Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
March 2024 5(3), 437–444

CYBER INFRINGEMENTS: ANALYZING JUDICIAL AND LEGISLATIVE SAFEGUARDS FOR WOMEN'S PRIVACY RIGHTS IN INDIA

Rupaksh Sharma [1], Dr. Susanta Kumar Shadangi [2]

[1]Research Scholar, ICFAI Law School, ICFAI University Dehradun
[2]Associate Professor, ICFAI Law School, ICFAI University Dehradun

ABSTRACT

Privacy is one of the necessary requirements that cannot be arbitrarily implemented in any society. People in the same continent may understand privacy as an individual right to privacy in different ways. Appreciation of privacy at global level can be interpreted in Universal Declaration of Human Rights as a liberty right, which is an inherent part of the mankind. With that is evident that privacy violation is not limited to the physical spaces; rather, a person can be violated in all types of computer media. As dependency on internet grows and, therefore use of virtual modes, there are several considerations since people may not be prepared for new technologies I n performing everyday tasks. The matter becomes more complicated when privations are committed against the most helpless in the society. Women and sexual minorities take most of the heat of privacy violations since the society today is embedded in a patriarchal system. Women may face various other sub-violations on the internet which may be included under the title of Technology Facilitated gender-based violence (TFGV). Infringement of privacy is a violation of fundamental rights as recognized under the right to life and personal liberty but privacy violations that take place on digital platforms is not acknowledged and recognized yet. Women are vulnerable to a range of sub-violations, referred to as Technology Facilitated Gender-Based Violence while using the internet. Infringing on someone's privacy is a violation of their fundamental rights, such as the right to life and personal liberty. However, privacy violations that occur on digital platforms are yet to be fully recognized and acknowledged. It is imperative to address these issues to ensure that women are safe and secure while using digital platforms. In this paper, research examines the adequacy of current Indian legal frameworks in protecting women's privacy in digital spaces. Its purpose is to propose legal reforms that enhance the protection of women's digital privacy rights, taking into account global standards and best practices. The research objectives underscore the discrepancies between statutory provisions and their practical enforcement, offering a critical analysis of the existing legal framework and proposing enhancements to more effectively safeguard women against cybercrimes

CorrespondingAuthor
Rupaksh Sharma
virupakshsharma92@gmail.com

DOI
10.29121/shodhkosh.v5.i3.2024.2159

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Keywords: Right to Privacy, Online Protection, and Technology Facilitated gender-based violence

1. INTRODUCTION

"Privacy postulates the reservation of a private space for the individual, described as the right to be left alone"

Justice Dr. D.Y. Chandrachud

When one come across the terms for the first time, then privacy and confidentiality have numerous different meanings. It has been used in many different contexts as well as in many different circumstances in various ways. According to Black Law Dictionary, "the right to privacy" is a generic term that brings together many rights deemed to be part and parcel of ordered liberty; these rights protect people's liberty to make basic decisions relating to themselves, their families and their relationship with other people.

In a wider context, privacy has been described as the ability of a person to control the amount and the nature of information as well as time, place and circumstances under which such a person will be willing to share information with others. It means his liberty to absent himself or participate as he pleases. Furthermore, he has every right to dictate how personal information is share since it his property.

On the other side, a man right to privacy concerns his freedom from harassment; and the right to be let alone. The concept of personal control is one of the key points being considered when discussing privacy. Privacy makes it possible for one to govern on the human side that is closely related to one's personality. The capacity to define what is personally relevant is actually integral to the human mind. Personal freedom is connected to items that can be disguised depending on the level of an individual's liberty. These issues concern areas in which people reasonably have the right to privacy. Analyzing the human mind, it becomes evident that one cannot discourse the facet of mind without discoursing the facet of body. Predictably, the essence of body's integrity and mind's sanctity can in general be achieved only if the formal individual freedom and actual legal right of each man to have ground for creating individuality is recognized. The personality's inviolability would be questioned if it lacked judgment in making a trait.

2. THE IMPORTANCE OF THE RIGHT TO PRIVACY IN THE CYBERSPACE REALM

There are two types of privacy in the current world: privacy in real life peroxide by the right of an individual to control access to spaces that one occupies and time that one spends alone and in solitude and privacy in cyberspace which is equated to the act of assembling user data from a variety of sources including the World Wide Web. In the virtual world, privacy refers to the gathering of personal detail, processing, distribution, and invasion. Equating the recognition of every person's right to plan his development as a personality with the expression of personal space rights. Because of this, one can conclude that privacy is an indispensable part of the worth of people. It enables people to have their own spaces they have total freedom they cannot get in the social setting to come up with their own innovations and personality. In view the call to conformity of society it allows the individual to retain one's stand, beliefs, thoughts, speech, concepts, outlooks, selects, paradigm and decisions.

Most privacy violations are carried out by people who know the victim, whether they are friends, relatives, workmates, competitors or colleagues. There are different forms of cyber crimes and these include; Some that falls under Section 66A of the IT Act 2000 and those that are not included but are of a great concern because they are cropping up from cyber crimes on women.

3. RESEARCH OBJECTIVES

1. In order to analyses the difficulties of applying the privacy laws for women in cyberspace and to discuss the legal changes.
2. And to know why cyber violence against women has become an alarming issue in India and at the same time to check the efficiency of the laws which have been enforced in such cybercrimes.
3. To study the impact and effect of the abuse women receive online on their rights in cyberspace and to measure whether or not legal measures are enough to protect these rights.
4. In order to understand the gender aspects of cyber harassment and appraise the reaction of Indian law.
5. In order to evaluate existing legal frameworks that may be currently governing women's digital privacy and identify ways in which these may be effectively enforced.

4. RESEARCH METHODOLOGY

This paper has adopted a doctrinal research approach, and it relies on secondary source materials, which include articles, books, and legal commentaries, which address cyberspace crimes and women privacy rights in India. This study behaves an elaborate legal analysis of the existing legal provisions, judicial precedents and assesses the effectiveness of the existing laws to protect women's digital privacy rights by identifying the legal loops

5. TFGBV (TECHNOLOGY FACILITATED GENDER BASED VIOLENCE)

With the advancement in our daily lives, technology has been the reason behind the increases in gender base violence according to UN Women. Those involved in such violence have been in a habit of using different forms of technology to hurt up their targets. From recurrent intimate terrorism to new incidences of gender-based harassment, hate mobilization or disinformation, antagonizes have today moved to tech to escalate the injuries they deal. The act of technology has seen stalkers and other perpetrators of abuse easily get close to their targets since it has been made

easier. There are new types of abuse and platforms have introduced new and horrible ways of abusing women through the use of artificial intelligence to create sexual images of women. The women and girls are at this moment exposed to & threatened with gendered abuse; misogynous, and sexism online. The invisibility of the perpetrators, use of technology gadgets that enable constant contact with the victims, the permanency of content generated on the internet, the ability to reproduce content once generated, and the possibility of hundreds and thousands of people seeing the act makes online gender-based violence a novel form of violence. Digital platforms have given rise to new and concerning forms of abuse, such as the use of artificial intelligence to create sexual images of women. Despite the existing anonymity, modern Internet spaces include feminine-inflected hate speech in the form of gender-based violence, misogyny, and sexism targeting women and girls. The main differences between online gender-based violence and other forms of abuse include the invisibility of the perpetrator; constant access to the victim through connected devices, they permanency of the content; the ability to reproduce it without breaking the law, and potential exposure to hundreds or even thousands of Internet users. Private photos or other personal information that is posted on the internet with malicious intent will be used similarly in future. Furthermore, using the internet, there are possibilities of few abusive people who can be in contact with other like-minded person and in unison attack a specific user or organization (Salter, 2017). These online mobs can bombards their victims with a never ending cycle of harassing contents, many women have decided to stop using the internet.

6. RIGHT TO PRIVACY OF WOMEN UNDER CYBERSPACE-

The idea of a woman or girl's right to privacy regarding electronic media has sometimes been interpreted solely as a right to protection against sexual predators. The right to privacy was initially understood in the context of the internet era as a protection against unauthorized access to one's digital property, such as computer equipment, digital data, emails, social media accounts, intellectual property, and the like. The idea of digital privacy infringement has broadened with the development of digital communication technology to include intrusive phone calls, monitoring, and digital surveillance, and the disclosure of private information on platforms that are accessible to the general public. This was expanded even further to cover the dissemination of revenge porn through electronic media.

It may be important to understand that illegal access to the device may violate the privacy of others by either manually operating it or using the data thereby produced in an unethical manner, or by operating on a remote control basis, in addition to violating the privacy of the device owner who can access the data stored there. Thus, the reason for violating someone's privacy through electronic media might either be sexual or not.[1] Women's privacy violations can happen in a variety of ways through cybercrimes, some of which may be defined and structured under Section 66 A of the IT Act 2000, and some of which are concerning because they are developing forms of cybercrime against women and are therefore neither recognized nor defined anywhere under the IT Act 2000. Some of the ways by which the privacy of women can be infringed are as follows-

1. CYBER STALKING AND BULLYING

Cyber stalking has been traditionally construed as a behavioral misconduct in the cyber space. According to Bocij, Griffiths & McFarlane (2002) cyber stalking is " A group of behaviors in which an individual, group of individuals or organization, uses information and communications technology to harass one or more individuals. Such behaviors may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, the solicitation of minors for sexual purposes and confrontation" [2]

In India, there were no cyber stalking laws until 2013. There were huge confusions regarding what constitutes cyber stalking. Although an attempt has been made to define cyber stalking [3]which is as follows- "In one word, when 'following' is added by mens rea to commit harm and it is successfully digitally carried out, we can say cyber stalking has happened' 'In one word, when 'following' is added by mens rea to commit harm and it is successfully digitally carried out, we can say cyber stalking has happened' Additionally, it should be noted that there are two stages to cyber stalking: (a) pursuing it digitally by following the victim, gathering data about the victim, and so forth to monitor the victim to cause harm to them; and (b) communicating the threat to invade their privacy digitally.[4]

[1] Debarati Halder & K. Jaishankar, *Cyber Crimes Against Women in India* (SAGE Publications India Pvt Ltd).
[2]Halder & Jaishankar, *Cyber Crimes Against Women* at 89-102
[3] Debarati Halder & K. Jaishankar, *Cyber Crimes Against Women in India* (SAGE Publications India Pvt Ltd 2010).
[4]Ibid at 97

The Indian government introduced anti-stalking laws (containing cyber stalking as well) with S.354D, IPC in 2013, which includes these two stages of cyber stalking. The provision states, It is considered a serious offence when a man persistently follows, contacts, or attempts to initiate personal interaction with a woman despite her clear signal of disinterest. Similarly, monitoring a woman's use of electronic communication or spying on her in a way that causes fear, distress, or serious alarm is also considered an offence. Interfering with a woman's peace of mind is not acceptable and can lead to serious consequences.

Further, provisions added to these Section states Provided that such conduct shall not amount to stalking if the man who pursued it proves that. It was pursued for the purpose of preventing or detecting crime, and the man accused of stalking had been entrusted by the State with the responsibility of preventing and detecting crime; or it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or such conduct was reasonable and justified in the particular circumstances. It should be noted that, thanks to advances in information technology, the victim can also play a big role in facilitating stalking by knowingly or unknowingly
providing personal information.

The act of stalking can be done by someone who has been entrusted by the State to prevent or detect crime, or it can be done under any law or to comply with a requirement imposed by any person under the law. Additionally, such behavior can be reasonable and justified in certain circumstances. It's important to note that victims can also unknowingly or knowingly provide personal information, which can facilitate stalking. With advancements in technology, this role of the victim has become more significant.

The victim's position as the data controller in such circumstances must not be ignored. But the victim should not be held accountable for the same. Even though victims may take precautions to preserve their privacy, such as distributing their data and information solely to recognized friends and acquaintances or blocking undesired connections, these efforts may not always be successful in the internet and digital communication era. Stalking is one of the most significant methods of privacy invasion in the digital age precisely because of this reason. The stalker's use of the data or information and the reasons behind it must be considered by the police and the prosecution. The authorities must approach cases of cyber stalking from the perspective of the previously indicated two stages of stalking. Since stalking may inevitably contain intimidation as well, it becomes imperative to integrate laws like S. 503 of the IPC (criminal intimidation) and 506 of the IPC (punishment for criminal intimidation) in this process. The police should also investigate to see if the victim's data was improperly accessed during the stalking procedure. Depending on the circumstances, laws like Ss. 43, 66, and 66C must be used. The courts still need to properly analyses, evaluate, broaden, and alter S.354D as a cyber-stalking law. Because it is a bailable offence and the only available retributive punishment is a jail term that may last one year to three years and penalties, this provision is a woman-centric law that does not completely protect the victim. Only in the event of a second conviction does cyber stalking under this Section become non-bail able. Five years in prison and a fine make up the punishment. But if and when the stalker is successful in getting bail, one must realize that there are still opportunities for the stalker to return and harass (and even exact retribution for the police complaint) the victim. In countries like the United States and United Kingdom, cyber stalking pro- visions essentially carries 'no contact order' as a civil remedy to restrict the stalker from contacting the victim for a considerable period[5] . The courts in India have not got much scope to test the effectiveness of this law yet. It is expected that if the courts take up more cautious views to protect the interest of the victim can be protected.

2. REVENGE PORNOGRAPHY

Victimizing by way of revenge porn has become a common phenomenon in India now. It's important to realize that while revenge porn effectively promotes online sexual assault against women, it also inevitably entails voyeurism, hacking, and stalking. There is no explicit law in India that governs revenge porn. But as it always violates women's modesty, it may be regulated under S. 354C of the IPC (voyeurism), S. 66E of the IT Act (violation of privacy), and S. 509 of the IPC (punishment for damaging women's modesty). It's important to consider the inappropriate representation of women when evaluating revenge porn. Regulating revenge porn, however, must take into account the many forms of harassment suffered by the victim as well as the invasion of their privacy. According to Professor Franks, one of the noted fore founders of cyber civil rights movements in the United States thus noted: Prior to 2013, only three states in the US made the illegal dissemination of private sexual photos a crime. On June 21, 2015, there were twenty-three states that had legislation in place, and at least seventeen more were in the process of doing so. It's a huge step forward that so many states are treating this issue seriously. However, it is imperative to guarantee that the rules being passed are clear, based

[5] Kavita Patel & Sumit Arora, *Gendered Cyber Harassment and Indian Law: A Critical Overview* (2022).

on strong principles, and actually safeguard victims. Unfortunately, a large number of these state laws do not meet these requirements. Unacceptably many of these laws see non-consensual pornography primarily as a form of harassment than as an invasion of privacy. In order to violate these regulations, a perpetrator must act with "intent to harass or injure" the victim. Requirements with the intent to do harm are poor legislation as well as bad policy. Although some contend that such demands are necessary to assure Constitutional compliance, the exact opposite is true: arbitrary distinctions concerning motive raise constitutional problems rather than providing solutions. A law becomes vulnerable to claims of both under-inclusiveness and viewpoint discrimination under the First Amendment if it only forbids the disclosure of sexually explicit images when it is done with the intention of causing distress while permitting disclosures done with the intention of making money or providing entertainment. The necessity of a national criminal statute is evident given these and other issues with many state laws governing non-consensual pornography, as well as jurisdictional restrictions that are insufficient for this transnational crime. A federal criminal statute is important to signify society's acknowledgment and condemnation of this major transgression as well as to give a single, concise articulation of the relevant elements of the offence.

This methodology should be applied in India. So even though section S.354C of the IPC and section S.66E of the IT Act which aimed at making voyeurism or the violation of personal privacy a crime might not exactly fight revenge porn effectively. In making laws for criminalizing revenge porn, the parliament needs to consider all aspects that define revenge porn. However, when a police is informed with a complaint of revenge porn, they have to factor of applying the provisions already in place for invasion of privacy through voyeurism, the harm that may be occasioned to the woman's modesty resulting from the same and the widespread defamation that may be occasioned by revenge porn. The recent judgment passed in the case of Ankit Agarwal v.State of Uttar Pradesh[6] .The state for unlawful communication of restricted photographs to the court held that the act amounts to a violation of the right to privacy. The court was quick to point out that all such actions are in complete violation of the right to privacy as provided by Article 21 of the Indian Constitution. it must be acknowledged that these laws may not be entirely effective at controlling revenge porn. The parliament must take into account all the elements that make revenge porn in establishing laws for criminalizing it. However, when the police are contacted with a complaint of revenge porn, they must take into account applying existing provisions that cover invasions of privacy through voyeurism, the harm that can result to the woman's modesty as a result of the same, and the widespread defamation that revenge porn may ultimately cause. In the case of Ankit Agarwal v. State of Uttar Pradesh the court addressed the unauthorized dissemination of intimate images, emphasizing that such acts represent a grave infringement of privacy rights. The court reaffirmed that such actions constitute a serious violation of an individual's right to privacy, as protected under Article 21 of the Indian Constitution.

7. PRIVACY INVASION THROUGH THE USE OF FAKE AVATARS

Any digital image of the victim, which could be created by the perpetrator with or without including the victim's likeness, and which contains words related to the victim that may or may not be fully accurate or true; created by the perpetrator and placed on the internet for the purpose of tarnishing and prejudicing the character of the victim and to deceive those who come across those images as to the true identity of the victim. Fake avatars presented are as described often created intentionally from data breach or stalking to ridicule and embarrass the victims. This can be construed as erasion of privacy especially when the victim has information shared without their consent of the victim. False avatars are made through both, sexual and nonsexual motives. Examples of creating false avatars include providing wrong information about the victim in Facebook, tweeter, Instagram, Orkut or any social sites, uploading morph of images of her in any adult social networking sites, and filling wrong and damaging information against her through e-mailing, blogging, chat logging or in Whats up. Therefore, fake avatars are used not for the purpose of sexual harassment only. When a victim is offended due to the creation of defamatory pictures of any nature or fictitious identity including fake profile or sharing of private life on the social networking sites, then it can be vied as construction of fake avatar and the necessary provisions has to be made as per the circumstances arising out of the case.[7]

Therefore, when the fake avatar is formed through unauthorized access to data, through the fraudulent use of unique identification features and so on, the police officer must consider applying S.43, 66, and 66 C of the IT Act. Fully aware that the creation of an artificial avatar would not be in the best interest of the shy woman is question, the aforementioned officer may also wish to use the defamation laws including S, 499, S.500 of the Indian Penal Code. The officer in question

[6] (2021) 6 SCC 522.

[7] Halder & Jaishankar, Cyber Crimes Against Women at 102-103

should contemplate under which of the related laws should form application; these include: S. 67 (publication of electronic material that is obscene); 67A (publication of electronic material containing a sexually explicit act, etc.); 67B (publication of material involving a child engaging in or abetting a sexual act; in the case of this fake avatar is in the category of sexual offences) (voyeurism and the penalty Adding to this, the police must consider S.13 (use of child for pornographic purposes) and S.14 (penalty for using child for pornographic purposes) of the POCSO act alongside S.11 (sexual harassment) and S.12 (punishment for sexual harassment) of POCSO Act if the victim is a young girl. However, since phantom avatars may result from stalking or use of data without permission, the officer who is to apply such legal requirements for stalking or unauthorized use of data in any of the aforementioned instances must ensure that he or she reviews facts, reasons and other states carefully.

8. VIRTUAL RAPE & ASSAULTS IN THE METAVERSE-

There are considerable difficulties in protecting legal personality of avatars within the metaverse. To solve this problem many-sided approach is necessary. First of all, the metaverse platforms have to set the rules of permissible conduct and the legal means to report/act upon the violations. But the primary question here would be how to apply the existing legal theories to make individuals accountable in the context of the metaverse Recently, a related case was adjudicated in the United Kingdom, involving a minor girl under the age of sixteen—who was subjected to a sexual assault by a group of adult men within an immersive virtual environment. The virtual assault is claimed to have inflicted considerable psychological trauma on the victim, akin to that typically resulting from a physical assault. This case illuminates a pivotal aspect of virtual reality technologies: the degree to which interaction in the VR can have psychological impacts as a result of high fidelity representations the actual physical environment, as defined herein above, may afford Were any of the above did actually transpire in real life it is important to state that no actual physical sexual assault has taken place in the above narratives However were such a situation to take place on the real physical world, such as gang rape, harassment or outraging the modesty of a woman metaverse.8 Regarding the applicability of the modern legislation to this case, there is an example of the state that introduced the very first step in addressing the problem, the United Kingdom has enacted the Online Safety Act in 2023. In accordance of section 5, the online platform about an individual legal obligation to court for the safety of the users, when they are exposed to any content which is Illegal in nature and which under the purview of virtual sexual assault of a person. Communication sites must put in measures of identifying content that is malicious and any form of sexual violence in virtual or augmented reality contexts. Likewise, Section 10 outlines particular steps by which the services target to shield children from virtual rape scenes or contact, as they design and implement their services to shield children from other malicious content such as simulated sexual violence. In addition, restrictions and duties have been placed on such sites in order for them to assist officers in charge in compounding and prosecuting offenses relating to virtual sexual assault and other unlawful acts. This section justifies Legal Exploitation of existing crimes in technological or digital contexts.[9]

There have been calls from many legal academics and practitioners for new legal provisions to protecting avatars in the metaverse. Luckily enough, the metaverse is relatively new digital world in today's world and as such it is still at its nascent stage regarding legal regulations. Alas, although there are a great number of laws existing in the modern society, they might not be sufficient enough to cope with the requirements of this virtual world. Because the metaverse does not recognize geographical boundaries of a country, a single crime may trail across various countries, making work and handling problems for investigators in terms of enforcement and standardization difficult. A number of important measures in various jurisdictions in today's transforming environment of privacy legislation aim at personal data and privacy. The European Union has formulated the GDPR laws that contain the rules and regulation related to data protection and consent, organization and transparency, data subject rights which has uplifted the privacy all over the world. A CCPA is the California Consumer Privacy Act that was enacted in the United States guaranteeing the Californians' extensive rights concerning their personal information, which include requesting the data, erasing it, and refusing data sharing. India passed the DPDP Act 2023 that outlines provisions for personal data protection at a national level, which are nearer to global practices, altered according to Indian situations. This is similar to the LGPD of Brazil but the LGPD adapts the legal and cultural norms of data protection and privacy of Brazil. In Canada the legal regulation of private-sector data is ruled under Personal Information Protection and Electronic Documents Act (PIPEDA) and consent with

[8] Tanu Chaudhary, Virtual Rape By the Avatars in Metaverse: Potential Legal Issues and Remedies, Legal Service India (last visited 28/08/2024), https://www.legalserviceindia.com/legal/article

[9] Online Safety Act 2023, c. 30, S. 25 (U.K.).

accountability as the main principles. All together they are now expressing a new global standard in data protection and privacy that has been incorporated into their respective legal and cultural systems.

9. CONCLUSION

The link between cyberspace crimes and women's rights protects legal issues remain phenomenal for the present legal framework. The foregoing digital offenses are a real risk to women's privacy and dignity, which therefore call for legal reform and enforcement. Another modern type of cyber stalking is revenge pornography, which is a distribution of intimate images without the consent of the depicted person with the goal of causing her or him emotional distress. This kind of behavior not only violates an individual's privacy right but also a cult to emotional and psychological abuses. In Indian law regime, The case of Shreya Singhal v.Union of India acts as an important source where the Supreme Court talked about the concerns in connection to freedom of speech on social media, and privacy, but stressed the importance in having legal prevention of such misuse.hreat to the privacy and dignity of women, necessitating a comprehensive approach to legal reform and enforcement. Revenge pornography, a pernicious form of online abuse, involves the non-consensual dissemination of intimate images with the intent to harm or humiliate. Such conduct not only infringes upon an individual's right to privacy but also perpetuates emotional and psychological harm. In the Indian legal context, the case of Shreya Singhal v. Union of India[10] serves as a pivotal reference, where the Supreme Court addressed issues related to online speech and privacy, emphasizing the need for legal safeguards against such abuses. However, one may argue that current legislation may be insufficient to completely capture more subtle development of digital privacy infringement. Similarly, the proliferation of fake avatars in virtual environments has emerged as a significant concern. These digital impersonations facilitate deceptive practices and can be used to perpetrate harassment or other forms of abuse. The legal landscape must adapt to address these novel forms of impersonation and their implications for privacy and security.

Some experiences of sexual exploitation as virtual rape and other types of sexual violence committed within the virtual environment are also illegible within the legal framework. As the case of Ankit Agarwal v. State of Uttar Pradesh[11] reflecting the common perception this year in the regarding the privacy rights in the contemporary world, the psychological harm caused by virtual offences can mirror that of physical assaults. The above case demonstrates why it is legal to set legal traps in minimizing some of the incidences that happen in virtual realities and the victims deserved justice.

In conclusion, it should be remembered that the defense from the cyber space criminology, the crime against women, is not an easy, unending process and we should remember that it requires and appeals constant actions of the law sector. In the attainment of general legislative measures, which is underpinned by multidisciplinary understanding and global trends, only lies the privacy and individual's rights in the advancement of the community's digital resolution. Therefore it can be concluded that the changes in technology and law must both be ongoing in order to meet these challenges adequately.

CONFLICT OF INTERESTS

None

ACKNOWLEDGMENTS

None

REFERENCES-

Amisha Rerru Singh, Right to Privacy in Cyberspace, Cyber Law Reporter, vol. 1, no. 1.

Debarati Halder & K. Jaishankar, Cyber Crimes Against Women in India (SAGE Publications 2016).

Kavita Patel & Sumit Arora, Gendered Cyber Harassment and Indian Law: A Critical Overview (2022).

Kingsley Napley, Policing the Metaverse: The Reality of Virtual Sexual Offences, Kingsley Napley (last visited Aug. 30, 2024), https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/policing-the-metaverse-the-reality-of-virtual-sexual-offences#page=1.

[10] (2015) 5 SCC 1

[11] (2021) 6 SCC 522

Online Safety Act 2023, c. 30, § 25 (U.K.).

Tanu Chaudhary, Virtual Rape By the Avatars in Metaverse: Potential Legal Issues and Remedies, Legal Service India (last visited Aug. 28, 2024), https://www.legalserviceindia.com/legal/article.