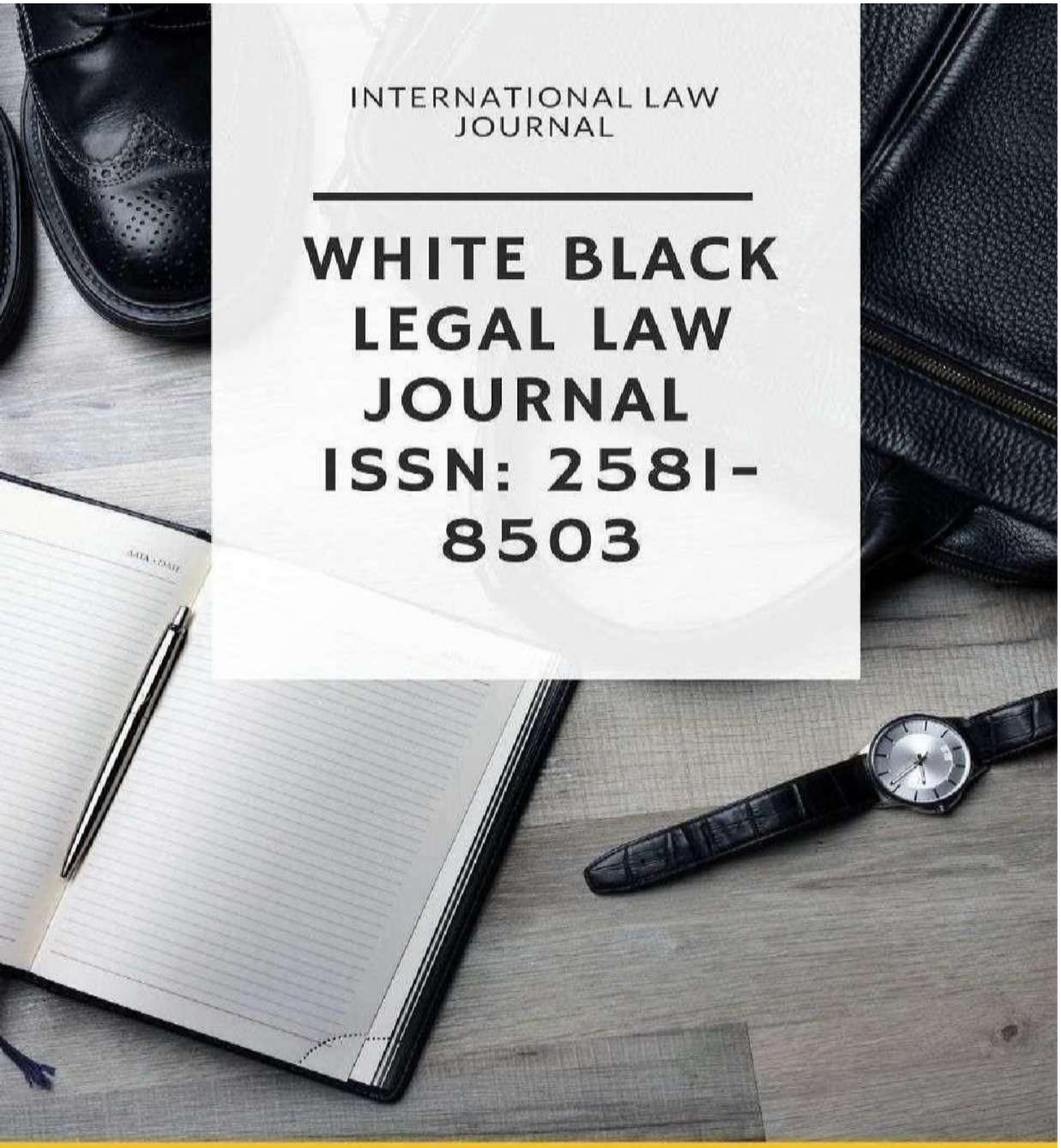

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

DIGITAL SEXUAL VIOLENCE: SOCIO-LEGAL ISSUES OF ONLINE HARASSMENT AND CYBERSTALKING

AUTHORED BY - B.GIRIPRASAD
BCA.LL.B(Hons), LL.M, Vels School of Law
Vels Institute of Science Technology & Advanced Studies (VISTAS), Pallavaram, Chennai

CO AUTHOR - B.KEERTHANA
B.A.LL.B, LL.M, Vels School of Law
Vels Institute of Science Technology & Advanced Studies (VISTAS), Pallavaram, Chennai

ABSTRACT:

Digital sexual violence has become a major social and legal problem in today's digital world, where rapid technological progress has turned traditional forms of gender-based abuse into widespread and borderless online harms. This article analyzes significant forms of digital sexual violence, such as online sexual harassment, cyberstalking, non-consensual intimate image sharing, sextortion, and AI-generated deepfake sexual exploitation, emphasizing how these actions violate dignity, privacy, autonomy, and equality. It looks at how the law and rules are changing in response to these crimes, including recent changes and court rulings that show that institutions are starting to take these crimes more seriously. However, even with these changes, there are still big problems that need to be solved, such as gaps in enforcement, limits on jurisdiction, problems with evidence, worries about platform accountability, and a strong social and cultural stigma that often keeps victims quiet. The paper goes on to talk about the difficult balance between fighting online abuse and protecting basic rights like freedom of speech and due process.(Great Britain: Parliament: House of Commons: Culture et al. 2014) The study underscores the necessity for a comprehensive framework that amalgamates consent-based legal standards, enhanced intermediary accountability, specialized investigative procedures, international collaboration, and extensive victim support systems through a socio-legal lens. It concludes that long-term prevention of digital sexual violence needs more than just changes to the law; it also needs changes to society as a whole to make sure that digital spaces are safe, welcoming, and respect people's rights.

KEY WORDS: Harassment, Stalking, Sexual Violence, Online Harassment, Sexortion, Deepfake, Online Safety.

INTRODUCTION:

Digital sexual violence has emerged as a critical human rights and legal issue in the digital age, as rapid advances in internet technology, social media, artificial intelligence and online communication have created new opportunities for harassment, non-consensual sharing of intimate material, cyberstalking and the production of sexually explicit deepfake content that inflicts profound psychological, social and reputational harm on victims (Indreswari et al. 2023). Recent changes to laws and regulations around the world show that more people are aware of these harms and the need for stronger protections. For example, the TAKE IT DOWN Act was signed into federal law in the United States in 2025. It makes it illegal to share intimate visual depictions without consent, including AI-generated deepfakes. It also requires covered platforms to set up quick notice-and-removal systems, with criminal penalties for violators and obligations on digital services to act quickly on reports of harmful content. This law aims to fill in the gaps in previous protections against revenge pornography and digital exploitation by linking removal duties to legal accountability. At the same time, the UK has changed its criminal law with new laws like the Online Safety Act 2023 and the Data (Use and Access) Act 2025. These laws make it illegal to make non-consensual deepfake intimate images and make crimes related to recording, sharing, or threatening to share intimate images without consent more serious. (Rachmawati et al. 2023)The UK is also working with tech partners to create deepfake detection systems. Changes to the Crimes Act 1900 in New South Wales, Australia, now make it illegal to make and share sexually explicit deepfakes and related audio material. This means that both the people who make and share this kind of content can be punished by law. Recent changes to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules in India have made it clear that AI-generated sexual abuse images and other illegal synthetic content are against the law. Platforms are now required to label and remove this content, and they must do so much faster than before. If they don't, they could face penalties under the Bharatiya Nyaya Sanhita, 2023 and related laws. This is a response to concerns about AI tools making sexualized images of women and children. These events around the world show that governments are more determined than ever to change their social and legal systems to deal with new types of digital sexual violence. They are trying to find a balance between protecting people's rights, privacy, and equality online and allowing

free speech and technological progress, even as more abuse and calls for more reform continue to change the legal landscape.

RESEARCH METHODOLOGY:

This study adopts a doctrinal and socio-legal research methodology to analyse digital sexual violence, particularly online harassment and cyberstalking. The research is qualitative and analytical, examining the effectiveness of existing legal frameworks. Primary sources include legislations such as the Information Technology Act, 2000, the Indian Penal Code, 1860, and the Bharatiya Nyaya Sanhita, 2023, along with relevant judicial decisions and international instruments like the Budapest Convention on Cybercrime. Secondary sources consist of books, journal articles, research papers, and government reports. The study relies on library-based research and focuses on legal gaps and enforcement challenges, with limitations arising from reliance on secondary data and underreporting of cases.

CONCEPTUALISING DIGITAL SEXUAL VIOLENCE:

To understand digital sexual violence, you need to see it as a type of gender-based harm that happens online, is made worse by technology, or is done through technology, rather than just in physical spaces (Valentine et al. 2019). It is not just "online misbehavior" or general cybercrime; it is a specific type of sexualized abuse that uses social media, messaging apps, emails, online gaming spaces, cloud storage, and more and more artificial intelligence systems to attack a person's bodily autonomy, dignity, privacy, and sexual integrity. Digital sexual violence includes things like persistent online sexual harassment, cyberstalking with sexual threats, sharing intimate images or videos without permission (also known as image-based abuse), sextortion, recording and sharing private content without permission, doxxing with sexual intimidation, and making or sharing AI-generated deepfake pornography without permission. What makes this type of violence different is that digital environments are unique. For example, anonymity lets perpetrators act with less fear of being caught; content can be copied and shared all over the world in seconds; harmful material may stay online forever; and algorithmic systems can spread abuse to larger audiences in minutes(United Nations. Economic and Social Council 2014). Digital sexual violence is an extension of structural discrimination into virtual spaces because it often reflects and reinforces existing inequalities in the real world, especially those based on gender, sexuality, caste, race, and other social hierarchies. It also causes layered harms, such as psychological trauma, damage to one's

reputation, loss of money, social isolation, and the silencing of public participation. This shows that its effects are real and deeply felt, even though they happen in a digital space. So, when we think about digital sexual violence, we need to see it as a serious social and legal problem that has to do with human rights, technology governance, and gender justice, not just as a minor online mistake.

THEORETICAL LENSES:

Scholars and policymakers utilize various interconnected theoretical frameworks to elucidate the reasons behind harmful digital behavior, its impact on individuals, and the appropriate societal responses, particularly in the context of recent legal reforms addressing non-consensual imagery and AI-generated abuse. Feminist legal theory posits that digital sexual violence is an extension of systemic gender inequality. Online harassment, cyberstalking, revenge porn, and deepfakes are not mere "technical problems" but rather manifestations of power imbalances entrenched in patriarchal norms that aim to control, objectify, and discipline women and marginalized genders. This lens stresses that the law needs to look at more than just individual acts of harm. It also needs to look at the underlying causes of these acts, such as misogyny, sexual entitlement, and gendered violence, which are still present offline and are made worse online. Second, from a human rights point of view, digital sexual violence is a violation of basic rights like privacy, dignity, equality before the law, freedom from degrading treatment, and in some places, the right to digital security. This means that countries must create protective and corrective systems that protect these rights for everyone. Third, cyberlaw and regulatory theory look at how legal systems change when technology changes, especially when new types of harm, like AI-enabled deepfake pornography and cyberflashing, move faster than old laws (Spurek 2026). Recent legal changes in the U.S. The TAKE IT DOWN Act makes it illegal to share intimate images without consent and requires platforms to take them down quickly. This shows an effort to fill in the gaps in previous cybercrime and obscenity laws by recognizing technology-facilitated sexual harm as a specific crime with responsibilities for intermediaries. The UK's Online Safety Act has also added new crimes, such as cyberflashing and threatening to share private photos, and platforms are now required to find and block unwanted sexual content. To deal with the special harms that AI-generated sexual abuse can cause, commissions in countries like India are suggesting clearer definitions and punishments for manipulated content and deepfakes under criminal law. Fourth, sociotechnical and communication theories stress how the design,

algorithms, anonymity, and affordances of digital platforms affect the creation and spread of sexually harmful content. This means that legal solutions need to be combined with technological governance and ethical design to deal with new risks. Collectively, these perspectives illustrate that digital sexual violence cannot be perceived merely as individual transgression; it constitutes a socio-legal issue encompassing power dynamics, technology, rights, and the development of legislative measures, necessitating comprehensive regulation that integrates doctrinal law, platform responsibilities, and societal standards.

FORMS OF DIGITAL SEXUAL VIOLENCE:

Digital sexual violence is a broad term that covers a lot of harmful actions that people do online, like on social media, messaging apps, email, online forums, gaming spaces, and AI tools. These actions are sexual and go against a person's privacy, dignity, freedom, and sense of safety. Here are the main types explained in detail:

1. **ONLINE SEXUAL HARASSMENT:**

   Online sexual harassment is any unwanted sexual behavior that happens on the internet. This could mean sending sexually explicit messages, unsolicited nude pictures, rude comments, repeated sexual advances, offensive jokes, sexual threats, or comments that put down a person's body or character. It happens a lot on social media, in comment sections, during live streams, and in private messaging apps.

   Sexual harassment is different from casual online arguments because it is targeted and happens over and over again. Its goal is to humiliate, scare, or silence the victim. Women, journalists, influencers, students, and people in the LGBTQ+ community are more likely to be affected. Even if the abuse is just words or text, it can have a big effect on someone's mental health, making them anxious, depressed, scared, and less likely to participate online. In a lot of cases, victims limit their online presence or censor their own thoughts because they are afraid of being harassed again.

2. **CYBERSTALKING:**

   Cyberstalking is when someone uses digital means to repeatedly and obsessively watch, track, or contact another person, causing them fear or distress. A cyberstalker might send messages over and over again, keep an eye on the victim's social media activity, make fake accounts to keep an eye on them, spread rumors, or threaten sexual violence.

Cyberstalking is different from one-time harassment because it happens over and over again. The person who did it may use technology to track check-ins, collect personal information, or change digital footprints. Sometimes, cyberstalking leads to stalking in real life or even physical harm.(Leung et al. 2023; Freeman et al. 2020) The psychological effects can be very strong because victims often feel like they are being watched all the time and are in danger. Digital platforms let people stay anonymous, which makes it harder for victims to take legal action and makes them feel more helpless.

3. NON CONSENSUAL INTIMATE IMAGE SHARING:

Image-based abuse, also known as non-consensual intimate image sharing, happens when private sexual photos or videos are shared without the consent of the person in them. These pictures may have been shared willingly in a private relationship, gotten through hacking, secretly recorded, or changed in some way.

Once this kind of content is put online, it can quickly spread to many different platforms, making it very hard to get rid of completely. The victim may feel embarrassed, lose their reputation, be socially isolated, or even lose their job. Victims, especially women, are often blamed for what happened to them in many cultures, which makes them less likely to report it. The permanence of digital content exacerbates the trauma, as victims may apprehend that the material could reemerge at any future point.

4. SEXTORTION:

Sextortion is a type of digital blackmail in which the person doing the blackmail threatens to release private pictures or videos unless the victim does what they say. These demands could be sending more explicit content, having sex online, or paying money. Sextortion often happens to teens and young adults, usually through fake dating apps or social media profiles. At first, the criminals may gain the victim's trust and get them to share private pictures. Then, they may use those pictures as leverage(Taneja et al. 2025). Hackers can also get pictures through data breaches or malware and then use them to blackmail people. Sextortion puts a lot of mental stress, fear, and shame on people. Some victims have very bad mental health problems, which shows how bad this type of digital abuse can be.

5. **DEEPFAKE SEXUAL EXPLOITATION:**

Artificial intelligence has made deepfake sexual exploitation a new and quickly growing type of digital sexual violence. This type of AI technology makes fake but realistic explicit pictures or videos of a person without their permission. Someone's face can be put on pornographic material to make it look real when it isn't.

The damage is not in the content's truthfulness, but in its effect. Even if the content is proven to be fake, victims may still lose their reputation, feel bad emotionally, and face social stigma. Deepfakes are especially dangerous because they are hard to spot and can be made quickly and cheaply. This kind of abuse shows how new technologies can be used to make sexual exploitation worse, which means that laws and rules need to be updated.

SOCIAL AND CULTURALION: DIMENSION:

The socio-cultural aspect of digital sexual violence cannot be comprehended in isolation from the overarching trends of gender inequality, power disparity, and social hierarchy that prevail offline, as online abuse frequently reflects and exacerbates existing cultural norms that condone or normalize the control of women's bodies and sexuality.(Rinehart 2025) In many cultures, patriarchal views still control how women act, dress, speak, and behave online. When women speak up in public digital spaces, whether as students, professionals, journalists, activists, or content creators, they are often the targets of online sexual harassment, cyberstalking, non-consensual image sharing, sextortion, or deepfake exploitation as a way to punish or silence them. Cultural attitudes that blame victims make things even harder. Survivors are often asked why they shared pictures, posted pictures, or interacted online instead of focusing on what the perpetrator did wrong. This makes people less likely to report the crime and makes them feel ashamed. In conservative communities, there is a lot of shame around sexuality. This makes image-based abuse even worse because it can hurt your reputation, which can hurt your chances of getting married, getting a job, and protecting your family's honor. This makes digital sexual violence not only a personal trauma but also a social crisis. Caste, class, religion, sexual orientation, and disability are all examples of intersectional factors that can make someone more vulnerable. Marginalized groups are more likely to be abused and have fewer ways to get help. The quick rise of social media and AI has made these cultural dynamics even stronger. Anonymity, viral sharing, and algorithmic amplification make it easy for misogynistic content to spread and make abusive behavior seem normal. Also, the

digital divide in knowledge and legal literacy means that many victims don't know their rights under new laws that deal with cyberstalking, image-based abuse, and deepfake exploitation. This leads to under-reporting and a lack of trust in the legal system. So, the socio-cultural aspect of digital sexual violence shows that it is not just a legal or technological issue, but a deeply rooted social problem caused by gender norms, moral policing, stigma, and unequal power relations. To make sure that everyone can participate in digital spaces with dignity, equality, and safety, both culture and the law need to change.(Karpinsky 2024)

LEGAL FRAMEWORK AND GAPS:

As technology has been used more and more for sexual harassment, cyberstalking, sharing intimate images without permission, sextortion, and deepfake sexual exploitation, the laws that deal with digital sexual violence have changed. However, there are still big holes in both their design and their implementation. In India, laws like the Bharatiya Nyaya Sanhita, 2023 (which replaced the IPC), Sections 66E, 67, and 67A of the Information Technology Act, 2000, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (which were strengthened by later amendments) make it possible to prosecute online sexual abuse. The latter also require digital intermediaries to do their due diligence and take down illegal content. Recent legal scrutiny of AI-generated content and deepfake sexual imagery signifies acknowledgment of emerging threats, and regulatory dialogues increasingly stress expedited removal timelines, traceability in severe offenses, and enhanced platform accountability. Still, these frameworks often see digital sexual violence as separate crimes instead of a separate, gendered type of harm. This makes it hard to apply and interpret them consistently. (Flynn et al. 2025)Jurisdictional challenges emerge due to the transnational nature of online abuse, complicating investigation and prosecution, which necessitates international cooperation. Evidentiary issues make enforcement even harder because digital content can be quickly deleted, changed, or stored on servers in other countries, and many victims don't know how to keep electronic evidence. Safe harbor protections for intermediaries are important for protecting free speech and innovation, but they can sometimes make it take longer or not be enough to respond to victim complaints. Also, the effectiveness of even well-written laws is limited by underreporting caused by stigma, fear of retaliation, and a lack of knowledge about cyber law. Countries like the UK and the US have made more clear laws against image-based abuse and deepfake exploitation, which shows that they are moving toward recognizing consent as an important part of digital sexual autonomy. However, because legal systems are

not the same everywhere, it is hard to enforce these laws in cases that cross borders. So, even though changes to the law show that people are becoming more aware of sexual harm that happens with technology, there are still gaps in clarity, enforcement capacity, victim support mechanisms, and international harmonization. This shows that the current legal system is still reactive and broken, and it needs a more complete, victim-centered, and technology-adaptive approach to effectively deal with digital sexual violence.

BALANCING FUNDAMENTAL RIGHTS:

One of the most difficult socio-legal problems in modern digital governance is how to balance fundamental rights in the context of digital sexual violence. This is because efforts to protect people from online sexual harassment, cyberstalking, non-consensual intimate image sharing, sextortion, and deepfake exploitation must work alongside constitutional guarantees like freedom of speech and expression, privacy, equality, and due process. On one hand, people who have been victims of digital sexual violence have a basic right to dignity, bodily autonomy, mental integrity, and privacy of information. When intimate content is shared without permission or when people are forced to stop talking about things online because of abuse, these rights are seriously violated. The right to equality is also at stake because women and marginalized groups are more likely to experience technology-facilitated sexual harm, which limits their ability to fully participate in digital spaces, find jobs, and engage in democracy. On the other hand, rules that require platforms to take down certain types of speech, monitor them, and punish people who break the law for certain types of speech must be carefully thought out so that they don't go too far and stop people from expressing themselves, being creative, making fun of things, or giving critical commentary. Too much surveillance, unclear legal definitions, or too much power to censor may make people less likely to speak their minds and hurt democratic values. So, the problem is making laws that are very specific about what constitutes a consent-based violation, provide procedural protections, and impose fair liability, all while protecting freedom of speech and innovation. Courts and lawmakers need to take a rights-based approach that understands that free speech doesn't include speech that hurts someone's privacy or dignity.(Clevenger and Marcum 2023) However, any limits must be necessary, proportional, and legal. The goal of this balancing process is not to put one right above another, but to find a way to protect people from digital sexual violence while still protecting the basic freedoms that are necessary for a free and open digital society.

TOWARDS HOLISTIC RESPONSES:

To move toward holistic responses to digital sexual violence, we need to realize that legal punishment alone is not enough to deal with the complicated and changing nature of online sexual harassment, cyberstalking, sharing intimate images without permission, sextortion, and deepfake sexual exploitation. A complete plan must include changes to the law, rules for technology, holding institutions accountable, helping victims, and changing society and culture. From a legal standpoint, there is a necessity for more precise and unequivocal statutory definitions that explicitly acknowledge digital sexual violence as a separate category of harm focused on consent. Additionally, there should be more efficient reporting systems, time-sensitive removal responsibilities for intermediaries, and enhanced frameworks for cross-border collaboration to tackle jurisdictional issues. To make sure that victims are treated with respect and seriousness, law enforcement agencies need to have special cybercrime units, digital forensic training, and procedures that take gender into account. At the technological level, platforms should take proactive steps to make safety a priority, such as better content moderation systems, AI tools to find deepfake and intimate image abuse, clear ways for users to file complaints, and accountability standards that put user safety first without limiting free speech. Support that focuses on the victim is just as important. This includes private reporting channels, legal help, psychological counseling, digital evidence preservation guidance, and rehabilitation help to lessen long-term social and economic damage (Powell et al. 2022). Schools and community groups need to teach people how to use technology, how to give and get consent, and how to behave responsibly online. They also need to challenge cultural norms that blame victims and treat men and women differently. Policymakers should also push for collaboration between governments, tech companies, civil society, educators, and researchers to come up with plans that change as technology does. A comprehensive response recognizes that digital sexual violence is not only a legal infraction but a societal concern entrenched in power dynamics, gender, and technology. Consequently, it necessitates cohesive solutions that uphold dignity, guarantee accountability, and promote safer and more inclusive digital environments.

CASE LAW:

Kamya Buch v. X Corp., Meta Platforms, Google & Ors (Delhi High Court, July 18, 2025)

Kamya Buch v. X Corp., Meta Platforms, Google & Ors (Delhi High Court, 2025) is a recent

and important case that deals with digital sexual violence. It was about the spread of AI-generated sexually explicit and defamatory content targeting a woman academic and activist on several online platforms. The petitioner went to court after finding out that manipulated and deepfake pornographic material using her name had been widely shared on social media and websites. This had caused her a lot of emotional pain, damage to her reputation, and violation of her privacy and dignity. The Delhi High Court said that the content was deeply harmful and violated the right to privacy and dignity under Article 21 of the Constitution because it was aware of how serious AI-enabled sexual exploitation is. The Court issued an urgent temporary injunction stopping anonymous offenders from publishing or sharing the material any further. It also told major intermediaries like X (formerly Twitter), Meta, and Google to remove the URLs right away and stop people from accessing them. It also told platforms to give out any identifying information they had about the people who uploaded the content to help with more legal action. It also told authorities to block websites that were breaking the law when necessary. The Court made sure that the petitioner's personal information was kept private in court records to stop more harassment. This case is very important for the study of digital sexual violence because it shows how Indian courts are using existing constitutional principles and cyber laws to deal with new harms like deepfake sexual exploitation, holding platforms more accountable, and saying that online abuse that causes sexual humiliation and damage to reputation is a serious violation of basic rights.

SUGGESTION AND FINDINGS:

The study finds that although existing laws such as the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 address certain aspects of online harassment and cyberstalking, they do not comprehensively define or recognise digital sexual violence as a distinct offence. Enforcement remains challenging due to anonymity, encrypted platforms, cross-border jurisdictional issues, and inadequate cyber forensic infrastructure, while underreporting persists because of social stigma, lack of awareness, and fear of retaliation. Platform accountability mechanisms are also often insufficient in responding promptly to complaints. In light of these findings, the study suggests introducing a clear statutory definition of digital sexual violence, strengthening specific provisions on cyberstalking and online harassment, establishing specialised cybercrime units with trained personnel, enhancing victim protection and fast-track procedures, imposing stricter compliance obligations on intermediaries, and promoting digital literacy and awareness programmes to ensure effective

prevention and redressal.

CONCLUSION:

Digital sexual violence is one of the most pressing social and legal problems of the modern digital age. As technology has advanced, traditional forms of gender-based abuse have become more complicated, cross-border, and quickly growing online harms. Online sexual harassment, cyberstalking, sharing intimate images without permission, sextortion, and using AI-generated deepfakes to exploit people are all examples of how digital platforms can be used to violate dignity, privacy, autonomy, and equality. Even though recent changes to the law, rules, and the courts show that these harms are getting more attention, the response is still scattered and often reactive, and it is hard to keep up with new technology and the speed at which information spreads online. Enforcement gaps, jurisdictional complexities, evidentiary challenges, and persistent social and cultural stigma make it hard to get justice. Victims often suffer from psychological trauma, damage to their reputation, and being left out of digital participation. At the same time, rules must carefully balance protecting people from abuse with basic rights like freedom of speech and due process. This means that rules must always be fair and based on rights (Carpenter 2024). In the end, dealing with digital sexual violence needs a full and coordinated plan that includes clear legal definitions based on consent, more responsibility for platforms, specialized enforcement tools, cooperation between countries, support systems for victims, and ongoing efforts by society to fight gender inequality and attitudes that blame victims. Digital spaces can only become safer and more welcoming places that respect human dignity and allow everyone to participate equally if they are built on a framework that is both holistic and rights-conscious.

REVIEW OF LITERATURE:

1. Carpenter, Perry. 2024. *FAIK: A Practical Guide to Living in a World of Deepfakes, Disinformation, and AI-Generated Deceptions*. John Wiley & Sons.
2. Clevenger, Shelly L., and Catherine D. Marcum. 2023. *The Link between Specific Forms of Online and Offline Victimization: A Collaboration Between the ASC Division of Victimology and Division of Cybercrime*. Taylor & Francis.
3. Flynn, Asher, Elena Cama, and Adrian J. Scott. 2025. *Image-Based Sexual Abuse and Bystander Intervention: A Mixed Methods Study of Attitudes, Barriers and Facilitators*. Springer Nature.

4. Freeman, Jerrid P., Cari L. Keller, and Renee L. Cambiano. 2020. *Higher Education Response to Exponential Societal Shifts*. IGI Global.
5. Great Britain: Parliament: House of Commons: Culture, Media, and Sport Committee. 2014. *Online Safety: Sixth Report of Session 2013-14, Vol. 1: Report, Together with Formal Minutes, Oral and Written Evidence*. Stationery Office.
6. Indreswari, Tri Laksmi, Kadek Cahya Susila Wibawa, and Juan Diaz-Granados. 2023. *IWLEG 2022: Proceedings of the 1st International Workshop on Law, Economics and Governance, IWLEG 2022, 27 July 2022, Semarang, Indonesia*. European Alliance for Innovation.
7. Karpinsky, Dave. 2024. *Deepfake Technology: The Dark Side of AI, Manipulation, and Digital Deception*. Independently Published.
8. Leung, Angel Nga Man, Kevin Ka Shing Chan, Catalina Sau Man Ng, and John Chi-Kin Lee. 2023. *Cyberbullying and Values Education: Implications for Family and School Education*. Taylor & Francis.
9. Powell, Anastasia, Asher Flynn, and Lisa Sugiura. 2022. *The Palgrave Handbook of Gendered Violence and Technology*. Springer Nature.
10. Rachmawati, Meida, Faisal Santiago, and Eko Eddya Supriyanto. 2023. *ICLSSEE 2023: Proceedings of the 3rd International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2023, 6 May 2023, Salatiga, Central Java, Indonesia*. European Alliance for Innovation.
11. Rinehart, Matthew. 2025. *Deepfake Video and Audio: Implications for Cybersecurity*. Independently Published.
12. Spurek, Sylwia. 2026. *Cyberviolence against Women: A New Face of an Old Problem*. Taylor & Francis.
13. Taneja, Sanjay, Swati Gupta, Mohit Kukreti, and Abhishek Singh Chauhan. 2025. *Mastering Deepfake Technology: Strategies for Ethical Management and Security*. CRC Press.
14. United Nations. Economic and Social Council. 2014. *Prevention, Protection and International Cooperation Against the Use of New Information Technologies to Abuse And/or Exploit Children: Report: 2014*.
15. Valentine, Catherine G., Mary Nell Trautner, and Joan Z. Spade. 2019. *The Kaleidoscope of Gender: Prisms, Patterns, and Possibilities*. SAGE Publications.