ISSN No:-2456-2165

A Study on Cybercrime Against Women: Special Reference to Dibrugarh University

Lakshmipriya Dutta
Dibrugarh University, Dibrugarh, Assam

Abstract:- Women's rights can be realized more effectively in cyberspace, from accessing information to freely and anonymously expressing themselves. However, cybercrime is a global phenomenon, and women are particularly vulnerable to this new type of crime. The vulnerability and safety of women are two of the most important concerns of any criminal or penal law, but women are still defenseless in cyberspace. Cyber-Crime against women is at an all-time high, and it may pose a serious threat to a person's overall security. The World Wide Web enables users to share information in the form of text, images, videos, and sounds. The widespread distribution of such content is especially harmful to women. There have been numerous reports in recent years of women receiving unsolicited emails containing obscene and obnoxious language. Women have been severely victimized in cyberspace, and cybercrime against women is on the rise. Some perpetrators attempt to defame women by sending obscene emails, stalking women through chat rooms, websites, and other means, creating pornographic videos in which women are depicted in compromising positions, often without their consent, spoofing emails, morphing images for pornographic content, and so on. Sex offenders look for their victims on social networking sites as well as job or marriage websites, where people post their personal information for better prospects. Women have become more vulnerable to cybercrime as a result of the disclosure of personal information. It is clear that female victimization leads to cybercrime and vice versa.

I. INTRODUCTION

Social media is an online social interaction platform. It is a platform that allows information sharing. Nowadays, everyone uses social media. It has become an essential component of our daily lives. However, social media use can have a detrimental impact on teenagers by distracting them, disturbing their sleep, and exposing them to bullying, rumor spreading, false views of other people's lives, and peer pressure. The dangers could be linked to how much social media kids use. More time spent on social media can lead to cyberbullying, social anxiety, depression, and exposure to inappropriate content. Social media may be addictive. When you play a game or do a chore, you strive to do it as well as possible. Instagram use increases the probability of women developing body image issues due to unrealistic or photoshopped content generated by influencers they follow or peers. Long-term Instagram use among women is linked to lower body satisfaction. Worse, social media puts young women under psychological pressure to conform to unrealistic norms in order to be socially acceptable, which leads to significant fears and body image concerns that undermine their self-worth. Many studies have found that women are more susceptible to body image promotion on social media. When women see photographs of celebrities or peers, they either take harmful actions to get such bodies or become nervous and despondent. Despite India's significant increase in internet users, there is a growing gender disparity among social networking site users, as evidenced by the total number of web users, the ratio of Facebook and Twitter users, their level of electronic literacy, and political tweets *(Chen, 2018).* Worse, women account for 29 percent of internet users in India, in accordance with a study carried out by Boston Consulting Group and the Retailers Association of India. The remaining 71% are men. One of the primary factors contributing to this predicament is men's and women's unequal access to the internet. In recent years, there has been an increase in the number of cybercrimes committed against women, which has mirrored this trend. Women are occasionally accused of "invading" or "trespassing" on men's turf, particularly when they express their opinions on difficult issues. This perception is especially prevalent when female users express their opinions on social media platforms. This notion is especially prevalent when female users are engaging in conversations about sensitive subjects. According to a report that was produced by the Observer Research Foundation in 2015 and distributed in 2015, there is a substantial lack of women's participation in the political debates that take place on Twitter in India.

II. CHALLENGES FACED BY WOMEN ON SOCIAL MEDIA

A. Some Major Cyber Crime Against Women

Due to harassment, some of the most well-known cyber crimes have caused thousands of women to suffer from despair, hypertension, and anxiety. The following are examples of major cybercrimes:

- *Cyberstalking:*

Women are the most often targets of online stalking. Cyberstalking is a method of stalking someone through the Internet for online harassment and abuse. A cyberstalker does not directly threaten a victim physically, but rather observes the target's online behavior to acquire information and make threats in various forms of verbal intimidation. Cyberstalking is more common among women who are pursued by men. There is no agreed-upon definition of

internet stalking. It entails tracking a person's Women are more prone to cyberbullying and internet intimidation.

- Women's increased visibility on social media often makes them the subject of oppressive operations. As a result, women face gendered hurdles both online and in public.
- Because of the challenges involved in identifying perpetrators and the complicated and limited access to justice delivery procedures, online offenses are frequently normalized. The public becomes distrustful of the court system as a result, further marginalizing women.
- In this scenario, social media is being exploited by rapists to persuade their victims into not reporting the crime. Harassers use these spaces to put down women who seek to challenge patriarchal social norms.
- According to one research, one-third of the women polled stopped expressing their opinions online owing to the apprehension of being abused *(Noelle-Neumann 1984).*
- Trolling has now expanded throughout the digital domain, resulting in instances such as suicides.
- According to an international poll, 20% of women who have been harassed offline experience the attacks are related to the online abuse they get *(Shanahan,1997)*
- Some people are stalked as a result of their online presence. This is especially prominent in countries with lax law enforcement, patriarchy, and widespread internet trolling.
- Counterfeit accounts are frequently made in order to negatively impact the reputations of perpetrators.
- With the epidemic's global restrictions forcing more people online, cases involving online sex discrimination have risen dramatically.

The majority of the disadvantages of networking sites that are particular to women are connected to body image concerns or experiences of social isolation. The following are some of the most significant disadvantages of social networking sites for women:

Women of younger ages, in particular, are more likely to attempt (unsuccessfully) to cope with difficult emotions or pre-existing mental health disorders by posting humorous material or perusing pseudo-mental health pages rather than seeking professional help.

Instagram use raises the risk of women having body image disorders due to unrealistic or manipulated material generated by celebrities they follow or their peers. Women who use Instagram for an extended period of time have lower body satisfaction.

Women with darker skin tones may be pushed towards skin-whitening remedies as a result of tailored marketing, while women with lighter skin tones may be persuaded by similar procedures to seek out possibly harmful tanning solutions that raise their risk of cancer.

Despite the fact that users often seek to interact with others, regular social media usage is likely to worsen symptoms of social isolation among women. According to Backe et al. (2018), over 900 participants aged 26-35 (about 75% of whom were women) reported greater feelings of loneliness as well as indicators of smartphone addiction.

Cybercrime includes acts such as stealing information from businesses and robbing bank accounts. Computer crime, often known as cybercrime, is defined as any crime that includes a computing device and a network. The computer might have been used to commit a crime, or it could be the target. Cybercrimes are offenses committed against people or groups of individuals with an illegal motive in order to intentionally harm the victim's reputation or cause physical or mental harm or loss to the victim, either directly or indirectly, through the use of current communication technologies, including internet messages, emails, notice boards and groups, and mobile phones. Such crimes may threaten a nation's security and financial health. The issues surrounding these sorts of crimes, notably those involving hacking, copyright infringement, child pornography, and child grooming, have gained prominence. There are additional privacy concerns when sensitive material is intercepted or disseminated, whether legally or illegally. Cyberwarfare refers to activity that crosses international borders and involves the interests of at least one nation state. Through the International Criminal Court, the international legal system seeks to hold actors accountable for their conduct.

In general, cybercrime is defined as "any unlawful act committed or facilitated by the use of a computer, communication device, or computer network in order to facilitate the committing of crime."*(Taylor,1982)*

Nowadays, cybercrime against women is a very familiar issue. Each second, a woman in India becomes a victim of cybercrime, and online platforms are now the new venue where a woman's privacy, dignity, and security are increasingly being challenged. Some criminals use technology to harm women by sending obscene emails, WhatsApp messages, stalking women using websites, chat rooms, and, worst of all, developing pornographic videos, most of which are created without their permission, spoofing emails, and morphing images for pornographic content using different programs available online.

Internet travels by posting messages (often threatening) on bulletin boards frequented by the victim, accessing chat rooms frequented by the victim, persistently bombarding the victim with emails, and so on. In general, the stalker's contacts are intended to inflict emotional pain and serve no legitimate purpose. He does not need to leave his house to find or harass his victim, and he has no fear of physical violence since he feels he cannot be physically touched in cyberspace. Thus, the batterers place their target under continual monitoring without her knowledge and utilize the information to threaten or discredit her by posting false material on the internet. Typically, a cyber stalker's target is

ISSN No:-2456-2165

new to the internet and unfamiliar with netiquette and online safety.

➢ *Harassment Through Emails:*

E-mail harassment is not a new notion. It is extremely similar to letter harassment. Harassment involves blackmail, threats, bullying, and even electronic infidelity. E-harassment is similar to letter harassment; however, it often causes problems when submitted from a fake ID. The emergence of e-mail as the main mode of communication has raised a number of difficulties that politicians and companies alike are concerned about. Because of the simplicity with which email is prepared and sent, individuals are not as careful with the email as they would have been if they had committed the contents of the email to paper. Harassment through email involves blackmailing, threatening and repeated sending of love letters in unknown identities, or sending humiliating emails on a daily basis. Email may accomplish all of the duties of traditional mail (or "snail mail," as it has been nicknamed.)

➢ *Defamation:*

Libel and defamation are both examples of cyberdefamation. It is publishing defamatory material about a person on a web page or disseminating it throughout the victims' social and acquaintance circles or organizations, which is a simple way to damage a woman's reputation by causing her severe mental agony and grief. Cyber defamation, often known as cyber smearing, is defined as the intentional violation of 'another person's right to his good reputation.' Cyber Defamation takes place through the use of computers or the Internet. Because of its speed, it is regarded as a greater threat. A defamatory item might be easily transmitted to a large number of people. Much later, once the harm has been assessed, actual proof of the magnitude of the offense emerges. A single false rumor circulated on the internet has the potential to trigger an unexpected and extraordinary shift in the value of the victim in the eyes of the general public. Women are particularly affected, as the Indian socio economic framework places a premium on women's modesty, reputation, and social position. People may express themselves almost too easily on the internet. The internet has plenty of intriguing places where someone may write a potentially derogatory comment or message, either purposefully or unintentionally. Public remarks on websites; blogs and comments to blog posts; social media such as Facebook, LinkedIn, and Twitter; chat rooms or list servers, and e-mail carrying libelous material to all of the person's friends are just a few examples. While some websites screen submissions for inflammatory or unlawful content, the screening algorithms are not designed to evaluate every post for derogatory information, resulting in a large number of defamatory remarks being published online.

➢ *E- Mail Spoofing:*

It often refers to an email that originates from one source but was sent from another. It has the potential to do monetary harm. Email spoofing is a method used in spam and phishing campaigns to deceive people into believing a communication came from someone or something they know or can trust. The sender of emails forges email headers in spoofing attacks so that client software shows the false source address, which most users accept at face value. It's a word used to describe fraudulent email activity in which the sender address and other portions of the email header are changed to make it look as though the email came from somewhere else. Unintentional users might make the email appear to be from someone other than the real sender by modifying some email attributes such as the From, Return-Path, and Reply-To fields. Email spoofing is feasible because the major protocol used to transmit email, Simple Mail Transfer Protocol (SMTP), does not include an authentication mechanism. Despite the fact that an SMTP service extension enables an SMTP client to negotiate a security level with a mail server, this precaution is not usually followed.

➢ *Phishing:*

Phishing is the effort to get sensitive data, such as a login and password, with the purpose of obtaining personal information. Phishing is the practice of sending fake messages that appear to be from a genuine source. It is a tactic used by cyber thieves to dupe email recipients into believing that the message is a way to get information such as usernames, passwords, PINs, bank account data, and credit card data by posing as a trustworthy business via email. Phishing is often carried out through e-mail or instant messaging spoofing, and it frequently urges people to submit information on a bogus website that looks and feels almost identical to the authentic one. Phishing is a type of social engineering method that is used to deceive consumers. Women are increasingly becoming victims of phishing attempts, posing a serious danger to a person's overall security. Here are a few examples of how it might happen. Phishers frequently utilize a variety of ways to target women. They may try to convince you by sending an email with an enticing subject line. Offers or rewards earned in fake competitions such as lotteries or contests by businesses giving a winning voucher are examples of common phishing approaches. Let's look at a few ways they may use phishing emails to target women.

➢ *Morphing:*

Morphing is the process of altering an original image by an unauthorized user or creating a false identity. Female photographs were discovered to have been obtained by fraudulent users and then re-posted/uploaded on other websites by creating fake profiles after modifying them. Morphing is the process of modifying or changing images of people using online morphing software. Teenage girls and women are frequently victims of cyber fraudsters who use their photographs uploaded online and misappropriate them by modifying the images. Perpetrators then use the changed images to blackmail you, create a fake online profile, engage in sexting, sex chats, pornographic content, take naked photographs, and so on. Morphing can harm your online image and create mental anguish; you may face threats from abusers and become a victim of their blackmailing efforts.

- *Trolling:*

Trolls start quarreling with or upsetting victims by publishing provocative or off-topic statements in an online group with the purpose of provoking victims into an emotional, distressing response. Trolls are professional abusers who, by establishing and utilizing false identities on social media, create a cold war environment in cyberspace and are difficult to track down. Trolling has a significant mental, emotional, and physical impact on its targets. Trolling may be used to divert attention away from more serious topics. Trolls are also employed to influence and impose strict cultural and social traditions and rules that may or may not be legally binding. It may potentially result in offline action. Trolls are typically hired to use deceptive tactics to publish offensive information on the internet. This approach generates social media trends, such as Twitter trends, by employing hashtags against individuals or organizations. Trolling victims may seek remedies under statutes relating to criminal intimidation, sexual harassment, defamation, voyeurism, internet stalking, and obscene content. Seeking legal remedies, on the other hand, places the responsibility on the target.Trolling and bullying are not defined under the Indian Penal Code of 1860. Various elements of the Code, when read in conjunction with the Information Technology Act of 2000 ("IT Act"), can, nevertheless, be utilized to combat cyberbullies and trolls.

- *Cyber Pornography:*

The other concern to female netizens is cyber pornography. This includes pornographic websites and pornographic periodicals created with computers and the internet. The publication, transmission, and causing to be communicated and published in electronic form of any content involving sexually explicit acts or conduct is punished under Section 67 of the Information Technology Act. This implies that accessing cyber pornography is not prohibited in India. Simply downloading, watching, and keeping such content is not an offense. However, it is illegal to publish and send cyber pornography via instant messaging, emails, or any other kind of digital communication. Online pornography, in my opinion, should be fully prohibited since it is responsible for falling morals and sexual permissiveness, which leads to sex crimes against women and children. Many of these pornographic websites portray women and children as sex objects, denigrating their position and portraying them as passive beneficiaries of degrading and/or violent acts, leading to unrealistic and false expectations and different types of physical, mental, and sexual abuse. These false and artificial representations frequently put victims under pressure to do or consent to behaviors that they find degrading, with significant mental and psychological health results and repercussions. Cyber pornography is mainly defined under sections 66 A, E, 67, 67A, and 67 B. All pornography related offenses are bailable as per Section 77B of the Information Technology Act, 2000, with the only exception being Sections 67A and 67B. This is the fundamental reason why criminals commit pornographic offenses and have the guts to repeat them, because they are allowed bail by law, not to mention the lengthy trial time. These provisions of the Act should be rendered non-bailable in order to instill fear in criminals; this would undoubtedly cut crime rates to some extent.

III. LITERATURE REVIEW

The growth of information and communication technologies (ICT) and social networking sites has contributed to economic and social development *(Al-Jenaibi, 2016; Backe et al., 2018; van der Gaag, 2010)*. The number of social network users in India has increased drastically, from 181.7 million in 2015 to 216.5 million in 2016 and a projected 250.8 million in 2017. Indian social network users have grown significantly over the past few years. Social media has become a natural extension of the Indian way of life for the country's citizens. Yet as the Internet and ICTs intersect with social life, it creates a space for strangers and intimate partners to commit a range of gender-based crimes online *(Backe et al., 2018; Jane, 2014a; Jane, 2014b; Vitis & Gilmour, 2017)*. While India's internet population may be exploding, there is a looming gender imbalance among social network users. This is visible in areas such as the number of internet users, the number of Facebook and Twitter users, digital literacy, and political tweets. The use of new technologies, such as smartphones, social networking sites (Facebook, Twitter, and Instagram), and personal blogs, is ubiquitous in contemporary life. Cyber violence is defined as the perpetration of gender-based harm and abuse by strangers and intimate partners through digital and technological means *(Backe et al., 2018)*.

As such, it has several manifestations, which will be considered in this study: gender-based hate speech, also referred to as e-bile *(sexually abusive discourse online; Jane, 2014a; Jane, 2014b; Vitis & Gilmour, 2017)*, image-based abuse *(non-consensual creation and distribution of images; McGlynn & Rackley, 2017; Powell et al., 2018)*; and non-consensual sexting *(BluettBoyd et al., 2013; Powell, 2010; Powell & Henry, 2017; Woodlock, 2014; Barak, 2005)*

The use of new technologies, such as smartphones, social networking sites (Facebook, Twitter, and Instagram), and personal blogs, is ubiquitous in contemporary life. The Internet has been described as a democratic space, in the sense of Habermas' "public sphere," where everyone has access and the freedom to express their ideas and opinions (Beck & Beck-Gernsheim, 2002; Castells, 2010; Giddens, 1992; Kaur et al., 2016). The use of these new technologies is expanding and has been recorded as being highest among 18–34-year-olds in 2019 (Datareportal, 2019). Some sociologists suggest that ICTs represent a space to construct identities outside the social constraints of social structures (Beck & Beck-Gernsheim, 2002; Oksman & Turtainen, 2004). Assumptions about the Internet being a democratic space can obscure the impact of unequal gender relations in cyberspace *(Faulkner, 2001; Henry & Powell, 2015)*. Inclusive participation could be affected by the political economy of the Internet *(Fuchs, 2017)*. There is a huge asymmetry in the visual representation of content *(Fraser, 2004)*. For instance, analysis of the most-viewed YouTube

videos indicates that corporate videos, which have other means of distribution, get more visibility as compared to independent content providers. It shows that pre-existing social, political, and economic inequalities have an impact on the ability of people to participate in online cultures and the way that participation is realized. *(Sarkar et al., 2021 https://doi.org/10.1177/0973258621992273)*

The study's investigation seeks to determine the most prevalent types of social media cyber crime against women, including internet harassment, taunting, coercion, threats or intimidation, impersonation, and the distribution of photographs and videos of women performing individual actions. It focuses particularly on how it influences women's daily lives in modern society. The number of Indians using social networks has increased dramatically in recent years. Due to the country's broad availability of internet access, India's population of social media users increased gradually, reaching 467 million in 2022. The use of social media in Indians' everyday online lives has become indispensable. Among the more well-known social networking platforms in India are Facebook (meta), Twitter, LinkedIn, Instagram, WhatsApp, YouTube, and Skype. According to the National Crime Records Bureau, an agency of the Indian government, 5752 people were arrested in 2014 as a result of 9622 recorded incidents of cybercrime in India. Technological innovation and the internet are mostly used in cybercrimes to carry out illicit actions that are forbidden and penalized under domestic criminal law. This article focuses on cyberattacks against women, although they can also be perpetrated against people, property, and the government. Cyberstalking, cyberpornography, sharing images and videos of women performing sexual activities, morphing, sending offensive or annoying messages, online bullying, blackmailing, threatening, or intimidating behavior, and identity fraud and impersonation are among the more prevalent and frequently reported types of cyber crimes against women.

The survivor faces an unseen mental, physical, and sexual health hazard as a result of cyber assault *(Backe et al., 2018; Kaye, 2017)*. It influences the psychological, social, and cultural components of an individual's identity *(Khanlou et al., 2018; Pashang et al., 2018)*. Anxiety and other trauma-related consequences might also be a result of cyberattacks *(Haynie et al., 2013)*. Several academics believe that different types of cyber violence can have both short- and long-term harmful effects on an individual's psychological state, physical condition (such as weight loss), and cultural and social involvement *(such as experiences of shame and ostracization; Button & Miller, 2013; Gillett, 2018; Madkour et al., 2014)*. There may be shame and embarrassment for women who are sexually abused online *(Bates, 2017)*. Because of their anxiety, victims of cyberbullying may choose to withdraw from online communities, which in certain situations may result in self-harm *(Van Laer, 2013; Vitak et al., 2017)*. Internet sexual harassment can also have financial consequences. For instance, a person's internet past may be used by future employers to deny them employment *(Citron, 2014)*.

There is a dearth of studies on various forms of gender-based sexual assault in the Global South compared to the Global North *(Bates, 2017; Citron & Franks, 2014; Dragiewicz et al., 2019)*. Most research in the Global South examines the magnitude and frequency of specific forms of cyberviolence such as offensive language, revenge porn, stalking, and harassment *(see, for example, Halder & Jaishankar, 2015, Jaishankar, 2019; Mirchandani, 2018)*. A subsystem of fear, shame, and self-censorship may develop as a result of the variety of psychological, social, and economic effects that cyberviolence has on women, maintaining and sustaining male supremacy and patriarchy. There are, however, surprisingly few studies that explore the experiences of cyberviolence in the Global South. In order to guarantee that experiences of violence are not isolated from the cultural and social context, this research intends to close this gap by examining women's experiences of cyberviolence in India. *(Bhat et al.,2022 https://doi.org/10.55529/jipirs.21.18.22)*

As of June 2016, the United Nations Human Rights Council declared the right to use the internet a human right. But what are the implications in a patriarchal society where cyber-violence, harassment, and discrimination against women mirror those in the real world? While the Union Ministry of Women and Child Development has formally announced the magnitude of cybercrime against women and the need for a concerted effort to address it, this study investigated the ground realities of the existence and effectiveness of Indian laws in protecting women (and girls) and allowing a secure and pleasant environment for them when they access the internet. The paper identifies common types of cybercrime against women, including cyber stalking, cyber pornography, circulating images or video clips of women engaged in intimate acts, morphing, sending defamatory or annoying messages, online trolling, bullying or blackmailing, threats or intimidation, and email spoofing and impersonation. It discusses the content of each category of offense, analyzes the relevant provisions, and highlights reported cases and judgments as examples. The paper concludes that neither the IPC nor the IT Act provisions fully reflect the ground realities of women's experiences, and that the first step towards providing legal remedies for women is to ensure that the online experience of harassment, threat-making, intimidation, and violence against women is accurately translated into written law through amendments to the two major statutes.

It suggests Cyber Communications grew into email communications in 1965, radically altering the game. These systems adapted quickly to the capacity for exchanging whole files or photos to make them more appealing to consumers. Communications grew into email communications in 1965, radically altering the game. These systems adapted quickly to the capacity for exchanging whole files or photos to make them more appealing to consumers. Additional steps that should be taken to address cybercrime against women in a comprehensive and effective manner In India, the number of social network users has risen dramatically from 181.7 million in 2015 to 216.5 million in 2016 and is expected to reach 250.8 million in

ISSN No:-2456-2165

2017. It is anticipated that this figure will rise to at least 336.7 million by 2020. 4 Some of the most popular social networking sites in India are Facebook, Twitter, Instagram, LinkedIn, YouTube, WhatsApp, and SnapChat. While India's internet population is growing, there is a growing gender gap among social network users. This is evident in statistics such as the number of internet users, Facebook and Twitter users, digital literacy, and political tweets. According to a Boston Consulting Group and Retailers Association of India study of internet users in India, approximately 29% of users are women, while the remaining 71% are men. The disproportionate access of men and women to the internet is a major contributor to this phenomenon. This phenomenon is closely related to the rise in cybercrime against women. Women users are frequently perceived as "invading or trespassing" on male space, especially when they express their opinions on politically sensitive and volatile issues. According to a 2015 report by the Observer Research Foundation, women are significantly underrepresented in political conversations on Twitter in India, mirroring the real-world marginalization of women in Indian political processes. According to the report, many female users, including prominent bloggers and activists, deleted their accounts due to online abuse and harassment of women.

According to official statistics provided by the Government of India's National Crime Records Bureau, 9622 cases of cybercrime were registered in 2014, with 5752 people arrested. In 2015, 11,592 cases were registered, representing a 20% increase over the previous year, with 8121 people arrested. Because the NCRB statistics do not include information about the victims' demographics, there are no official statistics available in India to inform us about the scope and nature of cybercrime against women. Indian women who use the internet today face a variety of cybercrimes. Neither the IPC nor the IT Act fully reflect the realities of women's lives. In many cases, such as morphing, email spoofing, and trolling, IPC provisions are applied through extrapolation and interpretation in the absence of more specific legal provisions. Although the IT Act includes a chapter on offenses, including computer-related offenses, the provisions focus on economic and financial issues; there are no specific provisions on cybercrime against women, despite the fact that it is widespread and widely reported. The first step towards providing legal remedies for women is to ensure that the online experience of harassment, threats, intimidation, and violence against women is accurately translated into written law via amendments to the two major statutes. It is critical to recognize that the law does not have the capacity to provide all solutions to the problem of cybercrime against women in India. Women should be trained to take preventive measures, such as exercising caution when posting photographs and video clips of themselves and their loved ones online and safeguarding passwords and other vital information that may jeopardize the woman's security and privacy. As a preventive measure, women internet users in India need to be more aware of how to improve privacy settings on social networking sites. Cybercrime against women is a symptom of the underlying patriarchal society, and patriarchy is part of Indian society. Dealing with the manifestations through legal, social, and political processes would only provide a temporary and superficial solution unless the root cause is addressed through long-term, multifaceted measures and sustained efforts. Above all, political will is the fulcrum that will allow India to address cybercrime against women in a comprehensive and effective manner. *(Mishra et al.,2021 http://hdl.handle.net/10603/454392)*

Cybercommunications grew into email communications in 1965, radically altering the game. These systems adapted quickly to the capacity for exchanging whole files or photos to make them more appealing to consumers. As far as India is concerned, there was an information technology revolution in the year 2000. This research work by the researcher analyzes the growth of cybercrime in India, especially with reference to women. People started using mobile phones and computers for interacting with their near and dear ones, and these tools were also used for e-governance. Suddenly, cyberspace has expanded its vistas and become part and parcel of the life of an individual, whether a man or woman. People use different kinds of social media, such as Orkut, Facebook, Instagram, and WhatsApp, to express their views and gather information. In India, cyberspace has gradually become a breeding ground for violence against women. Cybercriminals are harassing women by sending nebulous messages. They are harassed, and women's images are morphed. All of these offenses have generated a threat in the minds of women who use the virtual realm for fun as well as learning. Numerous international treaties identify freedom of expression and the right to live in dignity as fundamental human rights (UDHR, ICCPR, etc.). *(Mishra et al., 2021 http://hdl.handle.net/10603/454392)* In modern India, a new type of cybercrime is growing that is undermining women's dignity, something that is a fundamental right. This study examines the many reasons for cybercrime against women in India as well as the types of humiliation women encounter in the virtual realm through no fault of their own.

IV. THEORETICAL FRAMEWORK

The spiral of silence theory is a political science and mass communication theory proposed by the German political scientist Elisabeth Noelle-Neumann.

It asserts that an individual's view of how public opinion is distributed influences that individual's desire to communicate their own thoughts, which in turn influences the perceptions and, eventually, willingness of others to voice their opinions. The key premise is that social contact influences people's propensity to communicate their thoughts. Individuals will be more confident and outspoken with their opinions, according to the spiral of silence idea, when they discover that their particular perspective is shared throughout a group. However, if the person detects that their viewpoint is unpopular with the group, they are more likely to be reserved and keep silent. In other words, the individual's view of how others see him is more essential to him than the need for his opinion to be heard.

This hypothesis is acceptable because it assumes that in any given scenario, we all have an intuitive sense of what the majority view is. The spiral is created or reinforced when someone in the perceived majority speaks confidently in support of the majority opinion, causing the minority to become increasingly distanced from a place where they are comfortable voicing their opinion and experiencing the previously mentioned fears.

The spiral effect occurs when this starts a downward cycle in which anxieties constantly increase inside the minority view bearer, resulting in the minority opinion never being spoken. The media is crucial in this process, particularly in dictating or perceiving the majority view. The closer an individual believes their perspective is to the majority opinion, the more inclined they are to express it in public dialogue. A few other important tenets to note: this theory is heavily based on the idea that the opinion must have a distinct moral component (i.e., abortion, sexual harassment, etc.), and no one will experience the spiral of silence while attempting to decide what flavor of ice cream to have after dinner with roommates.

The theory has some weaknesses, or at least points of contention, two of the most notable are those of the vocal minority and the internet. The internet seemingly levels the playing field, where a minority opinion won't be felt by the individual as a minority opinion and might be voiced in that arena, whereas the individual would not have been so vocal in another place of public discourse.

In cybercrime, victims' statements or opinions are silenced or avoided. People may believe that society will never accept or mock them, causing them to remain isolated from the rest of the world. If victims make any type of report but do not obtain a suitable response, it becomes difficult for them to interact with anyone. As a result, I adopted the spiral of silence idea.

V. RESEARCH METHODOLOGY

Based on the previous research, an attempt was made to perform a qualitative inquiry into the nature and scope of cybercrime victimization as well as its impact on women victims. This chapter describes the current study's research strategy and methodologies. The procedures and tools used by the researcher to perform the research are referred to as research methodology (Babbie & Mouton, 2001) and include the research design, data collection, data analysis, and sampling design. In the present chapter, research design, data collection, tools of data collection, sampling design, data analysis, and statistical analysis of the study data have been given.

A. Research Design

The structure that has been constructed to seek answers to the research questions is known as the research design (Kumar, 2005). A research design is essentially a plan or blueprint for the investigation. A well-planned research design ensures that your procedures meet your research aims and that you employ the appropriate type of analysis for your data. By design, the present study is descriptive research, which, as the name implies, focuses on characterizing existing situations, behaviors, or characteristics by methodically obtaining information without modifying any factors. In other words, the researcher does not interfere; only the information is collected. A descriptive design is focused on explaining events and circumstances (Babbie, 2008). The reason for employing research design is that it helps and allows for getting the information in depth without any kind of modification. It also provides a picture of a situation as it occurs in a natural setting. Descriptive design helped me to develop my theory and also provided answers to the questions of who, what, when, where, and how. Another design that was adopted was an exploratory research design. When the researcher has no previous data or only a few studies to refer to, an exploratory research design is used. This study is sometimes casual and unstructured. It is a research instrument that gives a hypothetical or theoretical notion of the study topic. It will not provide specific solutions to the research challenge. This study is carried out to ascertain the nature of the problem and to assist the researcher in developing a better knowledge of the situation. Exploratory research is adaptable and lays the framework for future research. Exploratory research necessitates the researcher's investigation of several sources, such as public secondary data, data from other surveys, observation of research objects, and views about a firm, product, or service.

B. Aim of the Study

The purpose of the study is to determine the security of women on social media platforms, namely Instagram and Facebook. The study will further focus on the causes of unreported cybercrimes by victims.

C. Objectives of the Study

- To identify different types of cyber crime against women
- To examine and compare the security of women in different social media platforms, namely Facebook and Instagram
- To find out the causes of unreported cybercrimes by victims

D. Research Questions

- What are the causes of rising cybercrime against women? How does social media affect the lives of women?
- What are the social media platforms that are safer for women to use?
- What are the causes of unreported cybercrimes by victims?

E. Sampling Design

The sampling design is the approach you employ to choose your sample. There are several sampling designs, and they all serve as guides for selecting your survey sample. The goal of sampling design is to guarantee that your chosen sample allows you to generalize your findings to the overall population you're targeting. In this research, I

have chosen a non-probability sampling method. The criteria for selection in non-probability samples are not random, and the chances of inclusion in the sample are not equal. While non-probability sampling is easier and less expensive, there is a greater danger of sample bias, and conclusions about the entire population are weaker. And in this research, I have used a purposive sample. A purposive sample is a non-probability sample that is chosen based on demographic characteristics and the study's purpose. Purposive sampling, as opposed to convenience sampling, is sometimes referred to as judgmental, selective, or subjective sampling. Purposive sampling allows you to get the most information from a limited population. Purposive sampling enables researchers to collect responses for qualitative studies, resulting in more exact results. It ensures that the information you gather is relevant to your study. Purposive sampling allows you to target specific audiences for your research.

F. Data Collection

Data collection methods are methods for directly measuring variables and acquiring information. Data collection helps us get first-hand expertise and fresh insights into our study challenge, whether we are conducting research for business, government, or academic objectives. The process of gathering data is separated into two sections: primary data and secondary data.

- *Primary Data*

Primary data is information gathered for the first time through personal experiences or proof, typically for study purposes. It's also known as raw data or firsthand knowledge. The method of gathering information is costly since the analysis is performed by an agency or an external organization and requires human resources and expenditure. The investigator personally oversees and manages the data collection process. The majority of the data is gathered by observations, physical tests, postal questionnaires, surveys, personal interviews, telephone interviews, case studies, and focus groups, among other methods. In this research, as primary data collection I have employed a survey questionnaire, telephonic interview. Primary data is information that was not planned previously.

- *Secondary Data*

Secondary data is data that has previously been acquired and recorded by some researchers for their own purposes, rather than for the present study challenge. It is available in the form of data gathered from many sources such as government publications, censuses, internal organizational records, books, journal articles, websites, and reports, among others. This form of data collection is inexpensive, easily available, and saves both money and time. The one negative is that the material gathered is for another reason and may not fit the current study goal or be reliable.

For secondary data, I study journals, books, research papers, and so on.

G. Tools of Data Collection

Data collection tools are equipment or instruments used to gather data, such as a paper questionnaire or a computer-assisted interviewing system. Case studies, checklists, interviews, observations, and surveys or questionnaires are all data collection techniques. It is important to select data collection tools since research is conducted using a variety of methods and for a variety of goals. The goal of data collection is to collect high-quality evidence that can be analyzed to produce persuasive and reliable responses to the questions addressed. In my research, Under primary data tools two telephone interviews and survey questionnaires, a set of 14 questions was used.

H. Data Analysis Design

Data analysis is a subset of data analytics that focuses on extracting meaning from data.

For my research work, the data analysis design used is descriptive design and statistical design. For qualitative analysis as descriptive design, content analysis was used. This is a popular method for analyzing qualitative data. The content analysis approach is used with the study's objectives in mind. Some research papers and journals have been picked based on their dispersion and geological region.

Statistical analysis is the process of gathering huge amounts of data and then utilizing statistics and other data analysis tools to uncover trends, patterns, and insights. For this research survey questionnaire was used as statistical design.

In this research the facts and research findings are shown with the help of tables, bar diagrams and pie charts.

VI. FINDING AND ANALYSIS

This chapter discusses information analysis and research discoveries. Keeping in mind the planned aims of the research project, necessary and optional material were obtained and assessed accordingly. For this research study, named, ‘A study on cybercrime against women: Special reference to DIBRUGARH UNIVERSITY’ a total of 101 questionnaires were distributed online among Dibrugarh University students and the same figures were received from the respondents. The available data has been thoroughly discussed. To answer all of the questionnaire's questions, descriptive statistical analysis was utilized to establish ratios and percentages.

A. Data Analysis and Interpretation

➢ *Age Group of Sample Audience*

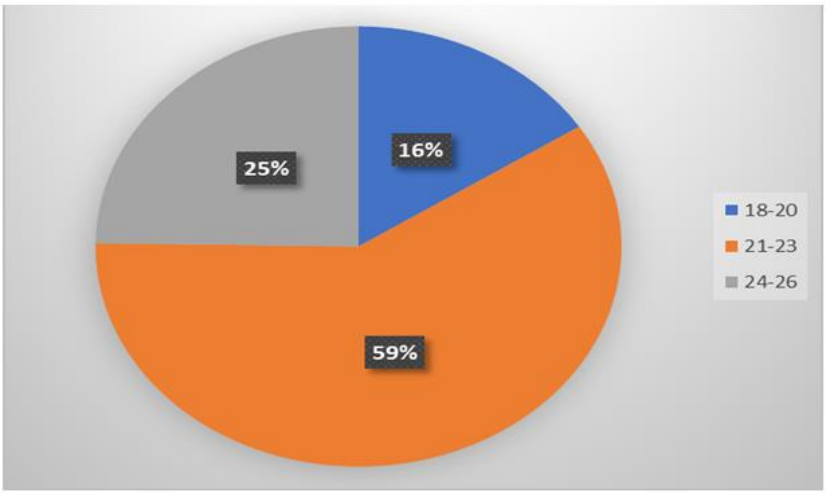

Fig1 A Majority of the Sample Audience (59%) Belongs to the Age Group 21-23 Years Old, the Second One is (25%) between 24-26 Years Old and the Third One is (16%) between 18-20 Years Age Group.

➢ *Which place do respondents belong to?*

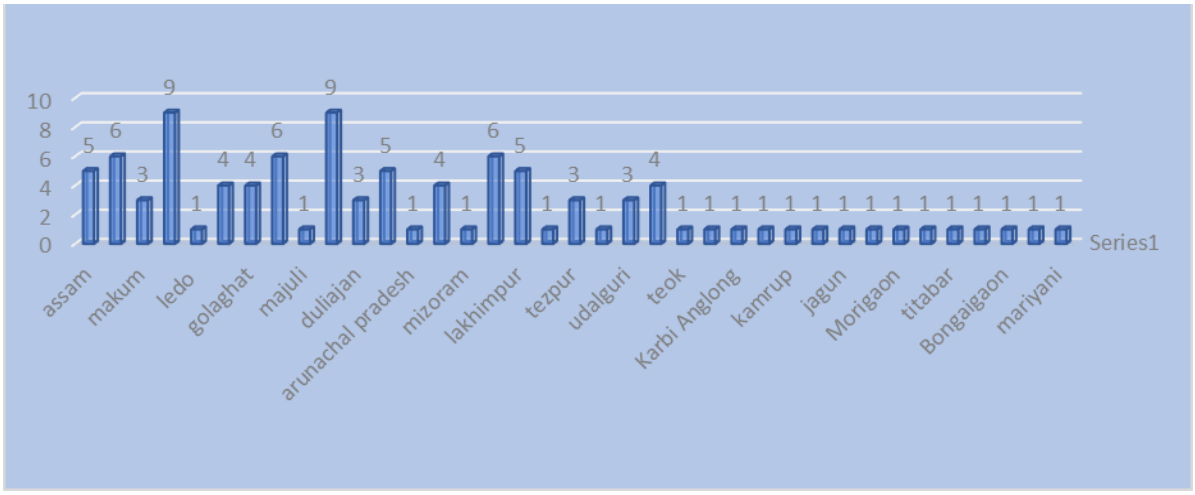

Fig 2 The respondents belong to different different places. Most of the people belong to Assam.

➢ *People who are and aren't on Social Media:*

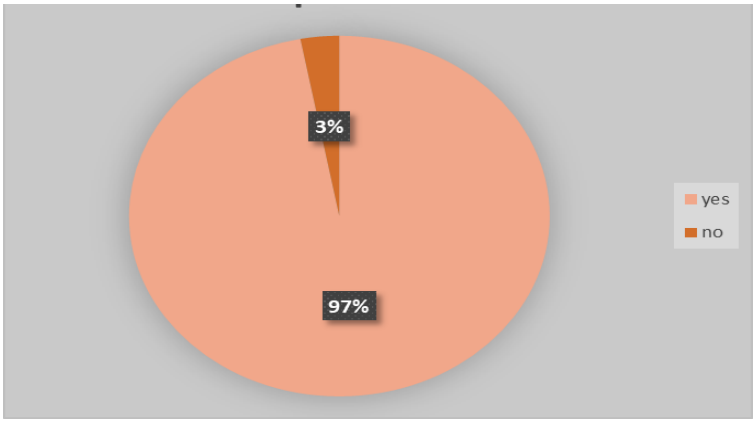

Fig 3 The following inquiry in the survey is about people who are or who are not on social media. 97% of people use social media and only 3% of people don't use social media platforms. From this survey I have found that most of the people are on social media.

➢ *Which One of the Social Media Platforms People Prefer the Most*

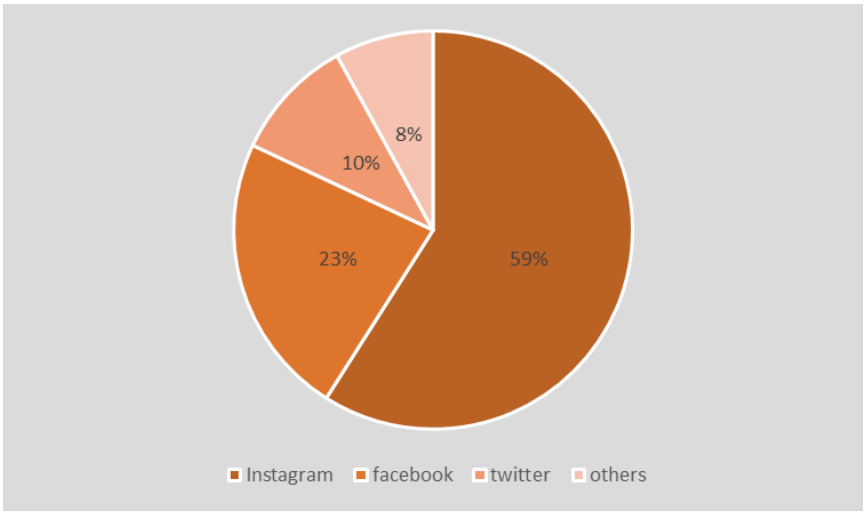

Fig 4 The above diagram refers to which one of the social media platforms people prefer the most. 59% of people use Instagram , 23% of people use Facebook , 10% of people use Twitter and 8% of people are on other social media platforms.

➢ *How many respondents are and aren't aware of cybercrimes?*

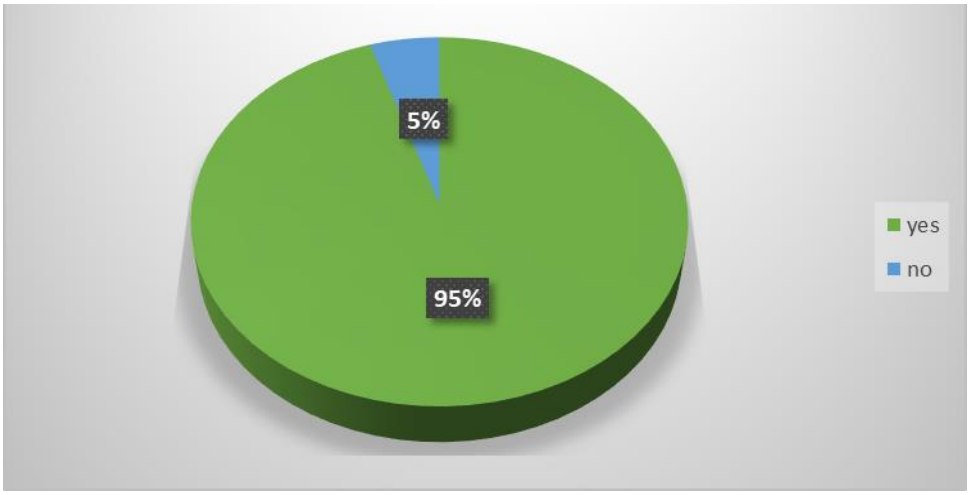

Fig 4 95% of the respondents are aware of cybercrimes. But 5% of the respondents are not aware of cybercrimes.

➢ *Respondents who are and aren't faced cybercrime*

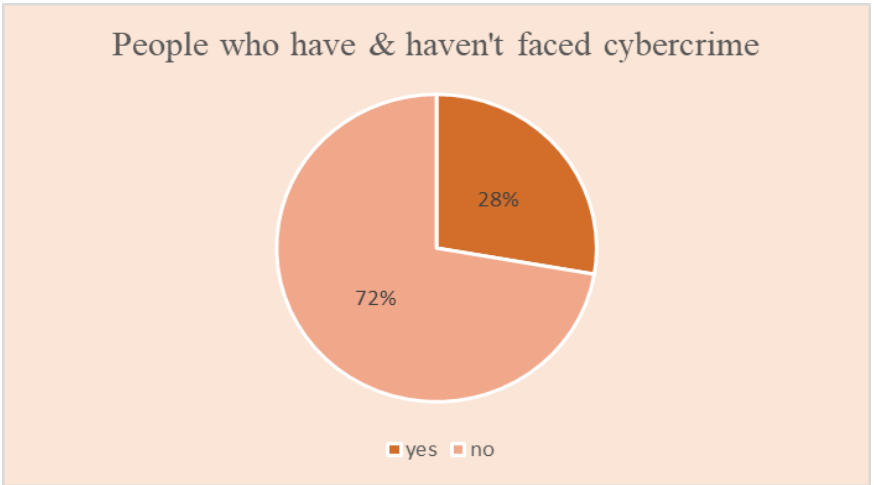

Fig 5 The following inquiry in the survey is about how many respondents are & aren't faced cybercrime. 72% of the respondents have not faced cybercrime yet. And 28% of the respondents have faced cybercrime through social media platforms.

➢ *How many respondents have and haven't seen women's harassment news online?*

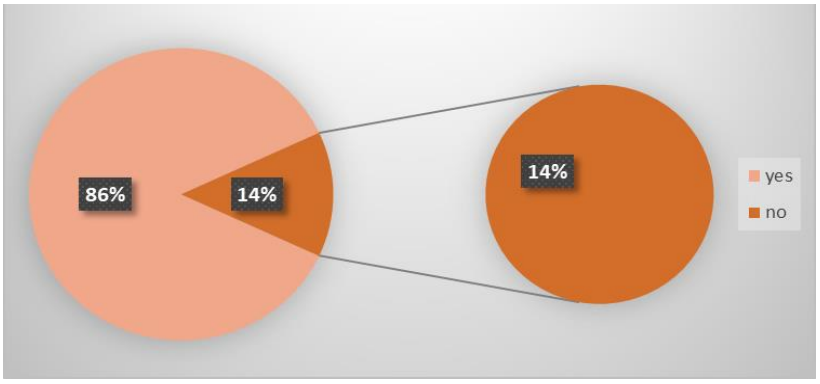

Fig 6 86% of the respondents have seen women's harassment news online and only 14% of the respondents haven't seen any news related to women's harassment online.

➢ *Respondents, those who have ever faced any kind of cybercrime, then from which platform?*

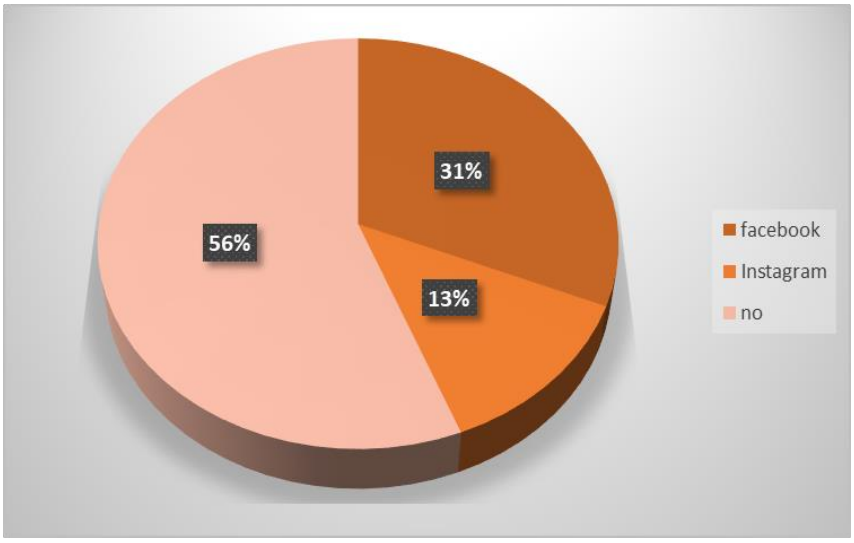

Fig7 56% of the respondents have not faced any kind of cybercrime yet. But 31% of the respondents have faced cybercrime through facebook and 13% of the respondents faced through instagram.

➢ *How many respondents have and haven't filed complaints against cybercrime?*

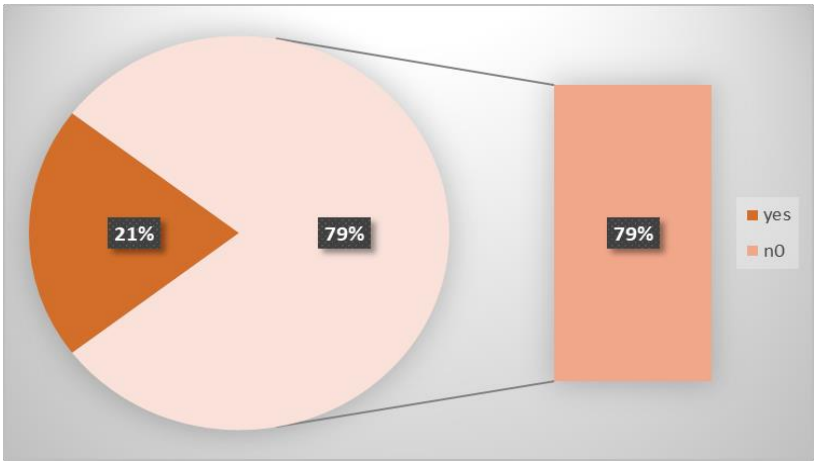

Fig 8 The following inquiry about how many respondents have or haven't filed complaints against cybercrime. Only 21% of the respondents have complaints against cybercrime. 79% of the people haven't filed complaints against cybercrime. Most of the people didn't face cybercrime. But those who had faced , they didn't get a proper response and some of them didn't report complaints against the crime because of the fear of isolation from society and the rest were unaware of cybercrime.

➢ *Are you satisfied with the way your complaint was handled?*

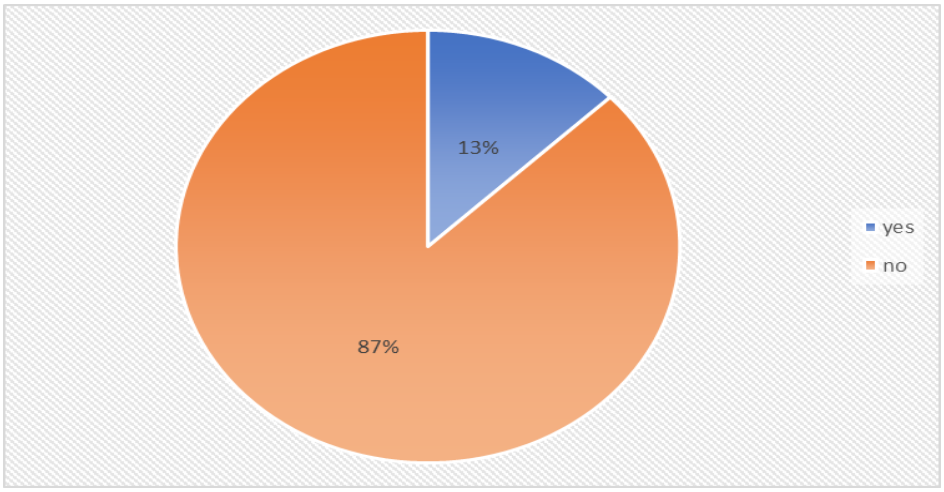

Fig9 According to the survey 87% of the respondents are not satisfied with the way their complaints have been handled. But only 13% of the respondents are satisfied.

➢ *What should you do if you visit a website that makes you uncomfortable?*

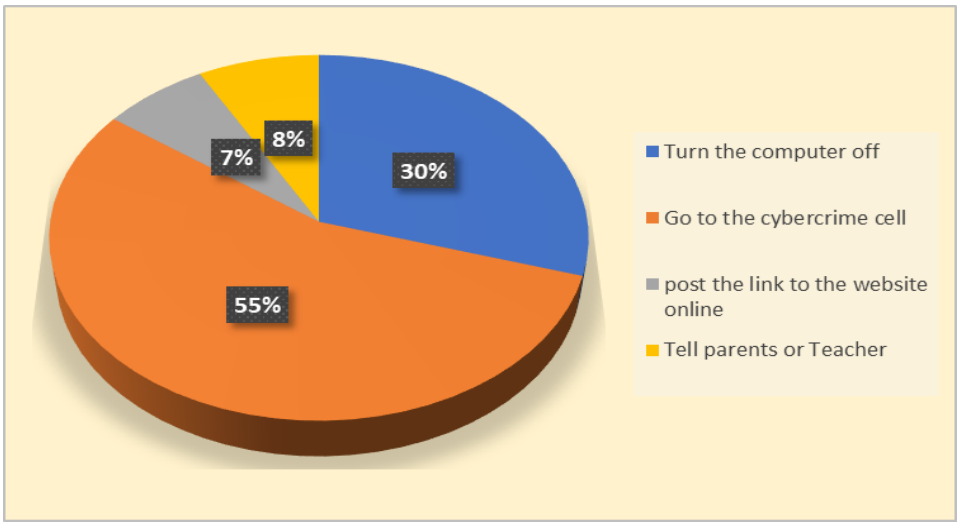

Fig10 Through the survey I learned that 55% of the respondents go to the cybercrime cell when they visit a website that makes them uncomfortable , 30% of the respondents turn off the computer, 8% tell their parents or teacher and the rest of the 7% post the link to the website online.

➢ *Respondents' Suggestion for Cybercrime Victims*

According to the respondents , the people who are facing or faced any kind of cybercrime then they should raise their voice against this evil crime. So ,many lives can be saved from being the victims. Victims should report to the police and also mentioned that don't trust everyone you talk to, never share personal personal information to anyone, or if anyone is facing any kind of uncomfort then immediately turn off the computer/ mobile or inform the cyber cell. It is also mentioned that not to click any link which we are not aware of.

Most of the people don't raise their voice because of fear of isolation or they think that society will never accept them , due to the reason they don't come up with any conclusion or action. But it will destroy not only their lives but also the criminals get more chances to target others. So please raise your voice. Most of the respondents suggested taking action and raising your voice to remain safe from cybercrime.

B. Interview Analysis

➢ *Cyber Violence: An Unseen Form of Violence*

- *Case 1.*

The most commonly reported and seen crimes that occur on social media involve people making threats, bullying, harassing, and stalking others online. While much of this type of activity goes unpunished or isn't taken seriously, victims of these types of crimes frequently don't know when to call the police. A similar incident once happened to one of my interviewers during her bachelor's degree.

ISSN No:-2456-2165

When she was a 2nd-year degree student. She used to stay very active on various social media platforms specifically on Facebook. Apart from her college friends, she had lots of friends online. A fraction of them were her school friends, some of her long-distance cousins, and some random mutual friends.

It was some random day, while chatting and scrolling on Facebook, she got a friend request from a girl named Riya Bora. The profile of this girl seems decent and they also shared some mutual friends. Hence, she accepted her friend request. After an hour or so she texted her a 'Hi' in her messenger. She replied to her back with a 'Hi'. And like this, their conversation started. Riya was nice and they were talking about normal things. She told her that she happens to be one of the juniors of her high school and that she knew her very well. And as they share mutual friends from her high school so whatever she was speaking seemed genuine to her. After a while, Riya gave her number and told her to add her on WhatsApp as according to her she was not that active in Messenger and she wanted to stay connected with my interviewer. The way of her texting was polite enough to convince her to add Riya to her on WhatsApp. Riya told her that she wanted her help in deciding her future study plans as my interviewer said.

After 2 days, my interviewer received a call from an unknown number. First, she rejected the call. She checked for the number in True Caller. There was no name and the number was from Karnataka. Just as she was wondering, there was another call from the same number. This time she received the call. The caller was a male with a very hoarse voice. He was asking for a girl named Puja. He very rudely asked her if she is Puja and why she is not answering his calls. She thought it was the wrong number and she politely declined and cut the call. She went to the washroom keeping her phone in charge. After a while when she came to check her phone, she was surprised that there were some 6 to 8 missed calls from that same number. Her phone was silent hence she couldn't hear it ringing. She was scared and surprised. She told her about the case. Her roommate told her that that person doesn't seem to be a gentleman and it would be better for her to block that number, so she blocked the number.

The next day, there was a call from another number that showed it was again from Karnataka. She told her roommate and both of them decided to block that number again. The following night she received calls from like 6 different numbers. She was afraid. She told her boyfriend about the whole case. He asked her if anyone with whom she has recently shared her number or not? To that, she recalled Riya and told him of their conversation the night before the incident happened. He was angry at her carelessness. He asked her if she really remembers any junior named Riya. She checked Riya's profile on Facebook and she found that she blocked her from Facebook and also from WhatsApp. She could connect the dots now. It was a scam that happened to my interviewer. It was a fake profile and the user distributed her number to various people online. Her friend told her that it's the work of a group of people who distribute any female user's number in their messenger group and start disturbing her and asking for any random girl. Eventually, this leads to blackmailing and abuse. By half an hour there were some 10 to 15 calls from different numbers in her phone. She was afraid like anything. She removed the sim from her phone that night. The very next day, they went to the police station and filed an FIR against these frauds. She also changed her sim that day and she reported all those numbers with the help of her friends. She didn't get a proper response from the police regarding the matter. After seeing her helpless, one of her friends suggested she change her number.

So now we can say that the cybercrime victims don't report against offenders only because no one comes forward to support them. According to the victims , they feel that if they raise their voice then society will not accept them or make fun of them. And also in the fear of isolation they do not make complaints against this evil crime.

- *Case 2. Similarly, Another Person Stated:*

In the year 2019, one random day, my interviewer was scrolling on Facebook, and suddenly a random guy added her to a group. In that group, everyone was a stranger. She didn't know anyone. She checked that guy's Facebook profile and found that he was her Facebook friend. But she couldn't recall when she accepted his request. Some messages were coming, and when I checked, they were from that particular group. In that everyone was using slang languages and asking for nude pictures and some sent nude pictures. My interviewer was totally confused and scared. It was tough for her to find out what was going on with her and why did the guy added her in that group? Some people from that group started to message her in her inbox and sent her some nude pictures. Instantly she blocked them. She also tried to leave the group but failed to leave .She realized that she was trapped.

So after 2-3 days, she deactivated her account and reported the incident, but she didn't get the proper response. Instead of helping her, they told her not to use Facebook or that type of social media. The police told her that she should be careful. This incident left her in doubt with social media. According to her, for many days she was in trauma and after a few months or so she created a new Facebook account.

It's not just one case, there are hundreds of cases that happen daily. Frauds and hackers always try to target Facebook profiles as well as Instagram pprofiles, irrespective of the various security and privacy policies claimed by Facebookok and other social media apps. Moreover, according to various surveys most of these victims are women and teenage girls.

ISSN No:-2456-2165

VII. CONCLUSION

According to the data analysis of a survey research regarding a study on cybercrime against women: Special reference to Dibrugarh University, the survey was able to evaluate the users' awareness level on cybercrime. The purpose of the study is to determine the security of women on social media platforms, namely Instagram and Facebook. The study will further focus on the causes of unreported cybercrimes by victims.

In response to the first research question, it is discovered that the fundamental goal of social media is the sharing of both private and professional details, resulting in a virtual treasure trove of easily available information. Because of these circumstances, cybercriminals now have easy access to social media. Online fraudsters may simply build a phony account on social networks and use advanced phishing methods to attack 185 directly. Social networking applications and links entice people to visit them and give their personal information. The cybercriminal assaults innocent users utilizing that information. Cybercriminals collect information held on social media using complex and sophisticated methods / malware tools and may engage in illegal activities such as theft, fraud, extortion, and intellectual property theft. Female users were the researchers' primary goal. A ccording to this study, pornography, extortion, morphing, cyber harassment, defamation, email threat, cyber stalking, transmitting obscene information, and sexually explicit materials are the offenses that women users are more likely to become victims of than males.

Female users are emotional by nature and readily persuaded. Any individual or group of individuals can readily approach female users and victimize them for personal or public advantage. Cybercrime causes identity theft and fraud, posting sexually explicit materials and vulgar comments on social media profiles causes reputation harm, cyberbullying and leaking personal information causes psychological harm due to private discussion over chat, cyber stalking caused by displaying current location through GPS system, spreading malware causes system and important data damage, information theft caused by unauthorized access to computer systems. Cybercrime is the result of a group effort to enhance digital technology. As a result, a multifaceted strategy from law enforcement agencies, the information technology sector, public-private partnerships, and information security organizations is required to collaborate in order to improve their abilities with such technologies and discover a solution to reduce cybercrime. Aside from such collaboration, users must also be aware of cyber-criminal activity on social media. To stop the crime, social media users must be extra cautious while publishing and sharing anything on the platform in order to reduce their chances of becoming victims of it.

In response to the second research question, social media usage among female users is on the rise and has been shown to aid research and connectivity. Awareness campaigns may help tackle cybercrime in a variety of ways. The possibility of a cyber-attack can be reduced by exercising caution when utilizing social media. Technology advances in order to move forward and make life easier. At the same time, hackers are rapidly developing strategies to exploit technology. Even if the government or corporate institutions are not in a risk-free zone, no individual in cyberspace is safe. All of them must realize the need to adopt preventative measures and raise awareness about cybercrime, which are as follows:

- Always use anti-virus, firewall, and internet security software and keep it up to date.
- Never give anybody access to your computer system.
- Always keep a backup of your important computer files.
- One should not share a computer system with another person since they may copy crucial data from the system in order to exploit the owner.
- To guard against malicious software attacks, install anti-firewall, anti-virus, and anti-spyware software on the machine.
- Never hand out sensitive information such as your computer password or login password to an unknown individual.
- Never, ever click on an unknown link.
- Never respond to spam.
- Always keep the privacy setting on.
- Data saved on a computer should be password-protected.
- Use a different password for each online account.
- In one word, no human is fully defenseless against cybercrime.
- For cyber offenders, there are penalties for fines, jail, or both.
- The technologically advanced legal system created specifically to cope with cybercrime.
- Many law enforcement authorities in India have specialized units for cybercrime under Indian cyber legislation.

These regulations serve as protections against cybercrime, allowing for secure electronic communication and In India, the 189 Information Technology Act-2000 and the Indian Penal Code have provided legal authorization to categorize cyber-criminal actions into distinct areas.

In response to the third research question, most cybercrimes go undetected because of the victim's hesitancy and shyness, as well as her fear of defaming her family's name. She frequently thinks that she is to blame for the crime committed against her. Women are especially vulnerable to cybercrime since the perpetrator's identity remains unknown, and he may repeatedly threaten and blackmail the victim using multiple names and identities. Women still do not go to the police to report sexual harassment, whether in the real or virtual world; they prefer to avoid the issue because they fear it would disrupt their family life. Cybercrime victims do not report criminals because no one comes out to assist them. According to the victims, if they raised their voices, society would reject or mock them. Also, for fear of being alone, they do not report this awful crime.

According to the findings of the study, women lack enough awareness about cybercrime. In the majority of situations, they become a primary target for cyber thieves. As a result, some preventative measures must be taken to keep crime to a minimum when using social media. The actions include raising knowledge about social media and cybercrime, remaining vigilant when using social media, and informing others about the related dangers.

REFERENCES

[1]. Bhat, R. M., Ahmad P. A., (2022). Social Media and the Cyber Crimes against Women- A Study. Vol: 02,1-5, (https://doi.org/10.55529/jipirs.21.18.22)
[2]. Backe, E. L., Lilleston, P., & Mc-Cleary-Sills, J. (2018). Networked individuals, gendered violence: A literature review of cyberviolence. Violence & Gender, 5(3), 135–146. https://doi.org/10.1089/vio.2017.0056
[3]. Sarkar, S., Ranjan, B.,(2021). Materiality and Discursivity of Cyber Violence Against Women in India. 5-10, DOI: 10.1177/0973258621992273
[4]. Malegi, S., (2021). Abuse of Women Through Social Networking Sites During Lockdown- Is Law Inadequate?. vol:9,(2021, Feb 2) , ISSN: 2320-2882
[5]. Uma, S., (2017). Outlawing Cyber Crimes Against Women in India. Bharati Law Review , 104-110.
[6]. Kumari, A., Sharma, K., & Sharma, M., (2015), Predictive Analysis of Cyber Crime against women in India and laws prohibiting them, International Journal of Innovations and Advancement in Computer Science, Vol.4, No.3.
[7]. Gupta, S., Singh, A., & Kunwar, N., (2017). Impact of Cybercrime on adolescents through Social Networking sites, International journal of Law, Vol.3, No.6.
[8]. Citron, D. K., Franks, M. A., (2014). Criminalizing Revenge Porn. Wake Forest Law Review, Vol. 49, 2014.
[9]. Pashang, S., Khanlou, N., (2022). The Changing Face of Gender-Based Cyber Violence during the COVID-19 Pandemic: Unmasking Virtual Identities.Journal of Concurrent Disorders.
[10]. Mishra, S., (2021). A Critical Study on Cyber Crime With Special Reference To Women In India. (http://hdl.handle.net/10603/454392).