

GENDER AND CYBER CRIMES

Vaishnavi Parate*

ABSTRACT

Hacking is the first thing that comes to mind when people hear the term cybercrime. Yet there is much more to cybercrime than that. Cybercrime has changed and opened up a new horizon since a new internet revolution was sparked by the appearance of numerous social media and dating applications. Individuals frequently fail to comprehend the gravity of today's gender-biased cybercrimes. People who consistently complain about the same things are often told to get thicker skin. Gender-based crimes can be described as "crimes that are intended against a woman because she is a woman or that harm women disproportionately" because these crimes are frequently committed against women. This essay will cover every aspect of gender-based cybercrimes and examine the legislation designed to reduce them.

Keywords: Gender, Gender Equality, Cyber Crime, Cyber Law, Social Media.

INTRODUCTION

The information and technological age that currently rules the modern India that we live in has made online communication the new norm for socializing and meeting new people. Millions of men and women use the internet every day as a medium for the unrestricted expression of ideas.¹ It has evolved into a means of disseminating and transmitting information for business, leisure, and a variety of other uses. The fact that people can use this stage for their antagonistic objectives makes this freedom not entirely advantageous. Over time, there have been an increasing number of reports of crimes being perpetrated online. "These crimes, commonly referred to as cybercrimes, include hacking, phishing, hate crimes, child pornography, bullying, stalking, etc²." Its prevalence has increased over the past 20 years, with women and children being their primary targets. Also, as the cyber world developed, the victimization of women

*LLB, THIRD YEAR, SHRI. NATHMAL GOENKA LAW COLLEGE, AKOLA.

¹ 'Cybercrime-Descriptive Portrayal of Crimes against Women in India'

<<https://www.legalserviceindia.com/legal/article-5858-cybercrime-descriptive-portrayal-of-crimes-against-women-in-india.html>> accessed 15 March 2023.

² ibid

increased. But the obvious question is why women are the main victims of cybercrimes such as cyberstalking and cyberbullying³.

CRIMES BASED ON GENDER

“Crime against women immediately comes to mind when discussing gender-based crimes because there have been numerous incidents of rape, sexual harassment, stalking, workplace sexual harassment, and other such crimes. The reality that there are more crimes against women and girls than against other groups cannot be ignored⁴.” So, there is a need to research these crimes because doing so aids in developing appropriate responses, interventions, and services for such gender-based crimes, particularly cybercrimes given that it has been observed that women and girls are most susceptible to many crimes committed online⁵. Because cybercrime cases make up such a small percentage of all instances reported in our nation, it is very simple to brush them off. It is nearly impossible to overcome the societal stigmas associated with cybercrime and women without a reflective response since they are so firmly ingrained in Indian society⁶.

KINDS OF GENDER-BASED CYBER CRIMES

“The list of cybercrime subtypes is virtually limitless. But, as was already mentioned, there is a major difference between cybercrime and gender-based cybercrime. We shall therefore concentrate on interpersonal cybercrimes depending on gender⁷.” Hence, the following are some examples of gender-based online crimes:

CYBERHARASSMENT OR BULLYING

“Bullying committed online is known as cyberbullying. Social media, chat services, gaming platforms, and mobile devices are all potential venues. It is a pattern of behavior meant to frighten, infuriate, or embarrass those who are the target⁸.” An example of cyberbullying is

³ infra

⁴ European Parliament. Directorate General for Parliamentary Research Services., *Combating Gender-Based Violence: Cyber Violence : European Added Value Assessment*. (Publications Office 2021) <<https://data.europa.eu/doi/10.2861/23053>> accessed 15 March 2023.

⁵ Japleen Pasricha, *Cyber Violence Against Women in India- A Research Project, Feminism In India* (May 12, 2021, 11:04 AM), <https://feminisminindia.com/2016/11/15/cyber-violence-against-women-india-report/>

⁶ ibid

⁷ ibid

⁸ Sneha Mahawar, ‘All You Need to Know about Gender-Based Interpersonal Cybercrime’ (*iPleaders*, 15 October 2021) <<https://blog.ipleaders.in/all-you-need-know-about-gender-based-interpersonal-cybercrime/>> accessed 15 March 2023.

when you are out with your pals and they unintentionally take an embarrassing photo, which they then post online and use to disseminate false information about you. Bullying on the internet and bullying in person coexist. Also, it is recognized that physical bullying and cyberbullying trigger similar biochemical responses in the body⁹.

STALKING

Cyberstalking is known as persistently contacting someone online without their consent. “Any number of incidents, such as threats, libel, slander, sexual harassment, or other attempts to intimidate or control their victim, may be involved¹⁰.” Example: You have an Instagram account, and one account keeps texting you even if you don't want to receive their messages. This is a sort of cyberstalking since they continue even after you tell the sender you don't want to receive their communications. The practice of stalking online has evolved from physical stalking. Furthermore, because cyberstalkers may quickly find sensitive information about a victim with a few mouse clicks, it can be even riskier than physical stalking.

MORPHING

“Morphing is the smooth transition from one image to another without any adjustments. Girls are typically impacted by morphing, where users download female images from numerous social media networks using either false or actual profiles before manipulating them¹¹.” As an example, today everyone uses social media. “Consider uploading a photo to Facebook. If someone copies your photo and then swaps out your body with a naked one, they may be held accountable for the crime of morphing. By threatening to publicize the modified photographs, the girl or her family may be subjected to blackmail.”

VOYEURISM OR OBSCENITY

Voyeurism is the practice of spying on unsuspecting individuals while they are undressed, naked, or involved in sexual activity. Voyeurism, however, is not just limited to seeing; in modern times, it also includes recording and photographing what is being observed¹². An example of voyeurism would be if someone covertly observed you changing clothes in the changing room and took images of you. Cyberstalking is the most frequent cybercrime against

⁹ ibid

¹⁰ Mahawar (n 7).

¹¹ European Parliament. Directorate General for Parliamentary Research Services. (n 4).

¹² ibid

women. Usually, the person is in a setting where they can expect some kind of privacy, like their house or another private space.

KID GROOMING ONLINE

Internet grooming is the practice of making friends with children online and earning their trust to abuse them. Sexual abuse, both offline and online, as well as the exploitation of children to get pornographic photographs and films are two negative effects of grooming¹³. An example would be if you were chatting with someone online and he later became your friend, leading you to believe you had found a friend in him. After a while, you realize that the other person's only goal was to hurt you. This is child grooming online; regrettably, anyone can do it, regardless of age, gender, or ethnicity.

SEXTORTION

“Sextortion is a type of online abuse in which a cybercriminal seduces a user into an intimate video or audio chat and forces them to pose nude or obtains intimate photos from them. They do this by using various channels, including instant messaging apps, SMS, online dating apps, and social media platforms¹⁴.” An example of sextortion would be if you were in a relationship with someone and sent them sexually explicit pictures and films while it was still going on. After the relationship ended, they threatened you about posting pictures and videos on social media. You don't have to be associated with that person all the time, though, as recent technological advancements have made it possible for someone to access your phone by simply clicking on a link or picking the wrong number.

REGULATION OF CYBER LAW

India created its own Information and Technology Act in 2000¹⁵ to ensure the safety of online activities there. The Act's Sections 66 and 67 address online offenses that could cause someone harm or injury¹⁶. Yet, it's crucial to remember that this act does not specifically address cyberstalking or cyberbullying. The Information Technology Act of 2000 only defines specific

¹³ ibid

¹⁴ Sneha Mahawar, ‘All You Need to Know about Gender-Based Interpersonal Cybercrime’ (*iPleaders*, 15 October 2021) <<https://blog.ipleaders.in/all-you-need-know-about-gender-based-interpersonal-cybercrime/>> accessed 15 March 2023.

¹⁵ The Information Technology Act, 2000.

¹⁶ ‘It_act_2000_updated.Pdf’ <https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf> accessed 15 March 2023.

offenses and specifies the penalties for them, none of which characterizes cybercrimes. In *US v. Grob*¹⁷, the term "cyberstalking" was used to describe an attempt to kill, hurt, or harass someone online that causes that person to reasonably fear for their safety. In India, "cyberstalking is punishable under Section 354 D of the IPC¹⁸ however, the IT Act does not contain any specific language addressing the protection of a woman's dignity¹⁹." "The Indian Criminal Code's Section 509 discusses the significance of protecting a woman's modesty. The protection of one's honor and the dignity of an individual are discussed in Articles 21 of the Indian Constitution and 5 of the International Declaration of Human Rights²⁰."

RULES UNDER THE IPC

"Stalking is covered in Section 354D of the Indian Penal Code (IPC). This section specifically addresses anyone who keeps tabs on a woman's use of the internet, email, or any other kind of electronic communication and whose actions are considered to constitute stalking." Voyeurism has been debated in the past from the standpoint of the IT Act. It has, however, also been covered by section 354C of the IPC. Voyeurism is specifically addressed to women under the IPC, whereas it is addressed to both genders in the IT Act. This is the main distinction between the two sections. Obscene image publishing and distribution are covered by Section 292 of the IPC. Hence, whether or not consent is obtained, each act entails recording and disseminating explicit content. Furthermore, under the purview of this clause, utilizing it for the financial benefit may result in punishment.

LIMITATION ON CYBER LAW

There is a serious issue with the country's laws not being adequate and the lack of an effective enforcement system. The IT Act's laws that address invasions of privacy are subject to a three-year sentence and are bailable. "Another issue is inadequate law enforcement, which, in one case, contributed to the death of a little girl named Vinupriya whose complaint was ignored by the police. Other cases, like *Kiran Girotra v. State*²¹, that demonstrate the law enforcement

¹⁷ *United States v. Grob*, 625 F.3d 1209 (9th Cir. 2010)

¹⁸ 'India Code: Section Details' <https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00037_186045_1523266765688&orderno=398> accessed 15 March 2023.

¹⁹ Cristian Moise, Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level, 7 *Journal of Law and Administrative Sciences JOLAS* 374, 374-383 (2015).

¹⁸ The Universal Declaration of Human Rights, art. 5

²¹ 2012 SCC OnLine Del 2673

agencies' lax approach to enforcing the law also come to mind. In this case, a delay in filing an FIR changed the court's ruling²².”

“A conflict of jurisdiction involving various courts located in various national jurisdictions is also likely to occur.” Also, “there are significant variations in country legislation, laws, and legal processes. Another issue is that Section 1 of the IT Act does not specify how a provision of this nature would be applied across transnational boundaries and countries.” However, “the Government may only use the extradition if a legitimate treaty exists between the two nations²³.”

DEVELOPMENT UNDER IT ACT

The development of technology is a source of untapped potential that can present both opportunities and serious dangers to the cultural dominance of a state or country or region. Regarding cybercrimes that are done, the Indian legal system is still a little nebulous and broad, and the gaps allow the perpetrators to get away with their wrongdoing²⁴. The IT statute has to be amended to include offenses like cyberbullying and stalking under separate headings or the same heading. Another issue of worry is the ignorance of the cyber laws that are now in place. To induce sufficient fear in the criminal, it is also necessary to render violations of the IT Act non-bailable. The issues affecting women are not seriously considered in this statute. The act's preamble makes clear that it covers a wide range of economic and business-related topics²⁵.

CONCLUSION

The seriousness of gender-based crimes against women has now begun to receive the attention it deserves. Although Indian laws do not meet the same standards as those throughout the world, there are various provisions designed to stop these gender-based cybercrimes. Nonetheless, the nation is still in the process of effectively classifying online behavior directed towards a specific gender as a crime. Thus, we require distinct rules for these types of crimes, and if they are implemented, the internet environment will be much better and safer for women. Today, the negative aspects of the internet are frequently ignored while discussing how

²² Rajiv Mehrishi, *Crime In India* 164, (Ministry of Home Affairs, Government of India) (2015).

²³ Cristian Moise, *Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level*, 7 *Journal of Law and Administrative Sciences JOLAS* 374, 374-383 (2015).

²⁴ *ibid*

²⁵ *ibid*

technology has altered the world. We talk about better trade, increased connectedness, and expanded communication, but we neglect to mention decreased security and increasing threat. The most significant aspect of this is that, while India as a nation has opposed major injustices against women, such as the Nirbhaya case or domestic violence against women, we are still ignorant of the effects and consequences of cybercrime as a whole, and the rising prevalence of these offenses calls for better, more effective laws as well as greater public awareness.

