property rights also falls under this kind of crime.

•**Software piracy: It**can be describes as the copying of software unauthorizedly.

•**Copyright infringement:**It can be described as the infringements of an individual or organization's copyright. In simple term it can also be describes as the using of copyright materials unauthorizedly such as music, software, text etc.

[3] AIR 2010 (NOC) 538 (BOM.), 2010 (1) AIR BOM R 45 2010 A I H C 1555, 2010 A I H C 1555, 2010 A I H C 1555 2010 (1) AIR BOM R 45, 2010 (1) AIR BOM R 45

•**Trademark infringement**: It can be described as the using of a service mark or trademark unauthorizedly.

3) **Cyber crime against Organisation:** Cyber Crimes against organization are as follows:

• Unauthorized changing or deleting of data.

• Reading or copying of confidential information unauthorizedly, but the data are neither being change nor deleted.

•**DOS attack**: In this attack, the attacker floods the servers, systems or networks with traffic in order to overwhelm the victim resources and make it infeasible or difficult for the users to use them.

•**Email bombing**: It is a type of Net Abuse, where huge numbers of emails are sent to an email address in order to overflow or flood the mailbox with mails or to flood the server where the email address is.

•**Salami attack:** The other name of Salami attack is Salami slicing. In this attack, the attackers use an online database in order to seize the customer's information like bank details, credit card details etc. Attacker deduces very little amounts from every account over a period of time. In this attack, no complaint is file and the hackers remain free from detection as the clients remain unaware of the slicing. Some other cyber crimes against organization includesLogical bomb, Torjan horse, Data diddling etc.

4) **Cyber Crime against society**: Cyber Crime against society includes-

•**Forgery:** Forgery means making of false document, signature, currency, revenue stamp etc.

•**Web jacking**: The term Web jacking has been derived from hi jacking. In this offence the attacker creates a fake website and when the victim opens the link a new page appears with the message and they need to click another link. If the victim clicks the link that looks real, he will be redirected to a fake page. These types of attacks are done to get entrance or to get access

and controls the site of another. The attacker may also change the information of the victim's webpage.

Stages of cybercrime:

The crime mentioned in the Bharatiya nyaya sanhita (BNS) 2023 involves mainly four stages of the crime i.e. intention,preparation,attempt & commission of crime.According to the several researcher, the commission of cyber crime involves the following stages:

1. Planning/Preparation-In this initial stage, the criminal carefully plans the attack. This involves gathering essential information such as system vulnerabilities, security weaknesses, and details about the server's location. The goal is to understand how to breach the system or bypass security measures.
2. Implementation/Execution-This is the stage where the crime is carried out. The criminal gains unauthorized access to the targeted system to steal sensitive data, alter information, or manipulate existing files, typically for malicious or financial gain.
3. Concealment–After committing the cybercrime, the criminal attempts to cover their tracks. This could involve making the breach appear as a system error or fault, thereby hiding their identity and the crime itself to avoid detection.
4. Conversion-In this final stage, the stolen data is quickly converted into something of value. This might involve selling the information on the black market or using it for personal financial gain, ensuring the criminal profits from the crime before the stolen data becomes obsolete.

Types of cyber crime:

1. Cyberbullying: This involves using the internet, social media, or other digital platforms to harass, threaten, or intimidate someone. It can include hurtful messages, spreading rumors, or online shaming.

2. Phishing: This is a fraudulent attempt where attackers send fake emails that appear to be from legitimate sources. These emails often contain malicious links or attachments designed to steal sensitive information, such as credit card details or passwords.

Case laws :

National Association of Software and Service Companies v. Ajay Sood & Others[4]

In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, (119 (2005) DLT 596) delivered in March, 2005, the Delhi High Court declared `phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages.

This case was one of the leading cases of phishing. Herein an agency head-hunting and recruitment were operated by the defendants. Defendants in NASSCOM'S name sent an email to a third party to obtain personal data for headhunting. Held damages of Rs.16 lakhs were made**.**

[4] National Association of Software and Service Companies v. Ajay Sood & Others 119(2005)DLT596

3. Cyber Defamation: This happens when false or harmful statements are made about someone online, damaging their reputation. It can occur on social media, websites, or in private messaging groups.

4. Cyber Pornography: It is a major threat to women and children security as it involves publishing and transmitting pornographic pictures, photos or writings using the internet which can be reproduced on various other electronic devices instantly. It refers to portrayal of sexual material on the internet.

According to A.P. Mali, "It is the graphic, sexually explicit subordination of women through pictures or words that also includes pornography is verbal or pictorial material which represents or describes sexual behaviour that is degrading or abusive to one or more of participants in such a way as to endorse the degradation. The person has chosen or consented to be harmed, abused, subjected to coercion does not alter the degrading character of such behaviour." Around 50% of the total websites on the internet show pornographic material wherein photos and pictures of women are posted online that are dangerous to women's integrity.

5. Cyber Threatening: in this type of crime, individuals are sent threatening emails or messages with demands or warnings, often to manipulate the victim into taking certain actions.

6. Email Bombing: This involves sending an overwhelming number of emails to a person or organization, typically with the goal of crashing their email system or causing a network failure.

Importance of cyber crime:-We are living in profoundly digitalized world. All organizations rely on their PC systems and keep their significant information in electronic structure. Government structures including personal assessment forms, organization law structures and so forth are presently filled in electronic structure. Consumers are progressively utilizing charge cards for shopping. Most people are using email, cell phones and SMS messages for correspondence. Even in "non-digital wrongdoing" cases, significant proof is found in PCs/mobile phones for example in instances of separation, murder, seizing, sorted out wrongdoing, fear-based oppressor tasks and so forth. Since it contacts every one of the parts of exchanges and exercises on and concerning the web, the World Wide Web and the Internet along these lines Cyber law is critical.

Law Against Cyber Crime And Cyber Criminals :-

- Hacking - Law applicable under Information Technology (Amendment) Act, 2008, Section 43(a)[5]

[5] Compensation for failure to protect data

• According to Information Technology Act, 2000, data theft criminal punished under Section 43 (b)[6]

• Identity theft comes under Information Technology (Amendment) Act, 2008, crime of identity theft under Section 66-C

• Email Spoofing tricks used by Hacker for hacking and it is a cyber crime under IT Act 2008, Section 43(a)

• Child pornography is a cyber crime which is prevented under Child Pornography Prevention Act of 1996 (CPPA)

• Prior to February 2013, there were no laws that directly regulate cyber stalking in India..

Cyber Crime's scenario in India(A Few Case study) :

1) **AIIMS Cyber Attack:-**In 2022 The All-India Institute of Medical Sciences, Delhi faced an attack on its server in November, 2022. The attack took place due to improper network segmentation and it was estimated that terabytes of data was stolen along with the details of 3-4 crore patients including details of high-profile politicians. A case of extortion and cyber terrorism was registered and it was found that the hackers were from China.
2) **Cyber-attack on Cosmos Bank:-**

In the year 2018, a bank in Pune knowns as The Cosmos Cooperative Bank Ltd. had faced a cyber-attack in which a sum of Rs. 94 crore was drawn off the bank. The hackers stole the details of various account holders and drew money from the ATM machines. The crime was not limited to one country but around 28 countries from where the hacker group wiped off the money. Also, some amount of money was transferred through SWIFT in a bank account in Hong Kong.

3) **State of Tamil Nadu vs. Suhas Katti :-**

This case was related to posting of obscene and defamatory message about a divorced woman in a Yahoo message group. The accused also used a fake email account for the purpose of forwarding emails in the name of the victim which resulted in annoying phone calls to the victim in the belief that she was soliciting. The accused person was arrested by the police after making complaint in February, 2004 by the victim. This case is considered to be the first case of Tamil Nadu in which the offender was offender was convicted under Section 469 & 509 IPC and Section 67 of Information Technology Act, 2000. It is one of the landmark cases related to cyber-crime management in India.

4) **Parliament attackcase :-**

The Bureau of Police Research and Development, Hyderabad had handled this case. A laptop was recovered from the terrorist who attacked the Parliament. The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament

[6] Penalties and compensation for data theaft

was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir. However careful detection proved that it was all forged and made on the laptop.

The legal framework :

There are two unique features of the Internet. Firstly, it is not confined to a particular boundary and the cyber-criminal can commit a crime from ay part of the world. The second unique feature is that it provide anonymity to its users which has its own boon and bane. For people who use this anonymity for putting out their opinion to the world it's a boon but the perpetrators who use this anonymity for commission of crime it is a bane. Therefore this features not only pose a challenge in crime prevention but also in the implementation of law. At present there is no 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. But the majority of the laws belong to the Bharatiya nyaya sanhita 2023 and the Information technology Act (IT Act), 2000. The BNS is the general criminal code of India which defines offences and prescribes punishment for the same. BNS covers laws and punishment pertaining to physical world and has been legislatively amended and judiciously interpreted to be applicable to cyber criminals. Whereas the IT Act is a specific code pertaining to use of information technology and crime committed through it. In 2008 IT Amendment Act was enacted inclusive of certain crimes related to cyber world. Both IT Act and BNS are complementary to each other on cyber-crime against women. The below mentioned table is taken from a discussion paper published by IT for Change it showcases the laws that a cyber-criminal can be charged with when he/she commits a crime against women. Following which the loopholes in the said laws is analysed.

Act	**Clause**	**Details of the offence this provision addresses**	**What forms of online VAW can this provision help in challenging?**
IT Act	Section 66E	The capture and electronic transmission of images of private parts of a person, without his/her consent.	– Non-consensual circulation and malicious distribution of sexually explicit photographic and video material about an individual.
	Section 67	The publishing or transmission of obscene material in electronic form.	– Graphic sexual abuse on social media and blog platforms, including trolling. – Sending emails/social media messages with sexually explicit content and images to an individual, against his/her will.
	Section 67A	The publishing or transmission of sexually explicit content in electronic form.	– Graphic sexual abuse on social media and blog platforms, including trolling. – Sending emails/social media messages with sexually explicit content and images to an individual, against his/her will.
	Section 67B	The electronic publishing or transmission of material in electronic form that depicts children in obscene or indecent or sexually explicit manner.	– Circulation of child pornography
BNS	Section 75	Sexual harassment, including by showing pornography against the will of a woman	– Graphic sexual abuse on social media and blog platforms, including trolling. – Sending video and pictures with sexually explicit content and images to a woman, against her will.
	Section 77	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.	– Non-consensual production, circulation and malicious distribution of sexually explicit photographic and video material about a woman.

	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	– Cyber-stalking. Only women are recognized as potential victims by the law.
	Section 356	Criminal Defamation that leads to reputational harm	-Though this is a gender neutral provision, it could be invoked by women bloggers and women on social media fighting slander and libel.
	Section 351 (4)	Criminal intimidation by anonymous communication	– Though this is a gender neutral provision, it could be invoked by women fighting trolls issuing threats, whose identities are often anonymous.
	Section 79	Word, gesture, act or exhibition of an object intended to insult the modesty of a woman.	– Though this provision does not explicitly address online sexual harassment and abuse, it could be invoked in such cases.

CONCLUSION: -

"The law is not the be-all and end-all solution." Victims are still not getting justice despite of a strong legal base in spite of them remaining silent. Cyber-crime against women is just a reality check of what really is going on in the real world. The lines between the online and offline world is getting blurred. Cyber-crime happens because the criminals think that is a much easier way with less punishment. With millions of users in the online platforms complaint mechanisms has also become fruitless.

For instance in the recent boy's locker room case where group of teenage boys from Delhi shared pictures of underage women and objectified them by passing derogatory comments on group chat in Instagram and Snapchat. When a girl shared the screenshots of the chats the group was busted. Women all over country raised voices but it could be seen that they were not shocked. The reason is that objectification of women has become quite normal in the society. Women have has accepted this mentality of objectification by male as every day new cases come into light. Years have passed and still women lives in the fear of going out alone outside in the real world. In fact the online world which she could go to in the safety of her home has also become an unsafe place.

It comes upon the women to take preventive measures such as usage of data security, not leaving digital footprint, keeping everything password protected. But this are all superficial ways. The major problem that has always been existing is the patriarchy and misogyny in the society. To solve this problem a long term measure need to be undertaken that will help in dealing with cyber-crime against women.

There is the need of the hour to evolve the societal and cultural norms with the development of information technology. Mandatory steps need to be taken. Steps like digital literacy, development of data security, providing access of technology to women and girls and most of all enactment of laws specifically on cyber-crime especially with reference to women.