Page 181 - 190 **DOI:** *https://doij.org/10.10000/IJLMH.112458*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 1

2022

Privacy in Digital Era: Blackmailing, Revenge Porn and its Relevant Laws in India

NIMA NIKITA MINZ[1]

ABSTRACT

The Right to Privacy and technological advancement have produced a condition of great strain and conflict. This study examines how progress necessitates fresh perspectives on the nature of such a right. The extensive gathering of data, along with the intrinsic benefits of modern tech, has generated the cynical notion that privacy is gone, and we should just accept it. Private information is no longer private since it has been taken or accessed through a variety of techniques, including data mining, phishing efforts, malware distribution, botnet assaults, and credit or debit card theft. People are attacked as a result of the use of these data, with the most common methods being blackmail or revenge porn. The Indian Penal Code, Code of Criminal Procedure, Information Technology Act, 2000, the Indecent Representation of Women (Prohibition) Act, 1986, and The Protection of Children from Sexual Offenses Act, 2012 are all significant legislation to be aware of.

Keywords: *Right to privacy, digital privacy, Data Protection , Blackmailing, Revenge Porn.*

I. INTRODUCTION

We are now functioning in the "digital world," which may be defined as a period wherein socioeconomic activity is mostly dependent on data. This is a result of technological advancements and application. The key trait of this period may be summed as a spike in the volume of skilled professionals, a somewhat more transparent world in terms of connectivity and internationalization. This paradigmatic change raises new moral and professional difficulties, namely with the security of personal data, the right to privacy, which is jeopardized by the focus on dissemination of data, and the safeguard of owners interests.

Technology is a social activity that encapsulates civilizations' ability to modify them by enabling the generation and manipulation of not just material items, but also ideas, culture, and societal interactions. Privacy, on the other hand, denotes a crucial and nuanced feature of these

[1] Author is a student at Hidayatullah National Law University, India.

 [ISSN 2581-5369]

social interactions. As a result, technology has an impact on people's perceptions of privacy, and people's perceptions of privacy are a critical component in determining the path of technological growth. Either we should take into consideration this complex and subtle interrelationship between technology and privacy in policymaking, or we hazard losing to regulate the present, parallel digital and privacy booms. "The right to privacy and the protection of personal data is universally recognized. They believe in human integrity and other concepts like freedom of speech and expression and association"[2]. Indeed, they have become two of the most important human rights issues of our day. New technologies, on the other hand, jeopardize individual rights by making it easier to gather, store, analyze, and combine personal information for use by not just government agencies, but also companies.

II. DIGITAL PRIVACY

With the passage of time, the idea of privacy has changed. Individuals identify and appreciate it in diverse ways situationally. Furthermore, privacy is frequently weighed against other values, such as the security and protection of society. There is a scarcity of empirical evidence on individuals' views of various facets of privacy, particularly in relation to actual conduct. In attempt to comprehend how actual individuals perceive the privacy rights and its worth within a social model and system of basic rights, empirical study on how individuals perceive privacy, whatever they define it, is required. However, as a result of the "digital revolution," the concept of privacy has taken on a new meaning.

In general, privacy refers to the right to be left alone, as well as the freedom from interruption or intervention. The right to have some discretion over how your private data is gathered and used is known as information privacy. The easiest way to understand the notion of digital privacy is to think of it as the protection of private persons' information when they utilize digital media. When individuals talk about digital privacy, though, they frequently refer to it in terms of its relationship to Internet usage. The more a user shares on social media, the less privacy they have. All of the data and information that one publishes is linked to clusters of comparable data. As the individual proceeds to share their creative expression, it is paired with the appropriate cluster, and their speech and expression is no more just in their or their social circle's hands. Bridging social capital might be viewed as a result of this. Data becomes connected when people form new and diversified connections on social media. This loss of privacy continues until bundling (when the links between the nodes get stronger and the

[2] Gilc.org. 2022. *Privacy and Human Rights - Overview*. [online] Available at: <http://gilc.org/privacy/survey/intro.html> [Accessed 2 January 2022].

 [ISSN 2581-5369]

network becomes more homogeneous).

III. WAYS BY WHICH PRIVACY IS INVADED

The way the internet permits data to be created, gathered, aggregated, exchanged, saved, and analyzed is continually altering and altering personal data and the types of security it deserves and may get. For instance, seemingly innocuous data such as IP addresses, search terms, and websites visited may now be aggregated and analyzed to identify individuals and discover personal information about them. Information about an user is created with each usage of the internet, from info provided on social networking sites to cookies gathering user browsing history, from users transacting online to mobile phones logging location data. In certain cases, the user is conscious that they are garnering data and that it is being accumulated, but in many cases, the user is oblivious of the information trail they are leaving online, has no idea who is accessing the data, and has no authority over how their data is dealt or for what reasons it is being used.

1. **Data Mining: -** On the web, everybody leaves a data trail. Whenever anyone starts a new social media account, they are required to enter personal information such as their name, birthday, geographic location, and personal interests. Companies also gather information on user activities, such as when, where, and how people engage with their platform. Companies keep and utilize all of this information to better target advertisements to their users. Users' data is sometimes shared with third-party organizations without their approval or information.
2. **Phishing: -** It is among the most prevalent methods used by crooks to get confidential private data. A phishing assault disguises itself as a communication from a reputable company and sends it by email, text message, or phone call. "These communications persuade recipients to share user credentials, financial information, or credit card numbers. Phishing attacks frequently take the shape of social media sites"[3]. A huge phishing attempt attacked Instagram users in August 2019, acting as a two-factor authentication system and directing visitors to a fake Instagram page.
3. **Malware sharing**: - Malware, often known as malicious software, is any programme or file designed to harm a computer, network, or server. "Computer viruses, worms, Trojan horses, ransomware, and spyware are examples of malware. These harmful programmes

[3] SearchSecurity. 2022. *What is Phishing? How it Works and How to Prevent it*. [online] Available at: <https://www.techtarget.com/searchsecurity/definition/phishing> [Accessed 2 January 2022].

steal, encrypt, and erase important information, as well as altering or hijacking essential computing processes and monitoring end users' computer behavior"[4].

4. **Botnet attacks:-** A botnet is a collection of linked devices that individually operate one or more bots. Botnets may be used to launch DDoS assaults, steal data, send spam, and give the attacker access to the device and its connection. The botnet's owner can use command and control (C&C) software to manage it. Many politicians and individuals are concerned about the disruptive potential of botnets, following the Facebook phoney ad debacle and the Twitter bot catastrophe during the 2016 presidential election.
5. **Payment card fraud:-** Credit card fraud refers to any type of fraud involving a payment card, such as a credit or debit card. The goal might be to receive goods or services, or to send a payment to a criminally controlled account. In reply to a post, fraudsters follow complains on social media and publish bogus connections or mimic bankers or RBI officials, asking for private information that no lender should ask for.

IV. INTERNET BLACKMAILING

The act of threatening to publish personal data (including photographs or video) with the public, friends, or family online until a demand is satisfied is known as "internet blackmail." Online blackmail may occur in any online platform, including a website or an app. On private chat networks where photographs and videos may be uploaded, blackmailers may be more inclined to make threats. They may, however, threaten to disclose information or photographs on more public social media platforms, such as their favorite. Blackmailers often begin their internet blackmail against young people by persuading, deceiving, or coercing them into revealing nude photographs of themselves. They may, for example, claim to have hacked their cameras or computer histories and possess sexual photographs or humiliating information. Once they get the information, they threaten to make it public unless they are paid or more photographs are provided. Because they are terrified of the repercussions of carrying out the threat, young people will frequently strive to satisfy the expectations. When a young kid refuses to cooperate, the criminal has followed out his threats in some circumstances, but not in others. When a hacker gets hold of an user's computer, a lot of Online blackmailing begins. The hacker then looks for incriminating data that he may being used against the user and manipulate their behaviour, culminating to a ransom demand. Sexually compromising pictures or recordings are frequently sought by the attacker. Instead of hunting for pre-existing embarrassing material on

[4] SearchSecurity. 2022. *What is Malware? Definition from SearchSecurity*. [online] Available at: <https://www.techtarget.com/searchsecurity/definition/malware> [Accessed 2 January 2022].

computers, attackers have merely seized possession of the victim's webcam and recorded compromising recordings, which they then use to blackmail the victim.

During the recent decade, India has seen an increase in cybercrime and sextortion, which is basically blackmail for sexual benefit. Sextortion is frequently carried out by a blackmailer who has access to an user's private videos or images. Victims are blackmailed for money, sexual favours, or more compromising material, with the threat that if they do not cooperate, the blackmailer would disclose the content they have on the internet. Retaliation pornography is quite prevalent when one spouse saves explicit material from a relationship. Victims are usually compelled to stay in relationships because to the risk of those explicit photos/videos being released online. People are routinely blackmailed by altering photos of their faces to make them look like sexual objects. "Sextortion and revenge pornography are commonly mixed with cyber-stalking. Social networking platforms and dating websites have a significant impact on these types of crimes"[5]. Because users of video-calling apps are unaware that they are being filmed, they add to the danger. There are mobile applications that record WhatsApp video and audio chats, apps that have accessibility to all of the material in one's phone gallery (such as games, photo-editing apps, and social networking apps), and data recovery tools for formatted phones. Lack of understanding of such phone applications and tech-based skills is one of the most prevalent reasons individuals become victims.

V. REVENGE PORN

Revenge porn refers to the non-consent or non-consensual distribution or online publishing of sexual or intimate material, such as images and films of a former partner, typically with private details attached, with the purpose to injure or destroy the person depicted. This crime received its name from a disturbing trend of deserted boyfriends or ex-girlfriends publishing images of women who had broken up with them on social media. It also includes photos that have been released by outsiders who may have hacked your phone, laptop, or cloud storage account. The impact of revenge porn on a victim's relations, career, and mental health may be devastating. This is a new occurrence in terms of abusing people and then blackmailing them. In India, getting justice for victims of revenge porn is a long and difficult process. Although incidents of revenge pornography do not usually reach the news, it is a country where rape tapes are widely distributed and sold. Revenge porn is just another way to scare women and exact vengeance on women who have abandoned them.

[5] National Institute of Justice. 2022. *Ranking Needs for Fighting Digital Abuse: Sextortion, Swatting, Doxing, Cyberstalking and Nonconsensual Pornography*. [online] Available at: <https://nij.ojp.gov/topics/articles/ranking-needs-fighting-digital-abuse-sextortion-swatting-doxing-cyberstalking> [Accessed 2 January 2022].

In basic terms, it's more like image-based sex assault, which is more commonly referred to as revenge porn. Even by pornographic standards, participation needs two willing individuals, so revenge porn is not consensual. It usually occurs between partners who, while their relationship was well, exchanged private or intimate photographs and videos, which were subsequently used as blackmail or done out of spite to injure the other person after a break or quarrel. As a result, when the relationship becomes tense, one of the former partners threatens or blackmails the other by releasing the photographs or videos publicly or to their friends and family.

Sharing content online or offline, such as uploading and sharing on the internet, adult websites, social media, and email, is one example of non-consensual pornography. The motivation might be as simple as emotions of betrayal or the desire to retaliate for pain that has been inflicted on them. This, however, does not excuse such behaviour. People who engage in such behaviour frequently have a bad reputation and lack empathy for others.

In today's digital era, it has become a simple approach for males to fulfil their weak egos and masculinity by punishing women. Many rapes and sexual assault videos are purchased in this way. Our patriarchal society's social concept has led to males punishing women for being in relationship, promiscuous, leaving them, or even refusing sex while in a relationship. Despite the fact that this revenge instrument is gender-neutral, women are disproportionately targeted.

Because revenge pornography has still not been recognized as a crime in India, there are no official data on it. It does, however, exist and is really genuine. As per data from the National Crime Records Bureau, there was a 104 percent increase in the quantity of obscene information shared online between 2012 and 2014. Only 35% of affected women reported their cases, according to a 2010 cyber-crime report, and 18.3 percent of women were unaware that they had been abused.

“The concerned minister of Law and IT recently spoke at an Internet and Mobile Association of India (IAMAI) event about revenge porn creeping in India, as well as other forms of online abuse in popular platforms used to manipulate, shame, and intimidate individuals by sharing their sexually explicit content”[6]. “According to a poll performed by the Cyber & Law Foundation in India, 27 percent of internet users in India aged 13 to 45 had been victims to such cases of revenge porn”[7].

[6] iPleaders. 2022. *What to do if you are a victim of revenge porn - iPleaders*. [online] Available at: <https://blog.ipleaders.in/victim-revenge-porn/> [Accessed 2 January 2022].
[7] Action Against Violence. 2022. *Revenge Porn: Prosecution Under the Current Indian Legal System*. [online] Available at: <https://www.actionagainstviolence.org/revenge-porn-prosecution-under-the-current-indian-legal-system/> [Accessed 2 January 2022].

 [ISSN 2581-5369]

State of West Bengal v. Animesh Boxi, a 2018 case, was India's 1st instance of revenge porn, in which the defendant was sentenced to five years in jail and fined Rs.9000 for publishing and sharing private photographs and recordings of his ex-partner without her permission as revenge porn. In the case of Subhranshu Rout v. The State of Odisha, which was just decided.

VI. PROVISIONS RELATED TO BLACKMAILING AND REVENGE PORN INDIA

(A) Indian penal code (IPC)

- ***Section 120B***: This section concerns with perpetrators who commit a criminal conspiracy, which is a crime punishable by death, life imprisonment, or stringent prison term of two years or more, and is also punishable by imprisonment for a year not exceeding six months, a fine, or both if someone is a party to it without committing it.
- ***Section 292:-*** Anyone who posts or threatens to expose personal and incriminating pictures of another person through any technological means, including applications and other social media platforms, is violating the law.
- ***Section 354 (A to D):-*** It specifies the penalties for several forms of sexual crimes.
- ***Section 384*:-** Extortion is penalised by any type of imprisonment, up to three years in jail, a fine, or both. Under this rule, the punishment is three years, and the offence is not bailable in any Magistrate.
- ***Section 406***: For perpetrating a criminal breach of trust, the offender faces up to 3 years in jail, a fine, or both under this law.
- ***Section 499***: This section enables individuals to file a defamation suit, with the following criteria: whoever makes or discloses any imputation concerning any person with the intent to harm, or realising or to have reason to believe that such imputation will harm, that person's public image, is said to defame that person, except in the cases hereinafter presumed.
- ***Section 500:*** This establishes the penalty for defamation, which is a non-cognizable crime. It specifies that anybody who engages in defamation will face a one-year sentence, with the possibility of a two-year sentence, as well as a fine.
- ***Section 503***:- "Whoever jeopardizes another's person, prestige, or assets, or the individual or reputation of anyone in whom that person has an interest, with the purpose to alarm that person, or to ignore to do any act that that person is legally

obligated to do, as Criminal intimidation can lead to a penalty of up to two years in prison, a fine, or a combination of the two..

- ***Section 506:*** It establishes a penalty for the commission of criminal intimidation, which includes a two-year jail sentence, a fine, or both. If the accused threatens the victim with death, serious bodily harm, or damage of property, or if the accused imputes unchastity to a woman, the accused faces up to seven years in jail, a fine, or both.
- ***Section 509***: This section discusses the penalties for a male who tries to offend a woman's modesty through words, gestures, noises, or items, intending for it to be seen or heard, thereby invading the woman's private. A person who does so will face a sentence of up to one year in jail, a fine, or both.

(B) Under the Information Technology Act, 2000

- ***Section 66E***: This part of the IT Act of 2000 deals with the penalties for violating an individual's privacy. The section's elements demand that intimate images of the victim's private body part be purposefully captured, published, or transmitted without their permission. Such criminals face a maximum sentence of three years in prison or a fine of not more than two lakh rupees, or both in some situations.
- ***Section 67***: This section deals with publishing or sending obscene and pornographic information by electronic means, and the offender faces a maximum sentence of 3 years in jail and a fine of Rs.5 lacs, with a maximum sentence of 5 years in prison and a fine of Rs.10 lacs if it is a second offence.
- ***Section 72***: Breach of secrecy and privacy is punishable under this law.

(C) Under the Indecent Representation of Women (Prohibition) Act, 1986

- ***Section 4*** forbids the act of publishing or mailing books, pamphlets, distribution, selling, letting for hire, or circulation in the form of paper, slide, film, writing, drawing, painting, or picture featuring obscene representations of women.
- Violations of Section 4 are punishable under ***Section 6***, with the criminal facing a period of incarceration as well as a fine.

(D) under Code of Criminal Procedure (CrPC)

- ***Section 108(1)(i)(a)*** :- The victim has the authority to contact the local magistrate and tell him or her about the individual she believes is distributing obscene material. The

magistrate has the power to hold such people in custody and force them to sign a bond forbidding them from spreading the information. The accused may be deterred as a result of this. Because the victim can submit a complaint with the magistrate without giving any specific proof against the perpetrator, this is a swift redress section.

(E) Other laws that control sexual assault include the Protection of Women from Domestic Violence Act of 2005, which was designed to offer relief to women who have been subjected to domestic violence. The Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013, protects women at work from sexual harassment; Section 376(2) refers to rape as a result of abuse of authority in particular cases; The Protection of Children from Sexual Offenses Act of 2012 was enacted to address the issue of child sexual exploitation..

VII. CONCLUSION

Modern technologies have not "generated" issues to privacy: in the case of online social networks, communication within the framework of "social networks" occurs even without them. Information communicated with friends or coworkers in the usual manner may be "leaked" by one of them, resulting in gossip, rumours, and other negative consequences. However, the sheer volume of individuals active in online social networks gives rise to additional characteristics: whereas conventional information routes are confined to a well-known set of people, making the "leak" traceable, the international web is open to anybody with a basic degree of technological understanding. Even if the information is confined to a small set of users, it can be exploited by others for financial, political, or personal gain. Personal responsibility is required while using contemporary technology, but this can only be achieved via ICT literacy. As a result, innovation in the realm of privacy, particularly in relation to new technologies, need novel legal and political frameworks to guarantee that the consequences of ICT are not only understood, but also effectively managed. This effort is frequently jeopardised by a lack of knowledge of privacy as a concept, as seen by the numerous methods in which privacy is treated and assessed.

*****

 [ISSN 2581-5369]

VIII. BIBLIOGRAPHY

- Agre, P. and Rotenberg, M. eds., 1998. *Technology and privacy: The new landscape*. Mit Press. https://pages.gseis.ucla.edu/faculty/agre/landscape.html
- Berman, J. and Mulligan, D., 1998. Privacy in the digital age: Work in progress. *Nova L. Rev.*, *23*, p.551. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1418&context=nlr/
- McStay, A., 2017. *Privacy and the media*. Sage. https://books.google.co.in/books?hl=en&lr=&id=fJNBDgAAQBAJ&oi=fnd&pg=PR1&dq=PRIVACY+in+digital+media&ots=Smbh2mdwSB&sig=leTcw4ZOydASi2kWAFRAYM0V3D8&redir_esc=y#v=onepage&q=PRIVACY%20in%20digital%20media&f=false
- Park, Y.J., 2013. Digital literacy and privacy behavior online. *Communication Research*, *40*(2), pp.215-236. https://journals.sagepub.com/doi/pdf/10.1177/0093650211418338
- Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A. and Beaton, M., 2013. Teens, social media, and privacy. *Pew Research Center*, *21*(1055), pp.2-86. http://assets.pewresearch.org/wp-content/uploads/sites/14/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.

*****