INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"SYNTHETIC HARM, REAL CONSEQUENCES: DEEPFAKE SEXUAL ABUSE AND LEGAL INADEQUACIES IN INDIA"

AUTHOR – SHELLY TOMAR, STUDENT AT AMITY INSTITUTE OF ADVANCED LEGAL STUDIES(AIALS), NOIDA

BEST CITATION – SHELLY TOMAR, "SYNTHETIC HARM, REAL CONSEQUENCES: DEEPFAKE SEXUAL ABUSE AND LEGAL INADEQUACIES IN INDIA", *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (4) OF 2026, PG. 605-615, APIS – 3920 – 0001 & ISSN - 2583-2344.

Introduction:

This Paper investigates the emerging phenomenon of deepfake sexual abuse as a variant of digital sexual violence, the interplay between technological availability, target vulnerability, and the absence of capable guardianship in facilitating these offenses. The research reveals a troubling correlation between the increasing accessibility of deepfake technologies and the surge in reported incidents of sexual abuse, underscoring a marked vulnerability among victims, particularly marginalized groups. Moreover, this study calls for interdisciplinary collaboration among healthcare providers, law enforcement, and technologists to develop preventative measures and support systems, thereby contributing to a more comprehensive approach to addressing the repercussions of digital sexual violence. By illuminating the mechanisms that facilitate deepfake sexual abuse, the research emphasizes the necessity for policy reforms and educational initiatives aimed at reducing the vulnerabilities of potential targets and enhancing protective measures within digital environments.

The rapid advancement of artificial intelligence and machine-learning technologies has given rise to deepfakes—synthetic media in which a person's likeness is digitally altered or fabricated. While deepfake technology has legitimate applications, its misuse, particularly in the creation of non-consensual sexually explicit content, has emerged as a serious form of digital sexual abuse. Deepfake sexual abuse predominantly targets women and marginalized groups, infringing upon dignity, privacy, sexual autonomy, and psychological integrity. As advancements in technology increasingly permeate daily life, emerging digital threats such as deepfake sexual abuse have sparked significant scholarly and societal concern, marking a new frontier in the landscape of digital sexual violence. Deepfake technology, which utilizes artificial intelligence to create hyper-realistic but fabricated media, poses unique challenges that complicate traditional understandings of consent, personal integrity, and privacy in the digital sphere. This phenomenon has drastically transformed modes of harassment and abuse, as it facilitates the creation of unauthorized visual representations that can lead to significant psychological and emotional harm for victims[1201]. Despite extensive discourse regarding the implications of digital sexual violence, there remains a glaring lack of comprehensive criminological analysis focusing on deepfake sexual abuse, particularly in understanding its prevalence, mechanisms, and victim experiences. The research problem central to this inquiry revolves around elucidating the criminological factors contributing to the rise of deepfake sexual abuse and how such offenses can be explained using Routine Activity Theory. This theoretical framework posits that crimes occur in the convergence of three essential elements: a motivated offender, a suitable target, and a lack of capable guardianship. Thus, this study will aim to determine how the elements of Routine Activity Theory intersect within the context of digital spaces, leading to the perpetration of deepfake sexual abuse.

[1201] Setyowati RM, Setya Watie ED, 'MUTED GROUP THEORY Anomalies in Online Gender-Based Violence Experienced by Women Journalists' (2024) 3(1) *Journal of Social Research* 279

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The primary objectives of this research are multifaceted. First, it seeks to dissect the mechanics of deepfake technology and its implications for understanding digital sexual violence, offering a delineated framework for categorizing incidents of deepfake sexual abuse. Second, the study aims to identify and analyze the vulnerabilities of potential victims and the environmental factors that facilitate these offenses, ultimately seeking to contribute to the broader dialogue surrounding digital safety and victim protection[1202]. Additionally, it will assess existing legal frameworks to evaluate whether current laws are sufficient to address this complex crime effectively, thereby identifying potential gaps and areas for reform. The significance of this inquiry cannot be overstated. Academically, it enriches the current body of criminological literature by applying a theoretical lens to an emergent form of digital violence that has largely remained unexplored.

Deepfake Sexual Abuse in India: An Overview

Digital tools changed how people talk and interact in India, and many people now use smartphones and social media. These tools bring growth but let risks grow too, and technology keeps changing. Some people use it for bad things like deepfake sexual abuse and digital sexual violence. This crime uses images of women to make fake and harmful content, causing emotional and mental pain[1203]. It ignores consent and personal choice, making women in India easy targets. Social norms and gender bias increase the risk for them. We must stop these crimes by looking at the tech and the social rules that let them happen. Routine Activity Theory helps explain deepfake sexual abuse by looking at the conditions needed for it to occur. The theory says three things must meet: a motivated offender, a suitable target, and an absence of capable guardianship. The bad actor has malicious intent and uses digital tools to do harm. The target is often a woman whose image is used in fake ways without her consent. A lack of protection shows gaps in personal support networks and legal rules for women's rights. India has the Information Technology Act, 2000 and the Indian Penal Code. These laws do not handle deepfake tech well, and we need to update them to fight this new threat. Stopping deepfake abuse in India needs many steps, including laws, education, and tech tools. Lawmakers must improve the rules and add clear bans on faking digital photos and videos. This could mean harsh prison time or fines for people who make or share fake content without consent. Campaigns need to teach people about these tools and the importance of consent. Tech companies must help by building tools to find deepfake content. This is digital guardianship. We can use the Routine Activity Theory to guide our work and build a plan to reduce deepfake abuse. Routine Activity Theory provides a robust framework for understanding deepfake sexual abuse by dissecting the necessary conditions for such crimes to occur. According to this theory, three elements must coincide: a motivated offender, a suitable target, and the absence of capable guardianship. In the context of deepfake sexual abuse, the motivated offender may be someone who harbors malicious intent, exploiting digital tools to cause harm. The suitable target often includes women who may find themselves represented in manipulated imagery without their consent. The absence of capable guardianship highlights gaps in both personal networks that typically provide support and the legal frameworks intended to protect women's rights. In India, existing legislation such as the Information Technology Act, 2000 and the Indian Penal Code has been inadequate in addressing the nuances of deepfake technology, thereby necessitating the strengthening and updating of legal statutes to combat this emerging threat effectively. Addressing deepfake sexual abuse in India also requires a multifaceted approach that

[1202] Romanishyn A, Malytska O, Goncharuk V, 'AI-driven Disinformation: Policy Recommendations for Democratic Resilience' (2025) 8 *Frontiers in Artificial Intelligence* 1569115
[1203] Setyowati RM, Setya Watie ED, 'MUTED GROUP THEORY Anomalies in Online Gender-Based Violence Experienced by Women Journalists' (2024) 3(1) *Journal of Social Research* 279

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

encompasses legal, educational, and technological solutions. On the legal front, legislative frameworks need to be enhanced to explicitly include provisions against the manipulation of digital images and videos. This could involve severe penalties for offenders who create or distribute non-consensual deepfake content.

Current Incidence and Trends :

The spread of digital tools caused a large increase in deepfake sexual abuse, and this violence creates new problems for current laws. People use deepfake technology to make and share fake images or videos. These acts cause deep harm to victims, and women face this most often. Recent findings show gaps in laws. We need better ways to stop violence that uses technology. Examples from many places show how hard it is to stop these crimes[1204]. Some regions try to write laws against deepfakes. India recognizes these challenges. It added rules to the Information Technology Act. This shows leaders must change laws to stop deepfake sexual abuse. Research shows that technology-aided sexual violence covers many harmful behaviors. Deepfakes are a scary part of this problem. Trends show that young women suffer most. This shows larger social problems with gender and sex. Studies show that attackers use these tools to stay hidden. Holding them responsible is hard, and early data shows these harms target specific genders. Countries like India still struggle to find good ways to regulate it. Writing laws that target digital sexual violence is hard. This difficulty is a big concern. We need broad legal changes. These changes should use routine activity theory to make the digital world safer. We must look at current cases and trends in deepfake sexual abuse. We must mix criminology, technology, and law to understand the problem fully. Routine activity theory gives us a way to study events that lead to these crimes. Offenders, targets, and a lack of protection meet in digital spaces. Leaders can plan better ways to prevent crime by seeing this pattern. Deepfake misuse is growing. Countries must work together now to build strong legal systems. Some regions have strict laws against digital sexual violence. Laws from other countries can serve as models for India and other nations. They help countries improve how they fight the threat of deepfake sexual abuse. The existing literature indicates that technology-facilitated sexual violence (TFSV) encompasses a spectrum of harmful behaviors, with deepfakes being an alarming addition to this landscape. Current trends reveal a disturbing pattern where young women are disproportionately affected by the consequences of TFSV, reflecting broader societal issues regarding gender and sexuality. Furthermore, studies have shown that perpetrators often exploit these technologies under the guise of anonymity, complicating accountability measures. While preliminary data highlights the gendered nature of these harms, the legal systems in various countries, including India, are still grappling with effective regulation mechanisms. The intricacies' of implementing laws that specifically target violations rooted in digital sexual violence remain an area of considerable concern, emphasizing the necessity for comprehensive legal reforms that draw upon insights from routine activity theory to promote a safer digital environment. In examining the current incidence and trends surrounding deepfake sexual abuse, it becomes evident that an interdisciplinary approach incorporating criminology, technology, and law is essential for a comprehensive understanding of the issues at hand. Routine activity theory offers a valuable framework[1205] for analyzing the circumstances and opportunities that facilitate such crimes. By recognizing the convergence of motivated offenders, suitable targets, and a lack of capable guardianship within digital spaces, policymakers can better strategize

[1204] Kulkarni, A., "Digital Violence and Gender: A Legal and Social Analysis of Cyber Crimes Against Women," *International Journal for Multidisciplinary Research* (2025).

[1205] Setyowati RM, Setya Watie ED, 'MUTED GROUP THEORY Anomalies in Online Gender-Based Violence Experienced by Women Journalists' (2024) 3(1) *Journal of Social Research* 279

preventive measures. Moreover, as evidenced by the escalating examples of deepfake misuse, the urgency for global collaboration in crafting robust legal mechanisms is paramount.

Socio-Cultural Factors Affecting Victims and Perpetrators

The growth of tech has changed how people act regarding sexual violence. It adds a new part to social and cultural factors. Victims often stay in weak positions. Social norms and stigma stop them from reporting crimes like deepfake sexual abuse. This shame mixes with fears of social rejection or victim-blaming. It stops them from seeking justice. Many attackers use these social weaknesses. They see online anonymity as a way to commit violence without getting caught right away. These patterns keep power imbalances strong. They keep the cycle of victimization going. They make legal accountability much harder in cases of online sexual violence. In India, the legal system for cybercrimes has changed over time. Enforcement of these laws stays uneven across the country.[1206] Social and cultural views on gender and sex influence how the law works. National laws like the Information Technology Act and the Indian Penal Code try to stop tech-based sexual violence. These laws often fall behind new threats like deepfake tech. The link between laws and cultural views makes things much harder for victims. People often do not believe the experiences of women. This keeps women from reporting digital abuse. A lack of trust in the law leads to low reporting numbers. We must use legal reform, public awareness, and victim support to fix these issues. This plan matches protection with the real daily habits that allow such crimes to happen. Perpetrators of digital sexual violence have reasons deeply rooted in social values. These values often make aggression against women seem normal. People often blame victims for the choices and actions of attackers. This view creates a dangerous setting. In this setting, society allows and sometimes forgives abusive acts. Routine Activity Theory shows how attackers work. They look for targets who do not have protection. Then they commit deepfake sexual abuse without being punished. We must build a strong community response to break these social barriers. We should focus on bystander help and broad educational programs for everyone. These steps help change social norms for the better. They protect potential victims from harm. They also stop current and future attackers from using online sites for predatory reasons. In India, the legal framework surrounding cybercrimes has evolved, but enforcement remains inconsistent, influenced by underlying socio-cultural attitudes towards gender and sexuality. Laws such as the Information Technology Act and the Indian Penal Code aim to mitigate tech-facilitated sexual violence, yet they often lag behind the pace of emerging threats like deepfake technology. The interplay between legislation and cultural perceptions exacerbates challenges for victims. Societal disbelief in women's experiences can inhibit them from reporting incidents of digital abuse, while a lack of trust in legal systems often leads to underreporting. The motivations driving perpetrators of digital sexual violence are deeply rooted in societal values that often normalize aggression[1207] against women. As victims are frequently portrayed as responsible for the actions of offenders, this perspective creates a dangerous environment where abusive behaviors are not only tolerated but, at times, excused. Routine Activity Theory illuminates how motivated offenders, when encountering suitable targets devoid of capable guardianship, carry out deepfake sexual abuses with relative impunity. To dismantle these socio-cultural barriers, initiatives must focus on fostering a community-oriented response, emphasizing bystander intervention and comprehensive educational programs. Such efforts can

[1206] Kulkarni, A., "Digital Violence and Gender: A Legal and Social Analysis of Cyber Crimes Against Women," *International Journal for Multidisciplinary Research* (2025).

[1207] Setyowati RM, Setya Watie ED, 'MUTED GROUP THEORY Anomalies in Online Gender-Based Violence Experienced by Women Journalists' (2024) 3(1) *Journal of Social Research* 279

contribute to reshaping social norms, ultimately serving both to protect potential victims and to deter current and future offenders from utilizing digital platforms for predatory purposes.

Comparison with Global Context

Technology-facilitated sexual violence (TFSV) is spreading and creates large social hurdles in every country. This trend reflects various cultural and legal backgrounds. We can understand deepfake sexual abuse within a routine activity theory framework. This framework looks at the role of opportunity, motivated offenders, and suitable targets. Countries with strict technological rules often show lower rates of digital sexual violence. These regions use active laws aimed at protecting victims. Low and middle-income countries add technology fast but often lack strong legal systems. This gap leads to more cases of TFSV. Supporting laws like India's Information Technology Act and the IPC show a growing need for better protection. These laws demonstrate how different countries respond to this new and growing threat. India's laws match the situation for TFSV in other nations. The country has made progress against deepfake sexual abuse and other crimes. The Information Technology Act and new amendments like Section 66E cover privacy crimes and the illegal sharing of images. The IPC also has rules to fight harassment and exploitation. Putting these laws into practice is difficult. Social views on gender and victim-blaming create hurdles. A comparison with nations that use strong measures shows that India must strengthen its legal response. These nations use full policies against TFSV. International examples provide a standard for better local laws. They encourage a focus on the needs of the victim when dealing with deepfake sexual abuse. Fighting deepfake sexual abuse and TFSV requires many different tools. These tools include legal, educational, and technical systems. Nations must work together across the world. No single country can solve this problem alone. Differences in laws show why world leaders must talk. They should share best methods and build a combined response[1208]. Some countries give TFSV offenders harsh penalties and offer full support for survivors. These systems show how to stop crimes and help victims recover. India's changing legal system can learn from these comparisons. The country can use international lessons to fight digital sexual violence and protect individual rights. Addressing the contextual disparities in combating deepfake sexual abuse and TFSV requires a multifaceted approach that encompasses legal, educational, and technological frameworks. Globally, there exists a pressing need for collaborative efforts, as no single nation can effectively tackle this issue in isolation. The discrepancies in legal provisions highlight the importance of international dialogues to share best practices and strengthen collective responses.

Institutional and Social Deficiencies

The rapid growth of digital tech reveals large gaps in social and legal systems. These gaps relate to the rules and prevention of deepfake sexual abuse. Many nations do not have full legal systems to handle the complex nature of tech-based sexual violence. In India, for example, the Information Technology Act and the Indian Penal Code provide some protection. But these laws do not cover the details of deepfake tech or its use for sexual exploitation. This lack of rules leaves victims at risk. It shows how legal systems fail to keep up with fast-moving tech used for harm. So, the lack of strong legal steps makes these crimes seem normal. This worsens the mental and social harm to victims. Social problems make deepfake sexual abuse harder to stop. Current cultural norms often shame victims who try to get help. Many regions, like India, share patriarchal values. These values can stop people from reporting digital sexual violence. Victims fear shame or being blamed for the crime. In this situation, victims turn to family and friends for help. They use these informal networks instead of official resources. This

[1208] Kulkarni, A., "Digital Violence and Gender: A Legal and Social Analysis of Cyber Crimes Against Women," *International Journal for Multidisciplinary Research* (2025).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

choice shows a lack of trust in official systems. It shows the need for broad campaigns to teach the public. These efforts can help victims and change bad attitudes. Researchers provide little data or stories on the effects of tech-based sexual violence. This gap exists in low-income and middle-income nations. This lack of data makes the problem worse. Leaders need these facts to create good policies. Current official responses often fail to work well. People often find them hard to reach. Police may not have the training or the tools to investigate cases of deepfake sexual abuse. This leads to less help for the victims who need it. The law's wording on sexual violence might not cover the problems of digital sites. This creates more walls for victims who want justice. Non-profit groups and advocacy teams must work with the government to establish full and broad systems. These systems should handle deepfake abuse reports. They should actively teach people about the risks of new tech. We can fix these social and official gaps. Doing so can reduce the harm to victims. It will help create a safer digital world for everyone. Consequently, the absence of robust legal measures contributes to the normalization of such offenses, exacerbating both the psychological and social impacts on victims. Social deficiencies further complicate the landscape of deepfake sexual abuse, as prevailing cultural norms often stigmatize victims seeking help. Patriarchal societal values, prevalent in many regions, including India, can discourage individuals from reporting incidents of digital sexual violence due to fear of shame or victim-blaming. In this context, victims frequently rely on informal support systems, such as family and friends, rather than institutional resources. This reliance signals not only a mistrust in formal mechanisms but also highlights the need for comprehensive awareness campaigns that can empower victims and dismantle harmful societal attitudes. The dearth of qualitative and quantitative research on the impacts of technology-facilitated sexual violence, particularly in low- and middle-income countries, further exacerbates the situation by lacking crucial data necessary for informed policymaking. Moreover, existing institutional responses often fall short in terms of efficacy and accessibility. Law enforcement agencies may lack the training and resources to effectively investigate cases of deepfake sexual abuse, leading to a diminished capacity for victim support. Additionally, the legal language surrounding sexual violence may not adequately address the unique challenges posed by digital platforms, creating further barriers to justice for victims. As such, organizations and advocacy groups are increasingly urged to collaborate with governmental bodies in establishing comprehensive frameworks that not only respond to incidents of deepfake sexual abuse but also work proactively to educate the public about the potential risks associated with digital technologies. By addressing these institutional and social deficiencies, it may be possible to mitigate the harm inflicted upon victims and foster a safer digital environment.

Integration of Routine Activity Theory in Policy Design

Technology-facilitated sexual violence is complex. We must understand the social dynamics that allow these acts to happen. Routine Activity Theory (RAT) provides a way to look at these dynamics. It helps people design better policies. The theory says crime happens at the meeting of three things. These are a motivated offender, a suitable target, and a lack of protection. Deepfake sexual abuse follows this pattern. Offenders find weak spots in digital profiles. The lack of legal protection lets these crimes grow. Rules must focus on better protection. Education and awareness campaigns help potential victims protect themselves. These steps help update laws for modern problems. Current laws do not stop the rise of online sexual violence well. Traditional laws in India are behind new technology. They do not keep up with the risks of digital sexual violence. India uses Routine Activity Theory to write better policies. The legal system then

understands and lowers the risks of deepfake abuse. Lawmakers improve the Information Technology Act and the Criminal Law Amendment. New rules target the unique parts of online sexual crimes. This makes laws proactive instead of just reactive. It helps identify targets and stops offenders from finding chances to commit crimes. India studies behavior online. It looks at situational factors too. This helps create a legal plan that fixes the causes of deepfake abuse. The law holds technology providers accountable too. Using this theory in policy helps experts and police work together. Tech experts and lawyers build a plan with many parts to stop digital sexual violence. This plan strengthens laws. It helps develop technologies with built-in safety features to stop offenders[1209]. Lawmakers must provide police with tools and training. This aids their reaction to changing crimes. Constant research and data on deepfake technology guide future laws. We need to know how common these crimes are and what they cause. India builds a strong legal system that fits online life. This improves the ability to fight deepfake abuse. It protects citizens from new types of digital sexual violence. In India, traditional legal frameworks often lag behind the rapid advancements in technology and the associated risks of digital sexual violence. By integrating Routine Activity Theory into the formulation of policies, the Indian legal system can better understand and mitigate the risks posed by phenomena like deepfake abuse. For instance, the Information Technology Act and the Criminal Law Amendment can be enhanced by provisions that specifically address the unique aspects of technology-facilitated sexual offenses.[1210] This ensures that laws are not only reactive but also proactive in preventing offenses through the identification of suitable targets and minimizing opportunities for offenders. By recognizing patterns of behavior in digital spaces and focusing on situational factors, India can develop a comprehensive legal approach that addresses the root causes of deepfake sexual abuse and promotes accountability among technology facilitators. Moreover, policy design informed by Routine Activity Theory encourages collaboration between technology experts, law enforcement, and legal practitioners to create a multi-faceted approach to preventing digital sexual violence. This integrated strategy not only aims at strengthening laws but also seeks to develop technologies with inherent safeguards that can deter potential offenders. Legislators must acknowledge the necessity for ongoing training and resources to law enforcement agencies to effectively respond to these crimes as they evolve. In this regard, continuous research and empirical evidence collection on the prevalence and implications of deepfake technology will inform future legislative efforts. By establishing a robust legal framework that reflects the intricacies of digital interactions, India can significantly enhance its capacity to confront deepfake sexual abuse and protect citizens against emerging forms of digital sexual violence.

Framework for Crime Prevention Policies

Digital threats are everywhere, and we must create strong crime prevention policies now. Technology grows and digital crimes change, so our laws must change too. Tech-based violence is a major problem in sexual situations. This problem shows big holes in our laws. We need a careful way to make online violence illegal. Recent research supports this goal. New rules must fit today's world and the harms of technology. We use routine activity theory to see how offenders and targets meet without protection. We must understand this to stop digital sexual violence. India's legal system provides a clear example of crime prevention policies against digital sexual violence. India updated the Information Technology Act and the Penal Code. These changes target cyberstalking and sexual image abuse, but police do not always enforce these laws well.

[1209] Kulkarni, A., "Digital Violence and Gender: A Legal and Social Analysis of Cyber Crimes Against Women," *International Journal for Multidisciplinary Research* (2025).
[1210] Eisenhut K, Sauerborn E, García-Moreno C, Wild V, 'Mobile Applications Addressing Violence Against Women: A Systematic Review' (2020) 5(4) *BMJ Global Health* e001954

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Stopping tech-based sexual violence remains a hard task. This shows routine activity theory is hard to use in different cultures. Young women face these crimes most often, so prevention plans must find likely targets. They must also put protections in place. The link between laws and digital threats is clear. We need flexible policies that support social rules and keep people safe online. We need a stronger system for crime prevention. To build one, we must use facts from research on tech-based sexual violence.[1211] Prevention is about more than just laws, and it also requires social changes. These changes help victims and stop attackers. India should combine public education with its new laws. This will make the internet safer. Communities should act like active protectors against offenders, and doing this lowers the risk of deepfake sexual abuse. In the end, we must stop digital sexual violence. This work needs police, leaders, and citizens to work together. This cooperation makes prevention plans useful during constant digital threat changes. Such an approach must reflect not only the current realities of digital interactions but also the nuanced ways in which these technologies can perpetrate harm. Through a routine activity theory lens, understanding the convergence of motivated offenders, suitable targets, and a lack of capable guardians is essential in crafting effective preventative strategies that address digital sexual violence. The legal landscape in India offers a compelling context for analyzing the efficacy of crime prevention policies targeting digital sexual violence. Recent amendments to the Information Technology Act and the Indian Penal Code aim to address issues such as cyberstalking and image-based sexual exploitation, yet enforcement remains inconsistent. The ongoing challenges in curbing technology-facilitated sexual violence reveal the complexity of applying routine activity theory within diverse cultural and legal contexts. Ultimately, addressing the multifaceted nature of digital sexual violence requires a collaborative effort between law enforcement, policymakers, and civil society to ensure that crime prevention strategies are effective, inclusive, and responsive to the evolving landscape of digital threats.

Case Studies of Deepfake Sexual Abuse

Deepfake technology appears in digital interactions, and it changes how we see online sexual violence. This technology creates very realistic, manipulated videos that lead to many crimes involving sexual exploitation. Offenders usually target women who face fake videos that cause permanent damage to their reputations and personal lives. Deepfake sexual abuse fits Routine Activity Theory and acts as a form of technology-facilitated sexual violence (TFSV). Offenders identify easy targets on digital platforms, and these sites lack enough protection to stop them. Many cases raise hard ethical questions, and legal systems must adapt to these difficult challenges. Digital anonymity hides people, and their experiences show the need for change. Few laws address deepfake sexual abuse, but India now sees the need for new rules to match the digital threat. The Information Technology Act and the Indian Penal Code offer help by covering voyeurism and image-based sexual abuse. These laws give ways to fight offenders, yet the details of deepfakes make it hard to win in court. Artificial videos of people in sexual scenes challenge ideas of consent and harm, and law enforcement struggles to keep up. This fact shows we need better protection for victims through legal steps and public campaigns to stop offenders. Offenders look for weak spots in the digital world and use them to cause harm. Offenders target women more often, and stories from victims show we need more research. This trend matches patterns in other sexual violence online, and young women make up most of the victims. Gender-based violence meets new technology, and this meeting shows that current laws fall short. We need specific ways to handle deepfake problems and support victims. Scholars say Routine Activity Theory explains how people become victims in digital spaces.

[1211] Sheikh, M. M. R., and M. M. Rogers, "Technology-Facilitated Sexual Violence and Abuse in Low- and Middle-Income Countries: A Scoping Review," *Trauma, Violence, & Abuse* 25, no. 2 (2024): 1614–1629.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Legislative frameworks addressing deepfake sexual abuse remain scarce;[1212] however, countries like India are beginning to recognize the urgency of updating laws to reflect this digital threat. The Information Technology Act, along with provisions under the Indian Penal Code that address voyeurism and image-based sexual abuse, provides some legal recourse against offenders. Yet, the nuanced nature of deepfakes complicates prosecution, as traditional definitions of consent and harm are challenged by the artificial recreations of individuals in explicit contexts. Law enforcement agencies often find themselves struggling to keep pace with the evolving technological landscape, thereby reinforcing the necessity for capable guardianship to protect potential victims from harm. The integration of specific legal measures to combat such abuse, as well as public awareness campaigns, can serve to deter motivated offenders who exploit the vulnerabilities inherent in the digital milieu. Women, in particular, have become disproportionately targeted by these digital assaults, aligning with trends observed in broader TFSV contexts, where young women often represent a majority of victims. The intersection of gender-based violence and technological advancements highlights the inadequacies of existing legal frameworks, necessitating more tailored approaches to address the unique challenges posed by deepfakes. Scholars argue that a more effective application of Routine Activity Theory can guide both victim support networks and policymakers in understanding the dynamics of victimization within the digital realm. As such, fostering interdisciplinary dialogues that include criminology, technology studies, and legal analysis will be crucial to developing comprehensive strategies aimed at preventing deepfake sexual abuse and mitigating its effects on victims.

Notable Global Incidents

Technology keeps advancing and the way digital sexual violence works has changed. The Nth Room case in South Korea shows this shift clearly. This case involved coercion and the abuse of both women and children. It showed the dark side of cyber sexual violence,[1213] or CSV. It showed the link between these crimes and deepfake tools. These events draw global attention and show that current legal systems are weak. Many laws fail to address the specific parts of digital sexual crimes. These laws often rely on old ideas of violence and do not cover new methods. Criminals use computers, phones, and the internet to find new ways to hurt people. We must check these legal systems to protect victims and find justice. This work shows that nations need to fix their laws soon. India faces many of the same challenges as other nations. These countries struggle to keep up with fast technology changes. The Indian Penal Code and the Information Technology Act help fight online crimes. These laws cover voyeurism and sharing obscene content in digital spaces. Police do not always act fast and social stigma slows them down. Officers often lack the technical skills to help with these cases. Deepfake tools make legal work harder for everyone. Criminals use these tools to create fake pornography without consent. This helps them avoid current laws that were written for a different time. We need broad plans that look past old definitions of sexual violence. Lawmakers must update their rules to match the reality of digital abuse. They should act fast to change these rules for everyone. The world is paying more attention to deepfake abuse, but a big gap still exists between current laws and digital reality. Events like the Nth Room show that we need strong global rules to stop these crimes. Researchers look at laws in the UK, Germany, and France to find better ways to act. These studies show how different places deal with the same problems. These countries now

[1212] Sheikh, M. M. R., and M. M. Rogers, "Technology-Facilitated Sexual Violence and Abuse in Low- and Middle-Income Countries: A Scoping Review," *Trauma, Violence, & Abuse* 25, no. 2 (2024): 1614–1629.

[1213] Sheikh, M. M. R., and M. M. Rogers, "Technology-Facilitated Sexual Violence and Abuse in Low- and Middle-Income Countries: A Scoping Review," *Trauma, Violence, & Abuse* 25, no. 2 (2024): 1614–1629.

have specific rules for online sexual violence and abuse. This change shows a better understanding of consent and privacy in digital spaces. We need a broad plan to fight deepfake abuse. This plan should include new laws, tech fixes, and prevention. People must work together to protect victims. This work stops people from committing crimes in a connected world. Such teamwork is necessary for safety. In jurisdictions like India, the legal response to incidents of digital sexual violence reflects broader challenges within many nations struggling to adapt to the rapid evolution of technology.[1214] The Indian Penal Code, alongside the Information Technology Act, offers some recourse against online sexual crimes, encompassing provisions against voyeurism and the distribution of obscene material. However, enforcement remains lethargic, hindered by societal stigma and a lack of technical expertise among law enforcement agencies. Additionally, the specifics of deepfake technology further complicate existing legal structures, as perpetrators utilize these tools to fabricate non-consensual pornography, thus evading the clear applications of current laws. Notable incidents such as the Nth Room reinforce the call for robust international standards to address these crimes effectively. Comparative legal analyses, such as those examining frameworks in countries like the UK, Germany, and France, shed light on how different jurisdictions are grappling with similar challenges.

Indian Specific Cases

The rise of deepfake technology has brought new troubles to digital sexual violence in India. It creates very difficult hurdles for the legal system. The internet grows fast. This growth lets offenders use the technology. They target vulnerable people. In certain Indian cases, women face harm from deepfake images. Attackers change their images to make porn without consent. These acts break privacy rules. They keep gender violence alive. This behavior supports old hatred toward women in society. The Indian courts see that cybercrimes are bad. But the courts fail to stop these fast-changing threats. They use old laws. These laws do not cover new technology in crimes against women. Analysis of shows these shortcomings. Routine Activity Theory (RAT) helps explain why these crimes happen. RAT says crime occurs when three parts come together. These parts are a motivated attacker, a good target, and no guard. Deep patriarchal values in India drive these attackers. They believe they have a right to control women's bodies. Young women and public figures are often targets. They lack digital skills and tools to stay safe. Law enforcement and lawmakers do not act as strong guards. This lack of action makes victims more vulnerable. The legal rules must change. They must focus on online safety to guard against threats. Findings in support this. Indian laws must change to handle deepfake sexual violence. The Information Technology Act provides some help. But it lacks the exact rules to stop deepfake crimes. Lawmakers must add new parts to the Indian Penal Code (IPC). They must create laws that punish making deepfake porn. They must also punish sharing it. This will give victims a way to fight back. India should use standards from global groups like CEDAW. This will make the local legal system stronger. It helps promote gender equality and stops cyber violence. India can fix its legal system with prevention and punishment. This will provide justice for victims of deepfake abuse. It fits the plan against digital sexual violence. Moreover, the interaction between deepfake technology and Routine Activity Theory (RAT) can elucidate the circumstances that give rise to these crimes. RAT postulates that criminal behavior occurs when three elements converge: a motivated offender, a suitable target, and a lack of capable guardianship. In the Indian context, the motivations for such criminal acts may stem from deeply ingrained patriarchal values and the perceived entitlement over womens bodies. The targets, often young women or

[1214] Mohan, Chathuri C., and Febin Baby, "Women Victims of Cyber Sexual Harassment: A Study with Reference to Kerala, India," *International Research Journal of Social Sciences*, Vol. 13, no. 4 (October 2024): 13–21.

those with public profiles, become susceptible due to a lack of effective digital literacy and protective measures. Additionally, the absence of vigilant digital guardians, such as active law enforcement and legislative response mechanisms, exacerbates the vulnerability of potential victims[1215]. Furthermore, incorporating international standards set forth in conventions like CEDAW could bolster the domestic legal framework, promoting gender equality and protection against cyber violence. By establishing both preventive and punitive measures, India can align its legal system with contemporary challenges, ensuring justice and support for victims of deepfake sexual abuse as part of a broader strategy against digital sexual violence, as outlined.

CONCLUSION

The way digital sexual violence uses deepfake technology shows large gaps in current laws. This fact is clear. Many countries try to regulate online violence, but they struggle to keep up with fast tech changes. For example, the UK, Germany, and France created specific laws for online sexual violence. These laws often fail. These crimes change constantly. India uses the Information Technology Act of 2000 and parts of the Indian Penal Code to handle these issues. Deepfake sexual abuse mixes consent with tech tricks in complex ways. This fact makes it necessary to rethink current rules. This shows we need broad reforms to protect victims and stop offenders. The rise of online sexual violence shows we need active legal changes and public awareness campaigns. Recent studies show that many forms of this violence affect young women the most. We must focus more on these groups. They face higher risks of being targets. Recent movements in India raised awareness about gender violence and digital abuse. These movements force lawmakers to look at harsher punishments and better victim protections. These sources talk about the effects on specific groups. A study of deepfake sexual abuse using Routine Activity Theory (RAT) shows these crimes happen often on easy-to-use sites. This theory says crimes happen. Bad actors find easy targets without any protection. This idea fits well with online sexual violence. These lessons call for new digital policies with better ways to watch over users. We need more monitoring of online acts. We also need better ways for people to report crimes. Indian laws must change to meet these unique tests. They should use global lessons to build a stronger legal system. This system must punish criminals. It must also give victims more ways to stay safe through broad protection rules. The advent of technology-facilitated sexual violence (TFSV) reveals the importance of proactive measures in both legal frameworks and social awareness campaigns.

Furthermore, the insights gleaned from analyzing deepfake sexual abuse through Routine Activity Theory (RAT) indicate that opportunities for such offenses are routine and often facilitated by accessible digital platforms. RAT posits that the convergence of motivated offenders, suitable targets, and a lack of capable guardianship contributes to criminal activities, a concept that applies significantly in the context of TFSV. The lessons from this analysis call for innovative approaches to digital policies that incorporate proactive guardianship measures, such as increased monitoring of online behaviors and improved reporting mechanisms. Legislative frameworks in India must evolve to address these unique challenges, integrating the lessons learned from global practices to foster a more resilient legal infrastructure that not only penalizes offenders but also empowers potential victims through comprehensive protective measures.

[1215] Mohan, Chathuri C., and Febin Baby, "Women Victims of Cyber Sexual Harassment: A Study with Reference to Kerala, India," *International Research Journal of Social Sciences*, Vol. 13, no. 4 (October 2024): 13–21.