© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1717122

Sextortion as an Emerging Cybercrime: An Analysis of Legal Gaps in the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023

DEEKSHA UPADHYAY[1], SWARNIM CHAUDHARY[2]
[1]*Quantum University*
[2]*Assistant Professor, Quantum University*

Abstract- ***Victims often find themselves trapped in financial pressure after being threatened with leaked private photos. That stems from predators using threats of exposure to extract money or demand new content, tactics rooted in emotional manipulation rather than actual data breaches. Even though Indian laws don't name sextortion as its own offense, rules under the information Technology Act, 2000, and the bharatiya Nyaya Sanhita, 2023, are used loosely to catch similar acts. As it happens, this leads to cases being mislabeled or dropped entirely because the exact nature of the harm isn't clearly defined. The legal system fails to offer clear direction when handling these offenses. So this gap means investigations stall and prosecutors struggle to build strong cases against perpetrators. A recent review shows how courts apply existing sections without creating special procedures for sextortion-specific harms. Without dedicated statutes, victims end up handling a maze of conflicting interpretations instead of receiving consistent support during trials. The article finds that the current laws are incapable of fully handling sextortion issues and strongly advocates for developing a more integrated, clearly articulated, and victim-friendly legal system in India.***

Keywords- ***Sextortion Coercion, Cyber Exploitation Privacy, Information Technology Act,2000 Bhartiya Nyaya Sanhita, 2023***

I. INTRODUCTION

Sexual extortion or sextortion is a form of cyber coercion where people are threatened that sexual or intimate materials will be exposed if they do not comply with demands for money, sex, or behavior. It is slowly becoming recognized as a form of image-based sexual abuse and technology-driven sexual violence, i. e. the use of digital platforms to control and harm. In this context, sexual exploitation refers to the use of threats, coercion, or blackmail to obtain sexual favors, images, or videos.Such cases may take place in different contexts and be perpetrated by people who are either known or unknown to the victim. For instance, an abusive partner may threaten to share private images as a means of preventing the victim from leaving the relationship, seeking custody of children, or relying on the legal system for help. It is a part of a controlling and dominating cycle that results in the victim being psychologically and emotionally hurt.

According to Indian judiciary, sextortion does not find a clear mention as a criminal offence. The Information Technology Act, 2000 along with reception of Bharatiya Nyaya Sanhita, 2023 to some extent, deal with it, but only through a scattering of different provisions. In fact, this primary issue of classification becomes quite complex as per the indivisibility of the rules at the same time one of the problems with enforcement is the lack of uniformity.
The paper basically attempts to examine whether the existing statutory measures are in force to effectively target sextortion or are these still based on usurping/overstretching of some sections which nevertheless, have some loopholes, legally-speaking? At present, the paper explores the way offences are categorized, the manner of conducting investigations, movements of cases in the court, and the rights and protection of victims as well. As a bonus, the authors are wondering whether the law rightly identifies sextortion as a combination of a cybercrime and sexual exploitation? The compound inherently involves studied doctrines, court decisions, and principles that are currently applicable in India. There is no question of fieldwork or real-time data. Just trying to explore the "internal composition" of Indian legal system as a result of which expose legal lacunae

and request new set of decisive rules that will help tackle sextortion in India in a most proper manner.

II. LITERATURE REVIEW

Sextortion is a problem on the internet. It is when someone threatens to share sexual pictures or videos of another person unless they do what the person wants. This can include giving them money, pictures, or videos, or doing something sexual. Sextortion is a type of cybercrime that is getting worse [1]. People are starting to realize that sextortion is a part of a problem called image-based sexual abuse [2]. This is when someone uses pictures or videos to hurt or control someone else. There is not a lot of research about sextortion, even though it is getting more common [3].

Some studies have looked at what's happening with sextortion. They used news reports and court cases to try to understand what was going on. These studies did not have enough information to really understand the problem. More recent studies are trying to learn more by looking at what victims say about who the people are that are doing this and how they are using them.

technology to hurt people. Sextortion is done by different types of people. Some are individuals who target kids, some are groups of people who want to make money, some are partners who are being mean, and some are big groups that work across many countries [4]. These people use media, dating apps, and messaging services to find their victims. They use tricks like pretending to be someone hacking or being very nice to get what they want [5]. People who do sextortion have many different reasons for doing it. Some want money, some want sex, some want power. Some want revenge. Often, sextortion is connected to types of cybercrime like romance scams or identity theft. This makes it very hard to stop. The people who are victims of sextortion are very hurt by it. They can feel anxious, depressed, and alone. Even think about killing themselves [6]. They are often very ashamed. Scared that people will find out. This makes it hard for them to tell anyone what is happening.

There are also problems with the law. Many places do not have laws that specifically deal with sextortion. This makes it hard for police to catch the people who are doing it. In India, cases are often handled under provisions of the Information Technology Act, 2000, and the Indian Penal Code, 1860[7].To stop sextortion, we need to be smarter about how we use the internet. We need to know how to protect ourselves and be careful about what we do. We also need to make sure that people who are victims of sextortion are not afraid to tell someone. In the end, sextortion is a growing problem. We need to do research and come up with better laws to stop it. We need to help the people who are victims and make sure that the people who are doing it are caught and punished. Sextortion is a type of cybercrime that we need to take seriously.

We need to keep talking about sextortion and how it is affecting people. Sextortion is a problem that is not going away. We need to keep working to stop it. Sextortion is a type of cybercrime that's very bad, and we need to do something about it.

III. RESEARCH METHODOLOGY

This research adopts a doctrinal method as its main approach for studying the question of whether the Indian legal system is capable of dealing with the crime of sextortion. It relies on secondary materials such as legal texts, court rulings, academic literature, and official reports.

This work concentrates on the dissection of the major clauses relating to the Information Technology Act, 2000, and Bharatiya Nyaya Sanhita 2023, which are at present the main legislations consulted in sextortion cases. The paper weighs up whether these laws really make sextortion a punishable crime, or whether they handle it only as a collateral effect within a disintegrated legal framework. Court rulings are used to get a fresh look at how judges see these matters.

An evaluative and interpretative method is taken to highlight the law-making gaps, contradictions, and the difficulties in implementing the law that the absence of a special sextortion provision brings about.

The research also examines how these loopholes affect the different aspects of the functioning of the legal system in the context of sextortion cases, i.e., investigations, trials, and victim support. Even though the main emphasis is on the Indian situation, a few comparative points have also been made. This is a paper-only study without any fieldwork, designed to find out how well the present framework works.

IV. CASE LAWS

Indian courts have clearly acknowledged the rising threat of sextortion as a cybercrime in their latest judicial pronouncements. In X v. State (NCT of Delhi) 2024, the Delhi High Court termed sextortion as a "major social evil", stressing that such crimes breach a person's privacy and dignity in the online world. Besides, the Court pointed out that sextortion is largely perpetrated through organized cyber networks and there are cross-border elements in it, which indicate its changing and complicated character as a cybercrime. This judgment practically demonstrates that sextortion is not just a private matter but a serious public issue that necessitates strict legal measures.

Just like that, in State of Haryana v. Jaibuna (2025), the Punjab and Haryana High Court referred to sextortion as "a much terrifying and inhuman breach." The Court made a point that offenders use digital platforms to secretly record or change the faces of victims and then blackmail them, usually for financial benefit. This decision directly relates to the technological aspect of sextortion, demonstrating how offenders leverage online tools not only to reach victims but also to carry out the criminal acts. It also shows how the judiciary has been uncompromising in refusing bail, thereby understanding the seriousness and the large-scale effects of these crimes. Moreover, in Captain Rakesh Walia v. State (2025), the Supreme Court of India responded to the issue of sextortion allegations being misused as a method of extortion. The Court dismissed the matter, among other things, pointing out that making false allegations can also be a form of coercion. This judgment is very important in that it brings out the dual nature of sextortion one hand, it is a real cyber crime causing substantial harm to privacy; on the other hand, it is a possible weapon of abuse. Indeed, it is important to highlight that the law needs to be applied cautiously and in a balanced way when dealing with incidents of this nature. In aggregate, these cases underline that sextortion is an endlessly changing form of cybercrime that leads to serious breaches of privacy, the wrong use of technology, and the law becoming extremely complicated. The courts' remarks indicate that the issue is becoming increasingly known and that there is a definite need for the development of legal systems capable of dealing with it effectively.

V. FINDINGS AND OBSERVATIONS

The research on sextortion as a new type of cybercrime shows that it is an offence that is growing very fast due to the increasing use of digital platforms like social networks, communication apps, and online dating websites. One major point is that criminals use the cover of anonymity and the help of technological means to find their victims, often by creating false identities, hacking, or through deception. Another essential point is that the reasons for sextortion are quite different. Some of them are making money, sexual abuse, getting revenge, and the feeling of having power. Besides, this crime is usually connected with other online crimes like identity theft and online scams, which make it harder for the authorities to solve them. The victims suffer from such psychological effects as stress, depression, loss of social contact, and, if things get really bad, they may even start thinking about suicide. Moreover, because they are afraid of being stigmatized and their reputation being ruined, a lot of victims do not report to the police, which makes the job of law enforcement even more difficult.

Legally speaking, even though laws like the Information Technology Act,2000[8] and the Bhartiya Nyaya Sanhita,2023[9] offer some solutions, sextortion is not directly covered by any specific regulation. This underlines the necessity of enhanced legal structures, increased understanding, and more robust preventive and investigative tools to fight against this escalating form of cyber menace.

VI. SUGGESTIONS AND RECOMMENDATIONS

To effectively address sextortion as an emerging cybercrime, legal, technological, and social measures need to be combined. If an important legal measure is the enactment of laws specifically defining and punishing sextortion as an offence, instead of depending entirely on the Information Technology Act, 2000, and the Indian Penal Code, 1860, for enforcement. Clearer definitions and harsher penalties would help in better enforcement and also serve as a deterrent. Besides, there is a requirement for augmenting cyber policing by imparting specialized training to police to handle digital evidence, investigate offenders, and provide a victim-friendly approach. Establishing fast-track courts for cybercrime cases can also ensure speedy justice. Furthermore, partnerships among different countries should be intensified for combating global sextortion operations. Awareness and knowledge of digital tools are very important factors in prevention. Schools should run programs giving children and other users information about staying safe on the Internet, protecting their privacy, and the dangers of sharing personal content. Social networking sites need to implement more powerful security features, such as improved monitoring of the content and quick reaction to reports of abuse.

In addition, victim support should be enhanced through confidentially maintained services, counselling, and simple reporting mechanisms. A main factor in the fight against sextortion and its decrease will be the empowerment of victims so that they can lodge reports without the fear of facing stigma.

VII. CONCLUSION

To sum up, sextortion has turned into a very serious and changing type of cybercrime that significantly threatens the privacy, dignity, and mental health of individuals. Besides that, the rapid growth of digital technology and online communication platforms has enabled offenders to exploit anonymity and technological means to target victims belonging to different age groups and even from different geographical areas. This paper demonstrates that sextortion is not just a legal problem but also a social and psychological issue, as it has a strong impact on the victims and, in most cases, the victims don't report the crime because of fear, shame, and stigma. On the other hand, although legal provisions such as the Information Technology Act, 2000, and the Indian Penal Code, 1860, offer partial protection, they are still not completely capable of tackling the varied aspects of sextortion. Therefore, it is a clear indication of the significant necessity for more targeted legislation, enhanced enforcement mechanisms, and better coordination at both national and international levels.

At the same time, awareness of digital literacy and responsible online behavior is very significant in the prevention of such crimes. Counselling of victims should also be prioritized. It is also necessary to create an environment where victims can report their cases without any fear of facing the consequences. In general, sextortion is a form of cybercrime that is increasing, and it calls for a well-thought-out and non-reactive method involving legal changes, security, and raising awareness of society to effectively fight and lessen it.

REFRENCES

Danielle Keats Citron & Mary Anne Franks, Criminalizing Revenge Porn, 49 Wake Forest Law Review 345 (2014).

Nicola Henry, Asher Flynn & Anastasia Powell, Image-Based Sexual Abuse: A Study of Victims and Perpetrators, Australian Institute of Criminology (2018).

United Nations Office on Drugs and Crime, Cybercrime and Online Exploitation Report (2021). Federal Bureau of Investigation, Sextortion: A Growing Threat and Prevention Advisory (2022). National Crime Agency, Emerging Threat Assessment: Sextortion (2019).

Internet Watch Foundation, Annual Report on Online Sexual Exploitation (2021). Europol, Internet Organised Crime Threat Assessment (IOCTA) (2020).

National Commission for Women, Cyber Crimes Against Women and Awareness Report (2022). Information Technology Act, 2000.

Bharatiya Nyaya Sanhita, 2023. Indian Penal Code, 1860.
X v. State (NCT of Delhi), 2024, Delhi High Court.
State of Haryana v. Jaibuna, 2025, Punjab and Haryana High Court. Captain Rakesh Walia v. State, 2025, Supreme Court of India.
Ministry of Electronics and Information Technology, Cyber Safety and Awareness Guidelines (India).

[1] Danielle Keats Citron & Mary Anne Franks, Criminalizing Revenge Porn, 49 Wake Forest Law Review 345 (2014).

[2] Nicola Henry, Asher Flynn & Anastasia Powell, Image-Based Sexual Abuse (2018).

[3] National Crime Agency, Emerging Threat: Sextortion (2019).

[4] Federal Bureau of Investigation, Sextortion: A Growing Threat (2022).

[5] Europol, IOCTA Report (2020).

[6] Internet Watch Foundation, Annual Report (2021).

[7] Information Technology Act, 2000; Indian Penal Code, 1860.

[8] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000