PROTECTING WOMEN AND CHILDREN AGAINST DIGITAL OFFENCES: A CRITICAL AND COMPARATIVE LEGAL PERSPECTIVE FOR IMPLEMENTATION IN INDIA

Madipeddi Shravani & S Vijay Amruth, NALSAR University

ABSTRACT

With the increase in accessibility of digital platforms, vulnerable groups like women and children are being subjected to cybercrimes such as cyberstalking, cyber bullying, online harassment, trolling, child grooming, and non-consensual image sharing (revenge porn). As these digital abuses often get viral, they escalate quickly on anonymous platforms and cause irreparable damage to the innocent victims.

Though there are Indian legal frameworks like the Digital Personal Data Protection (DPDP) Act, 2023; Bharatiya Nyaya Sanhita (BNS), 2023; Information Technology (IT) Act, 2020; and Protection of Children from Sexual Offences (POCSO) Act, 2012, these acts are silent on AI-generated offences, lack legal protections available to victims, and lack consistent enforcement. Also, these laws often overlap, creating ambiguity and inadequately addressing the slow and complicated complaint-filing mechanism.

Hence, this paper compares, examines, and analyses the legal frameworks of the U.S., Germany, Japan and England . The Online Safety Act of the UK law focuses on mandating the intermediaries, i.e., the platforms, to swiftly remove harmful content and empowers the Office of Communications to penalise non-compliant services. The German Penal Code (Strafgesetzbuch, StGB) expressly makes grooming practices illegal. Japan mandates that the victims prove that there is an invasion of their privacy, and also that the intimate pictures and their behaviour have caused irreparable loss to the victim. The Online Safety Act 2023 of England has imposed a statutory duty on online platforms and mandated them to assess and mitigate the risk which is associated with illegal content generated by abusing women and children, and to regulate harmful online behaviour by perpetrators. Also, by comparing Indian laws with the stringent laws of these countries, the paper recommends the best practices of hassle-free responsive authorities, intermediary responsibilities, and remedies to victims.

The paper highlights the need for comprehensive legislation and the implementation of women- and children-centric laws to prevent digital offences and promote a safe digital space for vulnerable people while aligning with global standards for strengthening victim rights.

Keywords: Digital safety, intermediary regulations, digital abuse, vulnerable groups, victim protection.

Introduction

The rapid expansion of digital technologies gave rise to new forms of crime that disproportionately target women and children. Cyberstalking, online harassment, revenge porn, and other technology facilitated abuses have emerged as pressing concerns along with existing gender inequalities. These also leave victims with limited legal recourse. Despite there being global recognition for these crimes, legal frameworks in many countries, including India, are inadequate in addressing the nature of digital offences against women and children.

India's current legal regime, primarily governed by the Digital Personal Data Protection (DPDP) Act, 2023; Information Technology (IT) Act, 2020; and Protection of Children from Sexual Offences (POCSO) Act, 2012, lacks comprehensive mechanisms to combat cybercrimes against women and children effectively. While initiatives like the Indian Cyber Crime Coordination Centre (I4C)[1] and the National Cyber Crime Reporting Portal represent progressive steps, but they lack in enforcement challenges, jurisdictional ambiguities, and legislative gaps. Also, these laws often overlap, which creates ambiguity. There is also a need to address the slow and complicated complaint-filing mechanism.

A comparative analysis with countries like the U.S., Germany, Japan and England reveals critical insights that could inform stronger legal protections in India. The stringent provisions of these countries recommend India to add those stringent legal provisions. This will help India to curtail the digital offences against women and children.

This study highlights key shortcomings in India's current legal system for digital offences against women and children and suggests changes based on comparative jurisprudence. This study aims to strengthen India's current cyber laws and give victims of digital abuse justice,

[1] *Measures To Ensure Safety And Security Of Women And Children On Online Platforms*, https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1808686 (last visited May 21, 2025).

deterrence, and rehabilitation by comparing them with international best practices and promoting a victim-centric approach.

Digital offences:

Cyber crimes

The easy accessibility and the popularity of the Internet have brought with them certain new crimes in the past fifteen years that include cyberstalking, cyber harassment, and online impersonation.

The United Nations has identified cyber stalking and other technology-facilitated violence as pressing and increasing dangers to women and girls worldwide. UN Women and other UN entities identify that digital abuse, such as stalking, harassment, and non-consensual posting of intimate information, has increased quickly, particularly as more parts of everyday life go online. They are disproportionately impacted, with young women aged between 18 to 24 being especially at risk for stalking and sexual harassment in online environments[2]. Digital gender-based violence not only harms women psychologically but also constrains their freedom of speech and engagement in public, political, and economic life[3].

UN reports highlight that technology-enabled violence is but a part of a larger continuum of gender-based violence that mirrors and reflects structural gender inequalities and damaging social norms. vulnerable groups, such as women, LGBTQ+ women, and disabled women, are at greater risk. The COVID-19 pandemic also accelerated these problems, as heightened online activity translated to a proliferation of digital abuse[4].

Even with the magnitude of the issue, legal and policy measures usually trail behind technological advancements. Most nations do not have definite definitions and effective legislation on dealing with online violence, and even where legislation is in place, enforcement

[2] *Urgent Action Needed to Combat Online Violence against Women and Girls, Says New UN Report*, UN Women – Headquarters (Sep. 24, 2015), https://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release.

[3] *Accelerating Efforts to Tackle Online and Technology-Facilitated Violence against Women and Girls*, UN Women – Headquarters (Oct. 8, 2024), https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls.

[4] *UN Report Highlights Growing Online Violence against Women and Girls, Related Research*, Vine – Violence Information Aotearoa, https://www.vine.org.nz/news/un-report-highlights-growing-online-violence-against-women-and-girls-related-research (last visited May 21, 2025).

is often weak because of a lack of awareness and resources among law enforcement institutions. Less than a quarter of law enforcement institutions around the world are doing anything about online violence against women.

The existing laws in India protect the vulnerable groups from sexual crimes in public and the workplace, but are silent as they face the same abuse in the digital space. Hence, the laws need to be expanded to include the Internet. Some of the abuses that women and children face in the digital space are explained in the sections below:

Cyber stalking

It means following a person and making or attempting to make contact despite a clear disinterest being displayed by the other person. Stalking may be committed both physically and through electronic media against women[5].

Stalking is perusing someone stealthily. So in cyber stalking, the victims are trailed, especially the victim, especially females, in order to have sexual favours in return. Paedophiles are generally adults. It starts with curious Netizens unaware of the safety precautions. It's believed that 75% of victims are females. Reasons for Cyber Stalking are Sexual Harassment, Obsession for love, Revenge and hate for love. Cyber Stalkers target and harass their victims via websites, chat rooms, discussion forums, emails, and open phishing websites. Megha Desai & K Jaishankar conducted a survey titled Cyber Stalking titled Victimisation of Girl Students, stating that 13% of the victims had an intimate relationship with their stalkers, i.e. 70% of harassment started through emails and online chats[6].

The number of cyber stalking/ bullying cases registered in India is mostly against women and children, which increased from 739 in the year 2018 to 1471 in the year 2022[7]. In India, cyber stalking is an offence under The Indian Penal Code's Section 354D and also under section 67 of IT act, 2000 where IPC expressly makes stalking, including cyberstalking, illegal. It punishes any man who persistently pursues or communicates with a woman via email or instant messaging, even when she expresses a clear lack of interest[8]. Offender for the first time faces

[5] Indian Penal Code, 1908, S 354 D.
[6] Hemangini Shekhawat, Cyber Crimes against Women, 5 INT'l J.L. MGMT. & HUMAN. 1673 (2022).
[7] Unstarred question no.226, Rajya Sabha, *GOVERNMENT OF INDIA MINISTRY OF HOME AFFAIRS.*
[8] *Cyber Stalking*, ISEA, https://www.staysafeonline.in/concept/cyber-stalking/law-says-with-regard-to-this-offence (last visited May 23, 2025).

three years imprisonment and a fine; repeat offenders face no bail and a maximum sentence of five years in prison.

The Federal Interstate Stalking Punishment and Prevention Act[9] was enacted in America to address both traditional stalking as well as cyberstalking by making the offence a federal crime to engage in a course of conduct intended to harass, intimidate, or place another person under surveillance, when such conduct crosses state lines, occurs within federal jurisdiction, or uses channels of interstate space such as the internet or electronic communications[10]. This legislation was passed as part of the Violence Against Women Act in 1996. This law specifically recognises cyberstalking, making it illegal to use digital gadgets to harass or intimidate someone or physically cross the borders of states with the intention of stalking[11].

Online Harassment

Online harassment includes blackmail, threats, bullying, and cheating, and it is the same as harassment that occurs through printed messages. Also known as "e-harassment," this issue arises when the IP Addresses are linked to false IDs. Section 354A of the Criminal Law Amendment of 2013 is one of the provisions of the Indian Penal Code that addresses sexual harassment.

When sexual harassment occurs on the Internet, there is very little that women can do to protect themselves. Most sexual harassment or discrimination laws have not been adequately updated to address new practices of harassment.

Child grooming

Child grooming refers to the actions of the offender to gain trust and retain influence over a child in order to prepare them for sexual abuse and prevent the child from disclosing it to others. The perpetrator starts his grooming behaviours in the earlier stages by engaging the child with activities of a sexual intention. In most of cases, the abuser is a person who is already in close contact with the child or a stranger who establishes a trusting relationship with the

[9] 18 U.S. Code § 2261A.
[10] *18 U.S. Code § 2261A - Stalking | U.S. Code | US Law | LII / Legal Information Institute*, https://www.law.cornell.edu/uscode/text/18/2261A (last visited May 21, 2025).
[11] Arunbaby Stephen, *Comparative Analysis of Cyber Stalking Legislations in UK, US and India*, 6.

child by approaching them[12]. Recently, these perpetrators started using online platforms to approach the children and engage in grooming acts.

To counter child grooming, India does not have a specific and uniform definition to criminalise the act; instead, our law enforcement agencies depend on the 2012 Protection of Children from Sexual Offences Act (POCSO), which only makes child sexual harassment illegal. So, child grooming can be filed under POCSO's Section 11, which consists of recurrent or continuous contact with a child via electronic or other methods, and includes behaviours like interacting with a child, stalking, or luring a child for sexually suggestive pornographic objectives[13]. Although these rules can be used in grooming situations, they only take effect when there is explicit content or a clear sexual motive behind the activities. In addition, Section 67B of the Information Technology Act of 2000 makes it illegal to publish, transmit, or facilitate any electronic content that shows minors engaging in sexually explicit behaviour. It also makes online connections that are fostered for such purposes illegal[14]. Nevertheless, it is unclear from this provision what exactly qualifies as "facilitation of online abuse, leading to ambiguity regarding which grooming behaviours are punishable.

To curb child grooming, Japan has introduced Article 182 in the Japan Penal Code in June 2023 as a part of a comprehensive revision of sexual offences. According to Article 182 (1), it is illegal to use unfair methods to meet with someone under the age of sixteen in order to engage in indecency. Furthermore, there will be more severe penalties for a meeting that really takes place after the request to meet (Article 182 (2)). While Article 182(3) addresses sexual abuse committed remotely without actual physical contact, Article 182(1) and (2) address the risk of sexual assault or abuse in a face-to-face setting[15].

While Germany's laws against child grooming are strong, particularly when it comes to internet sexual exploitation. The German Penal Code (Strafgesetzbuch, StGB) expressly makes grooming practices illegal. Communicating with a child with the intention to do sexual actions,

---

[12] Tomoyuki Sakai, Cyber-Grooming in the Japanese Penal Code, 53 HITOTSUBASHI J.L. & POL. 25 (2025).
[13] *Child Grooming: India Must Take Measures to Protect Children from Online Sexual Abuse*, Strategic Advocacy for Human Rights - SAHR, https://www.wearesahr.org/blog/child-grooming-india-must-take-measures-to-protect-children-from-online-sexual-abuse (last visited May 23, 2025).
[14] Jilsblognujs, *Addressing the Gaps in India's Child Protection Laws: Safeguarding Children from Online 'Grooming,'* The Journal of Indian Law and Society (Jun. 21, 2022), https://jilsblognujs.wordpress.com/2022/06/21/addressing-the-gaps-in-indias-child-protection-laws-safeguarding-children-from-online-grooming/.
[15] *Penal Code - English - Japanese Law Translation*, https://www.japaneselawtranslation.go.jp/en/laws/view/3581/en (last visited May 23, 2025).

whether those acts are performed in front of the perpetrator or a third party, is illegal under Section 176(4)(3) StGB[16]. This provision, which covers children under the age of 14, reflects Germany's stringent laws protecting children from exploitation and sexual abuse. Alongside criminal law, Germany's Protection of Young Persons Act (Jugendschutzgesetz, JuSchG) underwent a modification in 2021 to handle concerns associated with the digital world, including cyberbullying and cyber-grooming in a better way[17]. The law seeks to reduce the likelihood that children and adolescents would become victims of online sexual violence, and it specifically addresses the preservation of children's personal integrity online. These rules, which include safeguards against hate speech, online grooming, and other interaction hazards, are enforced by the recently created Federal Agency for Child and Youth Protection in the Media[18].

Revenge porn

The term "revenge porn" refers to non-consensual pornography, which is defined as "the distribution of sexually graphic images of individuals without their consent."[19] This covers images that were first shot with permission but were subsequently shared without permission by an outraged ex-partner. There aren't many remedies available to victims when they learn that their former partner circulated such content[20].

India has not yet enacted any laws to explicitly criminalize revenge porn while the majority of states in America have laws against revenge porn but most of them classify it as a minor offense, punishable by less than a year in jail and an insignificant fine[21]. Minority states consider revenge porn as illegal. Some states have no laws against revenge porn, which creates

[16] *Child Abuse (Section 176, German Criminal Code) | Lewik*, https://www.lewik.org/term/15665/child-abuse-section-176-german-criminal-code/ (last visited May 23, 2025).
[17] *Online Legal Issues*, UBSKM, https://beauftragte-missbrauch.de/en/themen/recht/online-legal-issues (last visited May 23, 2025).
[18] *Experts of the Committee on the Rights of the Child Praise Germany for Prosecuting International Perpetrators of Sexual Abuse against Children, Ask About the Rise of Child Pornography Cases and Children in Armed Conflict | The United Nations Office at Geneva*, (Sep. 6, 2022), https://www.ungeneva.org/en/news-media/meeting-summary/2022/09/la-pauvrete-parmi-les-enfants-la-violence-sexuelle-et-la.
[19] Danielle Keats Citron & Mary Anne Franks, Criminalizing Revenge Porn, 49 Wake Forest L. Rev. 345, 346 (2014).
[20] Apeksh vora, Note, Into the Shadows: Examining Judicial Language in Revenge Porn Cases, 18 Geo. J. Gender & L. 229, 231 (2017) (Noting that remedies do not, and cannot, address every experienced harm).
[21] Apeksh vora, Note, Into the Shadows: Examining Judicial Language in Revenge Porn Cases, 18 Geo. J. Gender & L. 229, 231 (2017) (Noting that remedies do not, and cannot, address every experienced harm).

a legal gap that leaves a person with few or no choices if they discover that their ex-partner has shared private, intimate images.

Unlike America, very few countries have laws on revenge porn and even the laws in these countries are silent when it comes to giving justice to the victims as they are not providing adequate justice to them. The distinctive characteristic of revenge porn is that it is both a sex crime and a cybercrime[22]. Hence, any legislation that addresses revenge porn should make it a point to incorporate aspects of both cybercrimes and sex crimes, and it should originate from the central government. so, in order to save the victim from a torturous trial and the humiliation, indignity, and disgrace that accompany a prolonged and complex prosecution, revenge porn laws should be of strict liability crime due to the nature of the offence.

Revenge porn as an offence in the American state laws have been categorised into copyright, privacy, tort and criminal statutes[23]. The victim automatically owns the copyright to the image if she has taken it herself, as that of a "selfie". The victim can issue a takedown notice to the website operator under the Digital Millennium Copyright Act to have that image removed[24]. However, the issue with this method is that victims have no right to monetary compensation at all. In addition, if the website is located in a foreign country, the victim is not protected by the Digital Millennium Copyright Act. As a result, a foreign website can be less or not at all responsive to removing the photos. Furthermore, even if that image is removed from one website, it does not necessarily mean that its internet existence has been entirely eradicated because digital images are simply easy to reproduce. The major drawback with this approach is that this act comes in handy only when the photographer is the victim herself, or else this act cannot be used. Another method is where the victim or her advocate files a complaint against the offender on charges of invasion of privacy claims, through unauthorised use of a computer. As this was what the prosecutors attempted to do in Crapps v. State[25].

Germany seems to have a stringent law compared to other countries, as a German court has

[22] Julie M. Allen, Sexual Cyberharassment: Revenge Porn & the Law, 45 N. KY. L. REV. 1 (2018).
[23] Woodrow Hartzog, How to Fight Revenge Porn, The Center for Internet and Society (May 10, 2013), http://cyberlaw.stanford.edu/blog/2013/05/how-fight-revenge-porn.
[24] Lorelei Laird, Victims are taking on 'revenge porn' websites for posting photos they didn't consent to, A.B.A. J. (Nov. 1, 2013), http://www.abajournal.com/magazine/article/ victims_are takingon_revengeporn_websites forposting_photostheydidnt_c/?utm_source =maestro&utm_medium=email&utmcampaign=tech_monthly.
[25] Crapps v. State, 180 So. 3d 1125 (Fla. Dist. Ct. App. 2015).

asked the offender to delete the intimate pictures of the complainant upon her request[26]. While Japan mandates that the victims prove that there is an invasion of their privacy, and also that the intimate pictures and their behaviour have caused irreparable loss to the victim[27]. it is a problematic approach when those images are uploaded anonymously by the offender.

If the offender has uploaded photos onto any digital platform, the victim has little chance of having their photos taken down from the Internet. Consequently, in order to avoid their internet presence, some victims have resorted to legally changing their names.

Indian laws on digital offences

In order to give law enforcement agencies a framework and ecosystem to address cybercrimes in an exhaustive and coordinated manner, the government established the Indian Cyber Crime Coordination Centre (I4C), which is under the Ministry of Home Affairs[28]. The government runs a program called "Cyber Crime Prevention against Women and Children (CCPWC)" under the Nirbhaya Fund. With the help of this project, measures are taken to raise awareness of cybercrimes. It further issues alerts and advisories. It also trains and gradually increases the capacity building of law enforcement, prosecutors, and judicial officers and improves cyber forensic facilities.

The government has also launched a National Cyber Crime Reporting Portal (www.cybercrime.gov.in) and introduced a toll-free number, 1930, to assist victims in lodging online cyber complaints. MeitY has been raising awareness among users, especially women and children, on the significance of digital safety when using the Internet through a program called Information Security Education & Awareness (ISEA)[29].

Information Technology Act, 2000

The only digital offences against women and children that are covered by the Information Technology Act, 2000 are Section 66E (violation of privacy), Section 67 (publication or transmission of obscene material), Section 67A (sexually explicit material), and Section 67B

[26] Philip Oltermann, 'Revenge Porn' victims receive boost from German court ruling, The Guardian, May 22, 2014, https://www.theguardian.com/technology/2014/may/22/revenge-porn victims-boost-german-court-ruling.
[27] Shigenori Matsui, The Criminalization of Revenge Porn in Japan, 24 Wash. Int'l LJ. 289, 293 94 (2015).
[28] *Measures To Ensure Safety And Security Of Women And Children On Online Platforms*, https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1808686 (last visited May 21, 2025).
[29] *Progression Pathway*, ISEA, https://staysafeonline.in/progression-pathway (last visited May 21, 2025).

(child sexual abuse material). These provisions criminalise only a certain type of cyber offences like unauthorised use of digital identity, online impersonation, voyeurism, and the distribution of obscene or sexually explicit content and include enhanced penalties for offences involving children.

Under section 65 of the Act, the first case that was registered is Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr[30]. It was held that cell phones fulfil the definition of a computer under the IT Act, 2000, whereas the unique Electronic Serial Numbers that are arranged into the handset programme are the computer source code, which is required to be kept and maintained by the law.

There are a lot of things to consider when reviewing the State of Tamil Nadu vs. Suhas Katti[31] case. In an attempt to enrage the victim and give the idea that she was soliciting, he posted her phone number and derogatory comments on other forums, as the victim had rejected his marriage proposal. As a result, the victim received numerous obnoxious and derogatory calls from persons who believed the woman was soliciting. To spread such abusive remarks on Yahoo groups, the perpetrator made a fake account in the victim's name with the intention of harming the victim's reputation. This case is highly significant with respect to online offences as this was the first case to be filed under Section 67 of the Information Technology Act of 2000, and highlighted the consequences of releasing pornographic material and asserted that no one can be absolved of their responsibilities. Due to the Chennai Cyber Cell's exceptional efficiency, this case was settled in just seven months.

The IT Act has significant drawbacks despite its characteristics. Some observers point out that there are several gaps in coverage for new digital offences like deepfake pornography, cyberbullying, and online stalking because the Act was initially created for the protection of financial transactions and e-commerce, not to explicitly address gendered cybercrimes[32]. One of the legal remedies for the victims is to file a complaint under relevant sections of the IT Act, as well as invoking provisions of the Indian Penal Code, 1908 such as Section 292 (obscenity), Section 354C (voyeurism), and Section 354D (stalking, including cyberstalking), to supplement the IT Act as in many cases, its provisions are insufficient to cover the offences.

[30] MANU/AP/0660/2005.
[31] CC No. 4860/2004.
[32] Akanksha Pathak & Mr Prateek Tripathi, *DIGITAL VICTIMIZATION OF WOMEN IN CYBERSPACE: AN ANALYSIS OF EFFECTIVENESS OF INDIAN CYBER LAWS.*

Additionally, victims can use internet portals set up by the government, like the Cyber Crime Portal, to file a complaint against digital offences and also to seek aid from cybercrime cells. Even though the IT Act of 2000 provides a fundamental legal framework for dealing with online crimes against women and children, its efficacy is constrained by enforcing them. Hence, there is a dire need for legislative and procedural changes. Given the large number of cybercrimes committed against women and children and the broad spectrum of digital offences that occur on a daily basis, it is evident that the amended IT Act of 2008 is clearly insufficient[33].

Responsibility of online platforms

In India, Intermediaries (such as social media sites and digital service providers) are required by the IT Act to exercise due diligence, remove illegal content as soon as they become aware of it, and follow government instructions[34]. The 2021 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules discuss these responsibilities in more depth, requiring platforms to designate compliance officers, set up grievance redressal procedures, and conduct proactive content monitoring.

The Online Safety Act 2023 of England has imposed a statutory duty on online platforms and mandated them to assess and mitigate the risk which is associated with illegal content generated by abusing women and children, and to regulate harmful online behaviour by perpetrators[35]. For this reason, the platforms must constantly identify, prevent and remove illicit content that includes child sexual abuse, sexual exploitation, coercive behaviour on minors, child pornography, intimate image abuse and other such sexual abuses.

To protect the children, the intermediate platforms are ordered to implement age restrictions and enforce safety measures to enable age-appropriate experiences while shielding the minors from the exploitative content[36]. If they violate the Act, the Office of Communications, being the independent regulator, has the authority to enforce compliance, issue codes of practice, and levy hefty penalties of up to 18 million, or 10% of a company's worldwide revenue[37]. Platforms

[33] Piyush Kumar Jalan & Surabhi Rathi, Indian Cyber Laws on Cyber Crime: Analysis, 3 INT'l J.L. MGMT. & HUMAN. 1558 (2020).
[34] Rupal Chhaya & Ahmar Afaq, Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code), 2021: A Critical Study, 102 J. PAT. & TRADEMARK OFF. SOC'y 623 (October 2022).
[35] *Online Safety Act: Explainer*, GOV.UK, https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer (last visited May 23, 2025)
[36] John Woodhouse, *Implementation of the Online Safety Act* (2025), https://commonslibrary.parliament.uk/research-briefings/cdp-2025-0043/.
[37] Hedvig Schmidt, *The Online Safety Act 2023*, 16 J. Media Law 202 (2024).

need to have clear complaint and content reporting processes so that victims may report abuse and get help quickly. The Act also mandates that platforms notify the National Crime Agency of any content involving child sexual exploitation and abuse. To further shield the users from dangerous platforms, Ofcom has the authority to ban access to non-compliant services in the UK.

Conclusion

The modern digital age has exposed women and children to cyber risks, which requires urgent legal and policy intervention to curtail these issues. India's legal framework though is progressive in nature, it lacks in certain aspects which includes addressing the offences which includes cyberstalking, revenge porn and online harassment. Indian legal frameworks, which include the IT Act,2000, and the DPDP Act,2023, are being amended according to the needs of society; however, these do not completely tackle the psychological and social consequences of digital abuse. Also, enforcement mechanisms lack technological and procedural inefficiencies.

The U.S, Germany, Japan and England have more stringent legal provisions against these digital offences, and these will offer valuable lessons and recommendations for India. The key recommendations that India can adopt from these countries to reform its legal system include the following:

Supporting victim support mechanisms: Indian legal frameworks should strengthen victim support mechanisms in Indian legal provisions. This also includes expedited takedown procedures for non-consensual content. Victim support mechanisms are important for strengthening victims' confidence.

Establishing a specialised forum: There is a need to enhance law enforcement capabilities through specialised cybercrime units. This will identify and resolve the offences at the earliest, since there is a need to provide protection against digital offences.

Including provisions for all digital offences: India needs to add provisions for all kinds of digital offences in its legal frameworks. As of now, India is lacking in providing provisions for revenge porn, which India can consider from many countries, even U.S. has provisions for

revenge porn[38].

Role and Responsibility of Intermediaries: The intermediatory platforms in India should take care of the content that is circulated on their platforms. If the platform finds any harmful content, it should immediately delete it. This provision is present in England[39]. India should adopt it to curtail digital offences from all ends in India.

Also, the UN has advocated for a multifaceted strategy that should be included in Indian Legal frameworks. The strategies include establishing comprehensive and consistent legal frameworks that recognise and criminalise digital offences, including criminalising all forms of online gender-based violence.[40]

By integrating these recommended strategies in Indian Legal frameworks, India can develop a strong legal ecosystem that punishes offenders and also empowers the survivors. As digital spaces are improving day by day, there is a strong need for the law to transform. This ensures that the internet remains a safe and equitable domain for women and children. Only through sustained legislative innovation, proper enforcement, and societal vigilance, India can effectively combat digital offences and uphold the fundamental rights of its most vulnerable citizens i.e., women and children.

[38]Apeksh vora, Note, Into the Shadows: Examining Judicial Language in Revenge Porn Cases, 18 Geo. J. Gender & L. 229, 231 (2017) (Noting that remedies do not, and cannot, address every experienced harm).

[39] *Online Safety Act: Explainer*, GOV.UK, https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer (last visited May 23, 2025)

[40]*FAQs: Digital Abuse, Trolling, Stalking, and Other Forms of Technology-Facilitated Violence against Women*, UN Women – Headquarters (Feb. 10, 2025), https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women.