REVENGE PORN AND BLACKMAILING UNDER CYBERCRIME AGAINST WOMEN IN INDIA: A SOCIO-LEGAL STUDY IN LUCKNOW CITY

Abstract

SUBMITTED TO THE
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY, LUCKNOW

FOR THE AWARD OF DEGREE OF

Doctor of Philosophy

IN

LAW

SUPERVISOR
PROF. (Dr.) SUDARSHAN VERMA
DEPARTMENT OF LAW
SCHOOL OF LEGAL STUDIES

SUBMITTED BY
IRSHAD AHMAD
ENROLLMENT NO. 160/15

DEPARTMENT OF LAW
SCHOOL OF LEGAL STUDIES
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY)
VIDYA VIHAR, RAEBARELI ROAD, LUCKNOW-226025 (U.P.), INDIA

2022

Abstract

Introduction

The development of technology has given us hope and brought enormous changes in pattern of our lives. These evolutions of Information Technology (IT) gave birth to the cyber space which became more familiar to the people, wherein internet provides equal opportunities to all without any gender discrimination to access any information, data storage, analyses etc. with the use of high technology. The revolution brought by information & technology and communication in twentieth century brought enormous changes in the way people organized their lives, economies, industries and institutions. These changes have brought enormous development in modern times and enhanced the quality of lives. At the same time, these have led to manifold problems including the problem of cybercrime. Women too are using the cyber space and they are much vulnerable to cybercrime. The physical world crime against women is now committed in the virtual world too and the crime of virtual world is known as the cybercrime against women. The women are much targeted in committing the cybercrime because of their vulnerability in cyberspace. The Information and Communication Technologies (ICTs) have replaced the lethal weapons of guns and swords in the hand of criminals with the feather touch board. The situation is further accentuated by the unpredictable nature of cybercrime, particularly cybercrime against women.

The term 'cybercrime against women' in India is mostly used to denote sexual crimes and sexual abuse on the internet, such as morphing the picture and using it for purposes of pornography, harassing women with threatening mails or messages, cyber stalking, etc. Traditional physical space crimes such as rape, molestation, blackmailing and stalking have gained new significance due to the development of information and communication technology.

Technology is the resource used by some perpetrators who target to defame women by sending obscene messages through Whats App, e-mail, and stalk women by using chat rooms, websites; and worst of all by developing pornographic videos, mostly created without their consent, spoofing e-mails, morphing of images for pornographic content by using various software available online. Popular perception predict that

women in India make most vulnerable targets on the internet and digital communication technology due to their gender and easy access of images of Indian women as porno-materials.

The issue of privacy and dignity of women in cyber space also needs more concern of the authorities, as it is the responsibility of the State to protect them. The concept of right to privacy for women and girls in relation to electronic media has often been narrowly understood as right to protection against sexual perpetrators. Art.17(1) of the International Covenant on Civil and Political Rights says, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". In ***Justice K.S. Puttaswamy (Retd.) Case,*** Supreme Court of India declared right to privacy as a fundamental right which is protected under Art. 21 of the Constitution. The victimization by way of revenge porn has become a common phenomenon in India. The revenge porn, a cybercrime against women is advanced form of the violation of right to privacy.

The accessibility of Internet-enabled devices like, computers, laptops tablets and mobile phones, as well as social media networks and social applications, which facilitates increased opportunities for some form of digital based sexual harm. In the last several years, a concept known as revenge pornography or 'revenge porn' has seen disgruntled ex-partners, without the consent of former partners, distribute private sexual images and videos on the Internet that were self-produced with the consent of those depicted. Revenge porn typically involves the use of text messaging or sexting. Sexual images and videos can include both images taken by the victim (a 'selfie') or a partner where consent was given, as well as images that have been obtained without consent through coercion or hacking a victim's devices, or through hidden video recordings, or through doctoring or superimposing the victim's face or identity with an existing pornographic image. The impetus for the distribution is the vengeance sought by an ex-partner following the breakdown of the relationship and aptly captured by the anonym 'revenge porn'.

The term 'revenge porn' was originally generated by the media to indicate that sexually explicit images were distributed without the consent of the person depicted in the pictures and videos. This term indicates that the reason for distributing such images or videos is for revenge. However, there are other motivations for distributing sexually

explicit images without the consent of the person depicted, which includes a desire to embarrass, humiliate or blackmail the victim.

The concept of revenge porn or image–based sexual abuse is extended with blackmailing (sextortion). It is not only the illegal distribution of (consensually) produced image and videos addressed, but also the creation and production thereof. Therefore, revenge porn with blackmailing is a crime.

In India the rate of cybercrime against women is ascending as per the 2016 National Crime Records Bureau (NCRB). The NCRB report 2016 states that in 2016 there has been 48,31,515 incidences of crime in India under Indian Penal Code(IPC) as well as under special laws (SLLs), which is 2.9% more than the crime incidences of 2015. Of these total crimes, the number of cybercrimes is 12317, which form 0.25% of the total crimes. This is inclusive of cybercrimes against women. The cybercrime incidences have increased at a rate of 6.3% during 2015-16 and 20.5% during 2014-15. The number of cybercrimes in India in 2014 and 2015 have been 9622 and 11592 respectively. It shows either there are not adequate laws to cover all incidences or there is lack of awareness of what constitutes cybercrime and seeking the help of law. The position becomes more critical when it comes to cybercrimes against women. The figures of cybercrime against women are not clearly available and we have to assume it from relevant Indian Penal Code and special law crimes and crimes booked under relevant sections of the Information and Technology Act 2000. Most of the cybercrime against women are included in crimes under Information Technology Act.

The number of cybercrime reported in Uttar Pradesh in 2016 is 2639 which is too low as compared to other crimes under Indian Penal Code and Special Law. This shows that there is lack of awareness as to what constitutes a cybercrime and which authority to report to. This figure is inclusive of cybercrime against women.

To facilitate smooth performance of this IT Act, 2000 several rules were also made. However, this version of the Information Technology Act 2000 suffered multiple drawbacks including those related to governing cybercrime against women. To rectify this, new amendment version of the Information Technology Act was brought in, which was made functional from 2008. Some extend to fill the gap but severely failed again to provide any effective solution for hate crime or for cybercrime against women.

As mentioned above, India does not have any consolidated focused laws on governing cybercrime against women. Similarly, the present Information Technology Act 2000 also suffered from several drawbacks, which have made the concept of cyber jurisprudence still a half- baked legal philosophy.

After *Delhi Gang Rape Case*, there has been a huge outcry over bringing out new reforms and penal provisions so as to protect to women against the crime. Therefore, in 2013, The Criminal (Amendment) Act passed and several new sections were inserted and some were amended in the Indian Penal Code such as sections 354, 354A, 354B, 354C, 354D. With the help of these new or amended provisions in Indian Penal Code, now the issues of MMS Scandals, pornography, morphing, defamation can be dealt in proper manner. But no amendment was made in the Information Technology Act, 2000 to protect women from cybercrime in cyber space.

The cybercrime against women, especially as per the researcher concern, the day by day increase of 'revenge porn and blackmailing' which has become a serious problem against the dignity of women in the Indian society. The criminal administration of justice system is also not well acquainted or equipped with digital technology to provide justice to victim of revenge porn and blackmailing and prevent them in future.

The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately, women are still defenseless in cyberspace. Indian women are not able to report cybercrime immediately as they are not really aware as to where to report such crimes or are not serious about reporting the same due to social embarrassment which they don't want to face.

Hypothesis of Research

- Revenge Porn and related offences violate the right to privacy of women victims.
- Honor related social norms prevent the women victims of cybercrime to file the case against perpetrators.
- Inadequacy of specific laws for the protection of women against cybercrime, despite the plethora of laws.

- ❖ The administration of criminal justice system is not acquainted and equipped with digital technology to provide justice to women victims of revenge porn and blackmailing and prevent such happenings.

Result of Hypothesis Tested

1. The First hypothesis of the research is that, Revenge Porn and related offences violate the right to privacy of the victims. Right to privacy is one of the precious fundamental rights conferred under Art. 19(1) (a) and Art. 21 of the Constitution of India, through the liberal interpretation of freedom of speech and expression and right to life by Indian judiciary. The researcher, while conceptualizing the revenge porn and blackmailing under Chapter III and through judicial interpretation of right to privacy under Chapter VI came to the conclusion that revenge porn cybercrime violate the right to privacy. Privacy is considered to be the extension of liberty of human beings. The protection of privacy requires the attention of state and non-state actors, where the 'informational confidentiality' is linked with the private matters like sexual integrity, autonomy on the person's body. Therefore, the second hypothesis has been proved.
2. Second hypothesis is that, Honor related social norms prevent the victims of cybercrime to file the case against perpetrators. The real fact the researcher collected the data from more than 500 respondents. After analysis the data is collected in Chapter VII. The researcher came to the conclusion that most of the respondent accepted the fact that most of the time aggrieved women always faced the apathy of family and society which blamed her for such crime, as society considered that women through her beauty, dressing sense etc, provoked the criminals to commit the crime against her. The women are both the co-partner (accomplice) and victim of the crime. The women are blamed for sexting, sharing of intimate images and other activities at social media. Therefore, the first hypothesis found proved.
3. The third hypothesis is the, inadequacy of specific laws for the protection of women against cybercrime, despite the plethora of laws. Researcher in chapter IV and chapter V discussed the plethora of laws in India and at international

level but their effectiveness to address the issue is lacking due to several reasons. Researcher under these chapters tried to find out the law addressing the cybercrime in general and revenge porn and blackmailing in specific. The researcher analysed under chapter IV traditional laws dealing specifically for crime against women i.e., Constitution of India, 1950; Indian Penal Code, 1860; Immoral Trafficking (Prevention) Act, 1956; The Dowry Prohibition Act, 1961, Domestic Violence Act, 2005; The Protection of Children From Sexual Offences Act, 2012 and Sexual Harassment of Women At Workplace, 2013 and critically analysed the Information Technology Act, 2000 *vide* amended in 2008 for protective laws for protection of women against cybercrime. In chapter VI international conventions, treaty, MoU of organizations and UN General Assembly resolution for protection of women from cybercrime specifically revenge porn and blackmailing have been discussed. Researcher found that the laws are not defining the cybercrimes adequately due to which the conviction is getting tougher for the judicial pronouncements. The reason behind is fast development of technology and the privacy policies of the internet platforms where the protection of the victim is not considered in terms of dignity and human rights but to facilitate the business model of the platforms.

There is no comprehensive law in India which can be able to deals the cybercrime against women particularly revenge porn and blackmailing. However, there are several laws but they have not considered the technicality involved while defining the crimes which provide the loophole for the escape of the accused, as the procedural aspect of the legislations is not compatible in respect of technological infrastructure and skills required for the same. Under these edges laws have not addressed the subject matter of modern development like revenge porn and blackmailing under cybercrime against women. Therefore, the third hypothesis is partially proved and partially disproved.

4. The fourth hypothesis is that, the administration of criminal justice system is not acquainted and equipped with digital technology to provide justice to women victims of revenge porn and blackmailing and prevent such happening in future. The cybercrime and its severity have been increasing day by day to combat this

crime. A technically and legally sound criminal administration of justice system is required. During the research, the researcher contacted with the police administration system which was basically the investigating authority of the crime. The decision of the judiciary is based on the inquiry report & presentation of the case before court by the police authority. The researcher during the research work contacted to various authorities of the police stations to know the process of investigation of the cases of cybercrime, particularly in the matter of cybercrime against women. The information was gathered from the police officials through the questionnaire. After discussing with the police officers in Lucknow, researcher did analysis of questionnaire in Chapter VII filled by them. In Chapter VII, the primary data with police administration collected strongly suggests that the technical skill, infrastructure and expert human resource for the same is lacking in the administrative agencies, where the police administration is the prime focus of the study. The researcher concludes that police lacks the relevant training and understanding of the technology behind revenge pornography and blackmailing to respond effectively against the crime. Therefore fourth hypothesis has been proved.

Framework of the Thesis

The whole research work has been divided into eight chapters:

Chapter I: Introduction

This chapter of introduction comprises the brief introduction and statement of problem as to the cybercrime against women especially the revenge porn and blackmailing. Researcher introduced research work and outlined research problem, hypothesis, research methodology and hypothesis testing by findings of data and the qualitative debates under the subject matter. Brief of the chapters of the research thesis is also included in this chapter.

Chapter II: Origin and Historical Development of Cybercrime in India

In this chapter, the researcher has mentioned the history of computer and various phases of development of generations of computer, how this computer development introduced the internet and invented the cyberspace where, all the computer activities are done. The criminals with the help of the computers commit the crime in the cyberspace and physical world crime deviated into cybercrime.

Chapter III: Conceptualization of Revenge Porn and Blackmailing under Cybercrime against Women

This chapter highlights the cybercrime against women in India especially cybercrime such as revenge porn and blackmailing which has been gaining much attraction now a days. The objective of this chapter is to clarify the concept of revenge porn and blackmailing. Revenge porn has the potential to severely harm victim and society as a whole, yet no research has been done as to the content of the concept. Revenge porn and blackmailing is advance form of violation of women's privacy rights and dignity. The conceptualization of revenge porn and blackmailing is necessary to be able to understand the severity of the harm caused by this offence on victim and to develop appropriate law governing specifically revenge porn.

Chapter IV: Cybercrime against Women: National Legal Perspective

In this chapter, researcher has made a detailed study of Indian laws dealing the issue of cybercrimes especially related to women. For this purpose, researcher has first provided the provisions available under the traditional laws i.e., under Constitution of India, under penal Laws and under special law i.e., The Information Technology Act, 2000 and then tried to evaluate the remedies available in the specific law dealing with the problem of cybercrime especially for the victims of revenge porn and blackmailing.

Chapter V: Cybercrime against Women: Global Legal Perspective

After going through the cybercrime against women, a national legal protection in the previous chapter; in this chapter the researcher has taken an analysis of the existing

International legal Instruments for cybercrimes related problems. Researcher has also tried to analyse the available legal protection at international level for tackling the problem of revenge porn which is adversely affecting the right to privacy in the present day and age.

Chapter VI: Judicial Articulation towards Revenge Porn and Blackmailing under Cybercrime against Women.

In this chapter the researcher has tried to analyse the decisions of the judiciary in various case laws related to privacy, decency, dignity in physical world which came to be applied to the virtual world. The researcher also analysed the cases wherein judiciary interpreted the crime of revenge porn and blackmailing through cybercrime to give justice to the victims of such crime.

Chapter VII: Analysis of Data Collected From Lucknow City Related Social Awareness and Impact of Cybercrime against Women

This chapter presents and analysed the primary data collected from the 542 participants of various colleges and universities with different academic background and it also included the analysis of the data collected from 22 Police stations in the city of Lucknow, Uttar Pradesh.

In this chapter the researcher attempted to provide an idea about the state of awareness about cybercrimes especially targeting women, considering the technological requirement and rapid development in this field. The Researcher has also tried to bring out the similarity of status and perceptions between the general crime against women and cybercrimes, through data analysis and in the form of chart and tabular representation.

Chapter VIII: Conclusion and Suggestions

This chapter is prepared on the basis of research study, certain conclusions are drawn, and some suggestions are also placed for consideration.

The revenge porn and blackmailing is one of the cybercrime against women which needs conceptual understanding and interpretation which seeks attention of the legislator to frame laws at national as well as at international level to curb this menace.

The revenge porn and blackmailing and related offences violate the rights of the women that are in general and right to privacy in particular. The privacy right in India is still in a state of infancy and evolution. The development of new technologies posed a serious threat to the citizen's right to privacy. Revenge Porn and related offences violate the right to privacy of the victims. Right to privacy is one of the precious fundamental rights conferred under Art. 19(1) (a) and Art. 21of the Constitution of India, through the liberal interpretation of freedom of speech and expression and right to life by the Indian judiciary. Privacy is considered to be the extension of liberty of human beings. The protection of privacy requires the attention of state and non-state actors, where the 'informational confidentiality' is linked with the private matters like sexual integrity, autonomy on the person's body.

In India, there is no specific law for regulating the cybercrime of revenge porn and blackmailing. Revenge porn and blackmailing is regulated by the way of various provisions of scattered laws, but it is not fully helpful for regulating the cybercrime of revenge porn and blackmailing. However, India does not have any direct law against revenge porn cybercrime.

The researcher concluded that, there was no specific multitude of supranational, international, state and regional laws, conventions, and norms concerned with the protection of privacy around the world. Which indicate that individual privacy is a universally cherished value with significant socio-political implications. Global civilization, having awakened seemingly overnight in an age of transparency, where individual privacy is more a perceived threat to communal well being than ever, now grapples with an aggressive reconfiguration of hitherto uncompromisable value.

The research find out that victims of abuse of intimate image are normally female and that the impacts of this abuse of intimate images are highly gendered. It also finds that generally there are two types of perpetrators of intimate image abuse exist. Type one perpetrators share images anonymously on large pornography sites, with motivations largely unknown, and type two perpetrators use threats to share images as part of a

broader pattern of coercive and controlling behaviour. Both types of perpetrator are predominately male. These patterns of victimization and perpetration support the need for the current intimate image abuse law to be adjusted.

As it is a well known fact that the crime of revenge porn and blackmailing are committed generally against women who are the soft target of the cybercrime, but it is a bitter truth that women victim of these cybercrime never came forward to register the case.

There is plethora of laws for the protection of women against cybercrime, but there is Inadequacy of law specific to cybercrime affecting individuals especially targeting the women. There are no comprehensive laws in India which could deal with the cybercrime against women in general and revenge porn and blackmailing in particular. However, there are several laws but they are not considering the technicality involved while defining the crimes which provides the loophole for the escape of the accused as the procedural aspect of the legislations is not compatible in respect of technological infrastructure and skills required for the same. Under these edges laws are not addressing the subject matter of modern development like revenge porn and blackmailing under cybercrime against women.

The administration of criminal justice system is not acquainted and equipped with digital technology to provide justice to women victims of revenge porn and blackmailing and to prevent them in future. The cybercrime and its severity is increasing day by day to combat this crime. A technically and legally sound criminal justice administration system is direly required. During the research, the researcher came into contact with the police administration system which is basically the investigating authority of the crime and the decision of the judiciary is based on the inquiry report & presentation of the case before court by the police authorities. The researcher during the research work contacted various authorities of the police stations to know the process of investigation of the cases of cybercrime particularly in the matter of cybercrime against women. The information was gathered from the police officials through questionnaire. After discussing with the police officers in the Lucknow, researcher did the analysis of the questionnaire filled by them in chapter VII filled by them. Where the primary data with police administration is collected is strongly suggesting that the technical skill, infrastructure and expert human resource

for the same is lacking in the administrative agencies. The conclusion drawn by the researcher is that the police lack the relevant training and understanding of technology behind revenge pornography to respond effectively against the crime.

SUGGESTIONS

1. There essential amendment should be made in The Information Technology Act, 2000 and The Protection of Children from Sexual Offences, 2012 to create revenge porn and blackmailing a new criminal offence under this Act.
2. Deterrent punishment for the proposed new offence of revenge porn and blackmailing should be inserted through amendment in The Information Technology Act, 2000 and The Protection of Children from Sexual Offences, 2012 to punish the accused of such offences. This may prevent the committing the offence in future and made an example for whole society.
3. With the changing nature of the technology, there is need to modernise the investigating agencies under Code of Criminal Procedure, 1973 empower them and facilitate cybercrime investigation activity without any fallibility.
4. "Cyber Police Cadre" should be created in every state which should be federally managed.
5. There is need of the hour to establish "cybercrime courts" in each and every district for the speedy disposal of the cases, which develop faith over judicial system.
6. Training on cyber crime against women with gender sensitization should be introduced so that the police can effectively respond to such cybercrime.
7. Free legal aid service should be provided to the women victim who fall prey to cybercrime.
8. There is a need for awareness-raising campaigns educating women and girls about cyber crime against women, their legal rights and the available support services.
9. The police administrative system should be made more well-equipped and trained in technology.
10. The "video hashing" technology is should be deployed to prevent re-uploading of content/ image/ videos.

11. Social media should deploy the Artificial Intelligence (AI) and machine learning tools to address the issues publication of intimate images.
12. Government should encourage women victims to report cybercrime when any revenge porn and blackmailing offence is committed against them.

The revenge porn and blackmailing case cannot be completely removed from the society. Complete alleviation of revenge porn and blackmailing under cybercrime against women is almost an impossible thing. But it could be mitigated by guarding themselves especially teen girls and women while using cyberspace. Some of the preventive and counter measures that can be adopt by women.

- ❖ They do not share intimate images & videos with anyone not even with their partners/ boyfriend.
- ❖ They can avoid taking explicit photos / pictures / shooting videos because these days no electronic devices are safe and it can be easily hacked.
- ❖ If any such cybercrime is committed against any women, first they should talk to their family and share the problem without any hesitation.
- ❖ If such cybercrime is committed against them, they must report the crime to the cyber police station or should file a complaint immediately at their nearest police station, give detailed information about all the crimes against them i.e., blackmail, coercion, harassment etc.
- ❖ If the image / picture or video appears on social media, immediately report it on that website and its organization. Revenge porn photo removal options are provided in most social media sites including Whatsapp, Facebook, Instagram, Twitter, Reddit, Snapchat etc. victim women can also check Cyber Civil Rights Initiative Comprehensive and learn to remove these posts online.
- ❖ Victim of revenge porn and blackmailing may ask search engines to remove the intimate image from different sites. For example, follow the instructions on the remove unwanted & explicit personal images from Google page.
- ❖ If any website has posted a picture without women victim consent and refuse to remove it, then victim can file a complaint to Federal Trade Commission (FTC) against the website and its parent organization.

- The first and foremost action should be to file a complaint with the Cybercrime cell as it will prevent the obscene material immediately from going viral. Also, it would help to find out the perpetrator in case of absence of knowledge.
- If women victim have any difficulties while filing a complaint at the police station, then she can call the National Commission for Women's helpline and explain the facts in details. The National Commission for Women will also assist with further legal matters.

Revenge Porn and blackmailing collectively are under-reported. Many were unaware of the fact that they were victimized. A culture of silence caused by victim shaming in the criminal justice system and society at large, forbid women from taking a stand. Having a defined law for these offenses would, in turn, bring recognition to these offenses. This would contribute to reducing victimization. Furthermore, there need to be provisions in the procedure in which these crimes are handled. A safe reporting system can be introduced by having trained qualified female counselors, to help the victims deal with the trauma along with, offering legal aid and counseling.