COMBATING IMAGE BASED SEXUAL ABUSE- GAPS AND CHALLENGES IN INDIA'S LEGAL SYSTEM RELATIVE TO BRICS, EUROPE AND USA

Deepa Kharb[*]
Ayushi Verma[**]

Abstract

Image-Based Sexual Abuse (for brevity IBSA) is a serious and growing form of online sexual violence. It involves the taking, sharing, or threatening to share intimate images of a person without their consent. This problem is often wrongly called revenge porn, a term that does not fully capture the many ways such abuse occurs. With the rise of social media, smartphones, and new technologies like AI and deepfakes, IBSA has become easier to commit and harder to control. Today, even fake or morphed sexual images can be created using ordinary photographs, causing severe harm to victims. Despite the seriousness of the harm, India does not have a single law that directly addresses IBSA. Instead, victims must rely on different laws such as the Information Technology Act, the Indian Penal Code/ Bharatiya Nyaya Sanhita, the POCSO Act, and data protection rules. These laws deal with obscenity, privacy, or voyeurism, but they do not fully recognise IBSA as a separate sexual offence. This paper critically analyses the adequacy and limitations of existing Indian laws, focusing on Sections 66E, 67, and 67A of the IT Act, alongside recent judicial developments recognising privacy, dignity, and informational autonomy as fundamental rights. Through a comparative study of legal frameworks in the United States, Europe, and BRICS nations, the paper highlights best practices, including victim centric remedies, platform accountability, and fast takedown mechanisms. The paper argues that India urgently requires a standalone, survivor centred, and technology responsive legal regime that explicitly recognises IBSA as a distinc sexual offence, covers AI generated abuse, ensures effective enforcement, and provides support to survivors in the digital age.

I Introduction

IN A distressing case, a married woman with a nine-year-old son sought legal intervention to block websites displaying her intimate images. The accused exploited her financial struggles and family absence to assault her, capture objectionable pictures, and later blackmail her. When her funds depleted, he leaked the images online.[1] In another tragic case, a party leader in Assam was arrested after a female colleague committed suicide following the leak of her private photos.[2] These instances are

* Associate Professor, Faculty of Law, University of Delhi.

** Research Scholar, The Indian Law Institute, New Delhi.

1 Arunima, "Delhi High Court issues directions and recommendations to MEITY and Delhi Police to deal cases regarding Non-consensual intimate images dissemination" *SCC Online Times* (Apr. 29, 2023), *available at*: https://www.scconline.com/blog/post/2023/04/29/delhi-high-court-issues-directions-to-meity-delhi-police-to-deal-with-cases-relating-to-non-consensual-intimate-images-dissermination/ (last visited on Nov. 10, 2025).

2 Biswa Kalyan Purkayastha, "Assam BJP leader, expelled after colleague's suicide over leaked photos, held" *Hindustan Times* (Aug 16, 2023), *available at*: https://www.hindustantimes.com/india-news/expelled-bjp-leader-arrested-in-connection-with-suicide-of-woman-colleague-over-leaked-private-photos-101692106851505.html (last visited on Nov. 10, 2025).

neither the first nor the last. There have been numerous instances where women are blackmailed to maintain relationships or extorted for money, among other reasons.

Adding to this series, recent incident from Surat shows how new technologies are intensifying IBSA in India. A man was arrested for creating AI generated obscene photos and reels of a primary school teacher and her husband, and posting them on Instagram. He acted out of revenge because he believed the teacher's brother had molested his sister three years earlier, and he continued uploading the AI generated content even after the police began investigating.[3] This incident illustrates how easily available AI tools now allow abusers to target women without needing any original intimate images, turning ordinary photos into sexualised, damaging content that spreads quickly and is hard to remove. Technology has amplified concerns about the misuse of digital tools in perpetuating the longstanding problem of revenge porn, allowing it to spread more rapidly and widely. The viral spread of deep fake videos in India involving many celebrities, especially women like *Rashmika Mandanna*[4] and *Alia Bhatt* [5] has become a disturbing trend. These videos, which splice their faces onto different bodies performing inappropriate actions, not only invade privacy but also tarnish reputations, highlighting a new dimension of revenge porn. While celebrities' cases often make headlines, the issue extends far beyond public figures. These instances are the ones that made their way to the newspaper and social media. Many instances remain hidden, affecting countless individuals who might not even be aware that they are victims.

Understanding the complexities and motivations behind this form of IBSA is crucial for developing effective strategies to combat it. The anonymity afforded by the internet, coupled with rapid technological advancements, has made it easier for perpetrators to engage in this abusive behaviour while evading detection. The rise of artificial intelligence (AI) and deepfake technology has further escalated the issue, enabling the creation of highly realistic but entirely imaginative and fabricated explicit content that can ruin reputations and cause significant psychological harm.

---

3 "Man Created obscene photos, reels of teacher to avenge sister's molestation" *Times of India* (Dec. 17, 2025), *available at*: https://timesofindia.indiatimes.com/city/surat/man-creates-obscene-photos-reels-of-teacher-to-avenge-sisters-molestation/articleshow/126044146.cms (last visited on Dec. 27, 2025)

4 Ankita Garg, "Rashmika Mandanna deepfake: 3 years jail, Rs 1 lakh fine, govt sends rule reminder to social media platforms" India Today (Nov 7, 2024) *available at*: https://www.indiatoday.in/technology/news/story/rashmika-mandanna-deepfake-3-years-jail-rs-1-lakh-fine-govt-sends-rule-reminder-to-social-media-platforms-2460104-2023-11-07 (last visited on Nov. 10, 2025).

5 The Hindu Bureau "Alia Bhatt deepfake video goes viral for the second time this year, sparks outrage" *The Hindu* (June 16, 2024) *available at*:https://www.thehindu.com/entertainment/movies/alia-bhatt-deepfake-video-goes-viral-for-the-second-time-this-year-sparks-outrage/article68296191.ece (last visited on Nov. 10, 2025).

Studies from India and comparative jurisdictions show that IBSA is widespread, underreported, and frequently intertwined with other forms of intimate partner violence, stalking, and extortion. Survivors describe IBSA as "torture for the soul",[6] marked by social rupture, the constant fear that images will resurface, an ongoing sense of existential threat, isolation from family and community, and constrained liberty in both online and offline spaces.

This article explores the multifaceted issue of IBSA, delving into its forms, motivations, and impacts on victims. It examines the challenges in preventing IBSA and delves into Sections 67 and 67A of the IT Act, examining their relevance, effectiveness, and limitations in addressing the issue of IBSA in India and the roles of various stakeholders. Furthermore, it provides an international comparison highlighting best practices. Also, the paper argues that India now needs a dedicated, survivor-centred and technology-aware framework that directly names IBSA, covers AI-generated and morphed images, and ensures fast takedown of content, better police response, and meaningful support services for survivors.

II Understanding IBSA: Forms, Motivations, and the impact of AI-driven deepfakes

The concept of "revenge porn" has evolved significantly since its first recorded use in July 2002 to describe a man's retaliatory actions against his ex-girlfriend by posting non-consensual sexual photographs of her on a dumpster and subsequent inclusion in the Merriam-Webster dictionary.[7] The term is defined as "sexually explicit images of a person posted online without that person's consent, especially as a form of revenge or harassment."[8] Encapsulates a form of digital abuse done with malicious intent, emphasising its use as a tool for humiliation and control. The landmark case of *State of West Bengal* v. *Animesh Boxi*[9] brought the term "revenge porn" into the Indian legal lexicon. Animesh Boxi was found guilty of distributing intimate images and videos of his ex-partner without her consent after their relationship ended. The court decided to sentence Boxi to imprisonment. Still, it referred to the victim as a 'rape survivor', which undermines the other dimensions of revenge porn that involve issues of consent, privacy, responsible use of technology and the insufficiency of legal structure to address the same.

William Shakespeare's famous line from "Romeo and Juliet", "What is in a name? That which we call a rose by any other name would smell just as sweet", suggests that the essence of an object remains the same regardless of its name. While this notion

6 Clare McGlynn, Kelly Johnson, *et.al.*, "It's torture for the Soul': the Harms of Image-Based Sexual Abuse" 30(4) *Social & Legal Studies* 541-562 (2020).

7 Nicola Henry, Clare McGlynn, *et.al.*, *Image-based Sexual Abuse: A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery* 3 (Routledge, New York, 2021).

8 "Revenge Porn", Merriam Webster *available at*: https://www.merriam-webster.com/dictionary/revenge%20porn (last visited on Nov. 10, 2025).

9 *State of West Bengal* v. *Animesh Boxi* GR: 1587/17.

holds in the context of the play, in real life, names carry significant weight and implications, particularly when discussing sensitive issues which have societal implications. The term "revenge porn" carries specific connotations that shape how people perceive the crime. It implies an act of retaliation, suggesting that the victim may have provoked the perpetrator, which can inadvertently lead to victim-blaming. This limited understanding can affect how society and the legal system address the issue. The term "revenge porn" is problematic for several reasons. It inaccurately suggests all non-consensual image sharing is motivated by revenge, ignoring other motives like sexual gratification, monetary gain, social status, or a desire for power and control.[10] It focuses only on ex-partners, overlooking the unfamiliarity of the perpetrator and other forms of digital abuse like surreptitious filming.[11] It implies victim-blaming by suggesting the victim provoked the perpetrator.[12] Comparing non-consensual sharing to commercial pornography misidentifies the harms involved and fails to capture the diversity of images. Finally, it focuses on the image content rather than the abusive actions. Sextortion, Sexting Involuntary Porn, and Cyber/Virtual Rape are some of the many synonymous terms used. These terms attempt to capture different facets of the crime. Despite these attempts, no single term fully encompasses the complexities of these crimes, especially with the advent of AI morphing and deepfakes. AI has made it easier to create non-consensual explicit content, complicating the crime further. The terminology must evolve to reflect these advancements and their implications accurately. That is how the scholars got more inclined towards the usage of IBSA and Non-Consensual Dissemination of Images (NCDII).

Both terms are broader and include all three principal actions: taking or creating, sharing without consent, and making threats. It can be in a private or public space. This also includes the covert filming of individuals' private parts, such as through "up-skirting" and "down blousing," as well as recording consensual sexual encounters without the other person's knowledge or consent.[13]

As technology is involved, it also covers the creation of deep fakes, "an image or recordings that have been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said"[14], that

10 *Supra* note 7 at 4.

11 *Ibid.*

12 *Supra* note 7 at 4; Senthil Amudhan, Manoj Sharma, *et.al.*, "Snapping, sharing, and receiving blame: A systematic review on psychosocial factors of victim blaming in nonconsensual pornography" 33 *Industrial Psychiatry Journal* 3-12 (2023).

13 Asher Flynn and Nicola Henry, "Image-Based Sexual Abuse: An Australian Reflection, Women and Criminal Justice" *Women & Criminal Justice* 1-14 (2019).

14 "Deepfake", Merriam Webster, *available at*: https://www.merriamwebster.com/dictionary/deepfake#:~:text=deep%C2%B7%E2%80%8Bfake%20%CB%88d%C4%93p%2D%CB%8Cf%C4%81k,not%20actually%20done%20or%20said (last visited on Nov. 10, 2025).

sexually depicts the victim. Technology has widened the motives behind revenge porn and other forms of IBSA by making abuse easier, faster, and more remote from the victim's everyday life. When intimate images could be shared only in private or on physical media, people generally needed a strong personal grievance or ongoing relationship to invest the effort and take the risk. Now, smartphones, instant messaging, and social media platforms allow images to be captured, stored, and circulated in seconds, often with little fear of being caught. This low effort and high impact environment encourage people to act on momentary anger, jealousy, or spite, because one click can inflict serious, visible harm on a victim's lives.[15] New editing tools and AI deepen this shift in motives. This has enabled political and ideological uses of IBSA for example, targeting female journalists, activists, or celebrities to silence them or discredit their work, where the motive is control and public shaming rather than private revenge.[16] At the same time, platform economies and content driven monetisation create financial incentives, "leaked" or doctored images can draw clicks, followers, and sometimes direct income, so profit and online visibility become additional motives to keep producing and circulating abusive material.

III Impact on victims: Types of harms

IBSA inflicts a multitude of harm on victim-survivors, predominantly women. As Martha Nussbaum highlights, the online objectification of women can be seen as an attempt by some men to "restore the patriarchal world before the advent of sex equality, the world in which women were just tools of male purposes."[17] Victims of IBSA suffer a wide range of harms, including emotional distress, social stigmatisation, and even physical danger. The psychological impact of having intimate images disseminated without consent can be devastating, leading to long-term trauma and a need for comprehensive support systems. These harms can be categorised into direct and indirect effects, each contributing to the pervasive and damaging consequences experienced by victim-survivors.

Direct Harms

Physical and mental harm

IBSA causes severe psychological trauma, including anxiety, depression, and emotional distress. Victims experience a profound violation of their personal and bodily integrity, which can lead to long-term mental health issues.[18] In addition to this, victim blaming

15 Debarati Halder and Subhajit Basu, "Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India" 34(2) *Information & Communications Technology Law* 163-186 (2025).

16 *Ibid.*

17 Clare McGlynn and Erica Rackley, "Image-Based Sexual Abuse" 37(3) *Oxford Journal of Legal Studies* 544 (2017).

18 *Id.* at 545.

is a common practice, where victims will face the consequences of taking their private picture in the first place and sharing it.[19] Consequently, this makes it challenging for a victim of non-consensual pornography to approach the court system for assistance.

Professional and economic harm

Victims often face significant professional and economic harm. The public dissemination of intimate images can lead to job loss, hinder career progression, and result in financial instability.[20] Employers may unjustly view the victim as a liability, further compounding their professional challenges.[21]

Violation of fundamental rights

IBSA violates the fundamental rights to dignity, privacy, and freedom of sexual expression and autonomy.[22] The deliberate disregard for the victim's self-worth perpetuates societal attitudes that objectify and dehumanise individuals, particularly women.

Public v. private privacy

The breach of trust inherent in IBSA, whether images were consensually created or not, undermines privacy expectations. This breach extends beyond the mere exposure of intimate content, including a betrayal of trust and confidentiality. The distinction between public and private spheres in privacy protection must be challenged to ensure equal safeguards in all contexts.[23]

Indirect Harms

Inhibiting sxual autonomy and expression

IBSA restricts an individual's confidence in the security of their privacy and dignity, undermining their rights to sexual autonomy and expression.[24] This fear can deter victims from freely expressing their sexuality and asserting their rights, restricting their ability to lead fulfilling lives.

Cultural harm

IBSA contributes to a cultural environment that trivialises the creation and distribution of private sexual images without consent. Perpetrators are often unpunished, while

19 Senthil Amudhan, Manoj Sharma, *et.al.*, "Snapping, sharing, and receiving blame: A systematic review on psychosocial factors of victim blaming in nonconsensual pornography" 33 *Industrial Psychiatry Journal* 3-12 (2023).

20 *Id.* at 4.

21 *Supra* note 17 at 545.

22 *Id.* at 546.

23 *Id.* at 547.

24 *Id.* at 548.

victims are unfairly criticised or blamed for the negative evolution of their morality.[25] This cultural acceptance not only exacerbates individual harm but also perpetuates societal norms that reinforce gender inequality and discrimination.[26]. The widespread dissemination of private sexual images without consent amplifies the harm inflicted on victim-survivors of IBSA. Addressing these harms requires comprehensive legal protections, robust support systems for victims, and efforts to challenge and change cultural attitudes that enable such abuses.

IV Key challenges in addressing image-based sexual abuse

IBSA comes with a range of complex legal, technological and social challenges which negatively impacts the efficiency of prevention, policing and prosecution. Though many jurisdictions have started to recognise and criminalise IBSA the legal frameworks are inconsistent, limited in scope and many do not address emerging forms of harms like fake or altered images or threats to share intimate photos. Laws differ significantly from place to place, and many do not cover things like fake or altered images or threats to share intimate photos. Victims have to prove they've been harmed, which can be challenging, and there's often no guarantee their identities will stay private. This can lead to further public embarrassment and distress. It is also difficult for police to catch perpetrators because they can conceal their identities online. Plus, there is insufficient awareness about these laws, and many victims face blame or misunderstanding. Additionally, policing and prosecuting IBSA presents numerous challenges that hinder effective law enforcement and justice for victims.

Rapid uncontrollable spread of images

One of the challenges in addressing the non-consensual dissemination of intimate images is the ease with which these images can be copied and republished. In the digital age, images can be duplicated effortlessly with a simple click. Once an intimate image is uploaded online, it can be downloaded, shared, and re-uploaded across various platforms and devices countless times.[27] This rapid and widespread distribution can occur within minutes, making it extremely difficult to track and control the dissemination of the image. Different online platforms vary in their content moderation policies and technological capabilities. While some platforms may have robust systems in place to detect and remove non-consensual intimate images, others may lack the necessary resources or technology to do so effectively.[28] This inconsistent

---

25 *Supra* note 19 at 5.

26 *Supra* note 17 at 549 -551.

27 Nicola Henry and Alice Witt, "Governing Image-Based Sexual Abuse: Digital Platform Policies, Tools, and Practices" in J. Bailey, A Flynn, *et.al.* (eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* 749–768 (Emerald Publishing Limited, Leed, 2021).

28 *Ibid.*

platform governance further complexify/perplex efforts to contain the spread of such material.

Variability in Legal Coverage

The nature of IBSA laws varies significantly across jurisdictions, leading to inconsistent protection for victims. This inconsistency creates gaps in the legal framework, making it difficult to address all IBSA forms effectively.

Many jurisdictions do not include digitally altered images or "fake porn" in their criminal laws. "Fake porn" or "deepfakes" involve the use of digital technology to change videos or photographs to make them sexual.[29] The difficulty in distinguishing between fake and real images can lead to significant harm and harassment for victims. Victims of digitally altered images experience similar distress as those whose authentic images are shared non-consensually, yet the legal protection is often inadequate. There is no consistency in laws that criminalise threats to share nude or sexual photos despite the significant psychological impact such threats can have on victims.[30]

Threats to sharing images can coerce victims into staying in abusive relationships or engaging in unwanted acts, thereby extending the perpetrator's control and causing prolonged psychological trauma. This omission in the law fails to recognise the coercive power of such threats. Victims often face significant challenges in identifying the person responsible for publishing intimate images without consent. Even when a suspect is identified, gathering sufficient evidence to prove their involvement can be daunting.[31] The anonymity provided by the internet, combined with technological tools like encryption and Virtual Private Networks (VPNs, allows perpetrators to conceal their identities and locations. This anonymity makes it challenging to trace the origin of the images and hold the responsible parties accountable. As a result, even if a specific instance of image distribution is halted, new instances can arise from different sources. The pervasive nature of digital content means that victims can never be entirely sure that the images have been permanently removed, leading to ongoing psychological distress.[32]

Adding to this, many jurisdictions primarily require proof of harm or distress to prosecute IBSA cases, which can be a substantial barrier to justice.[33] This requirement places an undue burden on victims, as distress is subjective and difficult to quantify. The necessity to prove harm can hinder prosecutions, allowing perpetrators to evade justice even when their actions have caused significant distress to the victim. The lack of anonymity provisions can further traumatise victims and deter them from reporting

29 *Supra* note 7 at 137.

30 *Id.* at 138.

31 Vaishnavi Sharma," Understanding Non-Consensual Dissemination of Intimate Images Laws in India with Focus on Intermediary Liability" 14(4) *NUJS Law Review* (2021) 5.

32 *Supra* note 13.

33 *Supra* note 7 at 138.

incidents of IBSA.[34] Public exposure can lead to secondary victimisation, increasing the psychological harm suffered and discouraging others from seeking justice. Further, there is a general lack of awareness and understanding of IBSA laws among the public and potential victims.[35] This lack of awareness can prevent victims from seeking justice and reduce the effectiveness of the laws. Victims may not report incidents without widespread knowledge of legal protections, and perpetrators may not be deterred.

Policing and jurisdictional issues

The digital nature of IBSA often involves cross-jurisdictional challenges, making it difficult for law enforcement to track and prosecute offenders. The anonymity provided by the internet, through measures such as encryption, VPNs, and proxy servers, further complicates the identification of perpetrators.[36]

Resource constraints

Policing IBSA is resource-intensive, requiring specialised training and technology. Many law enforcement agencies lack the necessary resources and training to handle IBSA cases effectively.[37]

Victim-blaming attitudes

Victim-blaming attitudes within the criminal justice system can hinder the provision of appropriate support and responses to victims. This can discourage victims from coming forward and undermine their confidence in the justice system.[38] Also, there is a need for comprehensive victim support services that address the unique needs of IBSA victims, including psychological support, legal assistance, and practical help in removing images from the internet.

Taken together these technological, legal, and social factors creates a highly complex environment for addressing the issue of IBSA. Effective responses to mitigate this issue require a multidimensional approach including technological advancements, more robust legal frameworks, and international cooperation to hold perpetrators accountable. Equally important is development of robust victim support systems and public awareness to incentivise prompt reporting and minimise stigma.

V Emerging global regulatory trends -Legal position in US, Europe and BRICS countries

Defining legal boundaries for IBSA, or revenge porn as most commonly understood, is difficult but critical. This abuse involves the NCDII of the victim to third parties,

34 *Id.* at 139.

35 *Id.* at 140.

36 *Id.* at 24.

37 *Supra* note 13.

38 *Supra* note 19.

irrespective of how the images were taken or disseminated. Majorly it involves two elements- (i) creation of explicit images and (ii) distribution without consent. In light of recent technological advancements or tools available for digitally altered imagery, it may also go beyond capturing image/recording video and can include producing digitally altered nudes or pornographic images or videos or threatening to create and distribute with or without knowledge.[39] Using terms like 'revenge porn' can be problematic as it restricts the act to ex-partners as it would create a loophole for other perpetrators of IBSA. IBSA can also involve sexual assault recordings or images obtained by hacking or digitally altered nude or sexual abuse imagery and deep fakes.[40]

Efforts are being made in different jurisdictions to address the spectrum of image-based sexual abuse through the introduction of various criminal and civil laws, though covering partially certain forms of IBSA as of now.[41] Legal frameworks addressing these issues swing between narrow and broad coverage, struggling to achieve efficiency and withstand constitutional scrutiny.

Despite these legislative attempts by governments worldwide, enacting or amending of criminal and civil laws, there remains a significant 'justice gap'[42] within their legal systems to address the pervasive harms and provide redressal to victims of IBSA. This section covers the specific laws enacted by different countries, though the laws are varying widely in scope and effectiveness. A comparative inquiry into the legal developments in the United States of America, Europe and BRICS countries highlight growing trends including civil remedies under tort law, criminalisation of nonconsensual sharing of intimate images, protection under privacy laws as well as imposition of heightened responsibility on the intermediaries and social media platforms.

Though civil law remedies have been available under tort law generally as well as under specific legislations across countries, they have been found inefficient in providing relief to the victims. A well-defined criminal law response is key to addressing the NCDII. Many jurisdictions have enacted laws penalising such dissemination targeted on the content of the distributed images, covering scenarios like consensually captured

---

39 Asher Flynn, Anastasia Powell, *et. al.*, "Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse" 62(6) *The British Journal of Criminology* 1341–1358 (2022).

40 Synthetic sexually explicit media (SSEM) is emerging as a small spectrum of IBSA due to the emergence of synthetic media technologies. *Supra* note 21.

41 Erica Rackley, "Seeking Justice for Victim-survivors of Image Based Sexual Abuse" in Nicola Henry, Clare McGlynn *et.al.*, (eds.) *Image-based Sexual Abuse: A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery* (Routledge, New York, 2021).

42 *Id.* at 135.

images shared without consent, stolen images or non-consensual capturing and sharing of intimate images like images or recordings of sexual abuse, rape etc.[43]

United States

USA does not have any specific federal law on IBSA, though there have been debates going on since 2010 on the viability of NCDII given the challenges posed by wide immunity to free speech under the First Amendment. Arguments support criminalisation on the basis of obscenity, being the unprotected form of speech under the First Amendment.[44]

Title 18 of the US Code section 1801,[45] the video voyeurism law makes it a federal crime to 'capture' the picture of the private part of someone, intentionally or knowingly, without their consent or when they have a reasonable expectation of privacy. This law punishes the perpetrator with imprisonment for up to one year when such a crime is committed against a US national both within and outside US boundaries, including all territorial boundaries and States that did not have video voyeurism laws at the time this federal law was passed.

However, the defences against a charge under this law would be available where the victim consented to the act. Also, when the victim was not in a place where they had a reasonable expectation of privacy, like a public place, the charge will not apply or when there was an absence of intention on the part of the perpetrator, for instance, when a photojournalist accidentally captures someone in the mode of undress[46] without intending to commit video voyeurism.

43 *Supra* note 28 at 5.

44 Danielle Keats Citron and Mary Anne Franks, "Criminalising Revenge Porn" 49 *Wake Forest Law Review* 345 (2014).

45 Video Voyeurism Prevention Act, 2004.

46 Video Voyeurism, *Eisner Gorin LLP, available at*:https://www.thefederalcriminalattorneys.com/video-voyeurism(last visited on Jan. 8, 2025).

Many states in the US have adopted their own statutes in response to many high-profile cases. New Jersey was the first state to criminalise NCDII.[47] The New Jersey Code of Criminal Justice, Section 2C:14-9 - Invasion of privacy, degree of crime; defenses, privileges (2013):

> It amounts to a third-degree crime punishable by three to five years if a person knowingly captures, records or reproduces an image of another person whose intimate parts are exposed or engaged in sexual activity without consent or where a reasonable person would expect privacy and also the non-consensual disclosure/dissemination of such images or recordings except for lawful purposes.

Another state law, the CA Penal Code[48] currently applies to a person who intentionally distributes or causes the image of intimate body parts or sexual acts of another person only when in breach of an agreement to keep them private. The law has a limited approach and does not cover hacked images. Besides, the liability is conditional on the intention to cause serious emotional distress to the victim, placing a heavy burden of proof on the victim defendant.

The Illinois statute on NCDII criminalised intentional dissemination of sexual images of an adult without their consent and obtained under the reasonable expectation of privacy provided the victim is identifiable directly from the image or through associated information. Punishments include imprisonment of one to three years and a fine of up to twenty-five thousand USD, as well as forfeiture of profits obtained by the illegal act deterring financially motivated perpetrators.[49]

47 The New Jersey Code of Criminal Justice, Section 2C:14-9 - Invasion of privacy, degree of crime; defenses, privileges (2013):

> An actor commits a crime of the third degree if, knowing that he is not licensed or privileged to do so, he photographs, films, videotapes, records, or otherwise reproduces in any manner, the image of another person whose intimate parts are exposed or who is engaged in an act of sexual penetration or sexual contact, without that person's consent and under circumstances in which a reasonable person would not expect to be observed. c. An actor commits a crime of the third degree if, knowing that he is not licensed or privileged to do so, he discloses any photograph, film, videotape, recording or any other reproduction of the image of another person whose intimate parts are exposed or who is engaged in an act of sexual penetration or sexual contact, unless that person has consented to such disclosure. For purposes of this subsection, "disclose" means sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, publish, distribute, circulate, disseminate, present, exhibit, advertise or offer. Notwithstanding the provisions of subsection b. of N.J.S.2C:43-3, a fine not to exceed $30,000 may be imposed for a violation of this subsection

48 The California Penal Code, Section 647(j)(4)(A) and (B) (CA Penal Code x 647(j)(4)(A) -(B) (2013)).

49 Beyens, J., and Lievens, E., "A Legal Perspective on the Non-consensual Dissemination of Sexual Images: Identifying Strengths and Weaknesses of Legislation in the US, UK and Belgium" 47 *International Journal of Law,Crime and Justice* 31 (2016).

The 2022 Violence Against Women Act (VAWA) Reauthorisation[50] introduced a new provision on non-consensual pornography as a civil rights action enabling victims to claim damages or injunctive relief against such acts. Protection from Harassment Act, 1997 provides a civil remedy for harassment, which may include IBSA, allowing victims to claim damages.

European countries

United Kingdom

The England and Wales Criminal Justice and Code Act, 2015, under ss. 33 and 35 & s,51 of Justice Act, 2016, criminalises non-consensual 'disclosure'- electronic and physical, of private sexual images or films, including altered images, with the intent to cause distress. The concept of disclosure is broadly defined to cover electronic distribution or physically showing an intimate image or video to a third person. The act prescribes a punishment of up to two years, which is harsher than California (6 months) but less severe than New Jersey (3-5 years) and Illinois (1-3 years). The statute has defined sexual content broadly to include pictures/recordings of part of an individual's exposed genitals or pubic area but does not require nudity. The Act excludes liability for images which have been edited to become sexual, like photoshopped/ morphed images, as was held in *Marina Marshall* v. *Lenisha Augustine.*[51]

The requirement of the perpetrator acting with an 'intent'to cause distress to the victim is problematic and makes the law complex. This not only diminishes the victim's sexual agency but is also in conflict with section 33(8), which clarifies that distress is a natural consequence in such cases and does not imply intent. The Abusive Behaviour and Sexual Harm(Scotland) Act, 2016, in contrast, penalises both intentional and reckless actions, including threats to disclose as an offence, providing broader legislative coverage than English and Welsh legislation.[52]

Belgium

The Belgian Criminal Code (BCC), Article 371/1, amended in 2015, criminalises 'showing, rendering accessible, or disseminating nude images or sound or video recording of explicit sexual acts without consent, punishable with imprisonment of six months to five years but no monetary fine.

In Belgium, the production, distribution, possession and acquisition, even watching or access to Child Sexual Abuse Material is criminalised. Article 417/43 of BCC post

50 Violence Against Women Act, *Feminist.com available at*:https://www.feminist.com/resources/explainer/violence-against-women-act.html#:~:text=Although the provision that allowed,2005, 2013, and 2022.(last visited on Dec. 8, 2025).

51 *Marina Marshall* v. *Lenisha Augustine* [2009] DOMHCV, 2001/0319 (DOMHCV).

52 The definitions of 'intimate situation'; film; and 'photograph' include a wider range of intimate images than the corresponding definitions in English law.

2016, explicitly mentions that realistic images depicting a non-existent minor engaged in a sexually explicit act, or depicting the sexual organs of that minor for primarily sexual purposes. It includes virtual CSAM and is in line with Cybercrime Convention. Article 417/9 of BCC criminalises displaying, making accessible or distributing visual or audio content of a naked person or a person performing an explicit sexual act without his or her consent or knowledge, even if he/she has consented to the creation of the content. The penalty is severe for aggravated forms -acting with malafide intention or for reasons of profit as per Article 417/10 BCC. Refusal to provide technical support to remove non consensual sexual images upon request of prosecution is also punishable under Article 417/56 BCC.

Australia

The Commonwealth Criminal Code of 1995 and the Enhancing Online Safety Act, 2015(amended by the Non-Consensual Sharing of Intimate Images Act, 2018)[53] criminalises revenge porn. Most Australian states except Tasmania. Have specific laws criminalising non-consensual image dissemination with penalties of up to three years imprisonment. Australian law prioritises the intent to distribute and the absence of consent over the intent to cause harm and provides robust measures against revenge pornography. The Enhancing Online Safety Act, amended in 2018[54] provide civil penalties, allowing the victims to report to the safety commissioner.[55]

Out of the jurisdictions covered, Australia has some of the most advanced legislative responses to IBSA globally. Almost all laws in Australia reflect the view that the intent to distribute and absence of consent is sufficient to constitute the offence, disregarding the element of 'intent to cause harm or distress'. Laws under NSW[56] and ACT's[57] NCP[58] provisions can be considered as being ahead of the other state laws since they contain retraction provisions, which allow the court to order the offender to take reasonable action to remove, retract, delete an intimate image, etc., in addition to the penalty imposed. New Jersey and Illinois statutes prioritise lack of consent as the core criterion for criminality, recognising the victim's sexual agency. In contrast,

53 Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, sch. 2. Amendment in 2018 added s. 474.17A creatingoffence which involves the transmission, making available, publication, distribution, advertisement or promotion of private sexual material.

54 Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018, s. 44B.

55 Kushanthi S. Harasgama and Paramie Munasinghe, "Combatting Non-Consensual Pornography through Legislation: A Multi-Jurisdictional Analysis", *SSRN* (July 26, 2021). *available at*: https://ssrn.com/abstract=3893483 or http://dx.doi.org/10.2139/ssrn.3893483 (visited on Nov. 15, 2025).

56 Crimes Act 1900 (NSW) and Crimes Amendment (Intimate Images) Act 2017.

57 Australian Capital Territory (hereinafter referred to as "ACT").

58 Crimes (Intimate Image Abuse) Amendment Act, 2017.

California and UK codes are similar in the requirement of proof of intent by the perpetrator to cause distress, thereby avoiding penalizing unintended disclosures. These laws vary in scope and effectiveness.

BRICS countries

IBSA, as a systematic class of sexual crimes against women and children, remain virtually unrecognised in scholarship and legislation in most BRICS countries including India.[59]

South Africa

South Africa has the most explicit legal framework on INSA. It uses multiple, overlapping legal tools to respond to non-consensual imagery in digital medium. The Films and Publication Amendment Act, 2019 (FAPAA) in section18F(1)[60] targets pornography and harmful digital content, categorically prohibits IBSA and child pornography. It expands the definition of film to cover internet content. It also inserted a provision prohibiting filming and distribution of films and photographs depicting sexual violence and violence against children.[61] It introduced a new offence for anyone who knowingly shares private sexual images or videos without the consent of the person depicted to cause distress/harm punishable with imprisonment for a term upto two years with fine and upto four years plus fine if the person depicted is identifiable. Focusing on consent and harm, it protects the sexual privacy and human dignity in digital environment. However, the requirement of proving intention to harm the person depicted in the image is problematic, complicating liability and emphasising on motive rather than *dolus* (*mens rea*)[62]

The Act also imposes obligations on the intermediaries to disclose the identity of the person who publishes prohibited content, a private sexual photograph or film or a film or photograph depicting sexual assault and violence against children.[63]

---

59 Aanchal Kabraand Rohit Gupta "Carving an Indian Mosaic for Image-Based Sexual Abuse" 34(1) *National Law School of India Review* (2022) 207 *available at*: https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1992&context=nlsir (last visited on Dec. 10, 2025)

60 S. 18(F)(1)- [with effect from March 1, 2022]
No person may expose, through any medium, including the internet and social media, a private sexual photograph or film if the disclosure is made— *(a)* without the consent of the individual or individuals who appear in the photograph or film; and
(b) with the intention of causing that individual harm.

61 S. 18G. Prohibition against filming and distribution of films and photographs depicting sexual violence and violence against children. The provision inserted by FAPAA, 2019 came into effect since March 1, 2022.

62 Blake Martin, "Image Based Sexual Abuse and the Requirement of Motive under FAPAA: A Critical Assessment" *Obiter* (2024) *available at:* https://doi.org/10.17159/m4hg4w41 (last visited on Dec. 6, 2025).

63 Films and Publication Amendment Act, 2019 (FAPAA), s. 18F(6).

Originally, the FAPA in 1996 and 1999[64] version defined child pornography narrowly to include a visual representation, or a scene of a child/ a person depicted as a child engaged in a sexual act, which arouse erotic rather than aesthetic feelings. The 2004 amendment expanded this definition to include any image or any description of a person, real or simulated, under the age of 18 years that depicts sexual conduct or participation or assistance in such conduct or showing or describing the body, or parts of the body, of such a person in a manner or in circumstances which, within context, amounts to sexual exploitation, or in such a manner that it is capable of being used for those purposes of sexual exploitation".[65] The broadened definition criminalises not only the sexual act but also the creation, storage and distribution of such exploitative images with or without consent, in any medium. It becomes crucial in regulating IBSA involving/relating to children by aligning child pornography with the dignity, privacy and safety of the child, which lies at the core of IBSA.

South Africa High Court[66] held that even when there is no direct capture by the accused, recording of minors in situations that suggested sexual exploitation would fall under the definition of child pornography under FAPAA, 2004. The accused in this case had deliberately put mobile phone in bathroom knowing the children would be naked while bathing and then downloaded in an internet enabled desktop, indicative that the accused appellant intended to create child pornography.[67]

In addition to this, Chapter III of Criminal Law (Sexual Offences and Related Matters) Amendment Act (SORMA), 2007 covers a very wide range of sexual offences against children- (i)consensual sexual act with children[68], and (ii) sexual assault, sexual grooming, exposure of children to sexual offences/acts/ genital organs, child pornography and use of children for pornographic purposes.[69] Though the Act is not designed specifically to include online intimate image abuse, it can apply to IBSA if minor or persons with mental disabilities.[70] Sexual exploitation may involve activities like prostitution and CSAM/Combat Child Sexual Exploitation Material (CSEM).[71]

---

64 FAPA,1996 s. 24B; *See*:*Beale* v. *S*, 2019 (2) SACR 19 (WCC) (decided on 3rd May 2019).

65 *Wilms* v. *S* [2020] 1 All SA 286 (WCC) (11 September 2019), South Africa High Court in para 39.

66 *Id.* para 37.

67 *Id.,* para 41.

68 Criminal Law (Sexual Offences and Related Matters) Amendment Act (SORMA),2007, ss. 15,16.

69 *Id.,* ss. 17-20.

70 Criminal Law (Sexual Offences and Related Matters) Amendment Act Amendment Act, 2021, ss. 25 and 26.

71 Daniel Manoj, Ranjit Immanuel James *et. al.*, "Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation" 4 *Child Protection and Practice* (2025).

The Cybercrimes Act[72] deals with revenge pornography or non-consensual pornography. This provision, unlike FAPAA, removes the requirement to prove 'intention to cause harm' and instead focusses on intentional or unlawful disclosure as well as threat to disclosure covering psychological and coercive harms caused by such conduct. It applies particularly in digital context, taking in account the role of social media platforms and messaging apps and digital storage. The provision aligns with constitutional right to dignity as well as provides an alternative to crime under FAPAA, in case proving intent to cause harm may get difficult.

Brazil

There is no dedicated legislation on IBSA rather it has different laws to tackle different stages of IBSA. The Brazilian Penal Code has undergone renewal and changes in relation to sexual crimes ensuring sexual freedom as an aspect of constitutional value of human dignity and individual self-determination in this regard. In 2018 it created a criminal offence under Article 218C of the Penal Code[73] criminalising the non-consensual offering, exchanging, making available, transmitting, selling or exhibiting for sale, distributing, publishing or disseminating, by any means, of sexual or nude content punishable with imprisonment for one to five years or an aggravated penalty when the there is a purpose to humiliate or to take revenge on account of an intimate relationship with the victim. Where the content has been recorded or collected with the consent of the victim, it shall still be punishable if the circulation or dissemination is without consent. This is in conformity with the global practices. Where the victim is under 18 years of age i.e. a minor, the Statute of Child and Adolescent (ECA)[74] applies which criminalises the recording, dissemination and possession of sexualised imagery involving minors and carries harsher penalties upto including imprisonment upto eight years. More recently, the Digital ECA[75] was passed, providing a framework for protecting children(under 12 years of age) and adolescents(12-18years of age) in response to series of videos on adulteration of children posted by a social media influencer. It imposes proactive child safety and data protection obligations on technology providers for any product or service accessible by minors and on intermediaries to remove content violating children's rights including sexual abuse and exploitation.[76]

The second provision is article 216B which criminalises unauthorised recording of sexual intimacy covering the person who produced, photographed, or filmed scenes of nudity or sexual acts of an intimate or private nature.

72 Cybercrimes Act 19 of 2020, s.16.

73 Penal Code Amendment(Law no. 13/718/2018).

74 Law No. 8,069/1990.

75 Law No.15,211/2025.

76 Anna Sophia Oberschelp de Meneses, "Diego Bonomo, Brazil Adopts Law Protecting Minors Online", *Global Policy Watch*, Oct. 9, 2025 *available at:* https://www.globalpolicywatch.com/2025/10/brazil-adopts-law-protecting-minors-online/ (last visited on Nov. 7, 2025).

The Maria da Penha Law, 2006,[77] basically a law to protect women against domestic violence, covers sexual, psychological violence beyond physical violence. It recognises ISBA a a domestic, gender-based violence by the perpetrators in intimate and close relationships and allows for protective orders, though is seen to be not applied in internet cases. In addition to the criminal penalties, civil penalties such as compensation are allowed under Article 186, 187 and 927 of the Civil Code.

Brazilian laws are progressive and align with best practices though, currently do not explicitly address AI generated sexual content and deepfakes.

Russia

Russia does not have a dedicated law on IBSA or revenge porn but relies on general privacy, obscenity, public order and data laws. Article 137 of the Criminal Code is a provision covering invasion of privacy and prosecutes unauthorised collection or dissemination of information related to private life of an individual, including videos and images, provided it constitutes victim's personal or family secret. Penalties are harsher if committed using mass media or internet or done in abuse of official position. However, if the access or intrusion is with consent, subsequent dissemination of the photo or video is not made culpable by this provision.[78]

Article 242 applies to illegal production and distribution of pornography, provided the image qualifies as pornographic before the court.[79] However, the provision does not cover AI manipulated images and deepfakes. In 2024, a new law[80] introduced article 272.1 which though enacted to cover illegal use of data obtained through hacking, applied in cases where intimate images were included in the hacks. Similarly, article 163, provision on extortion, can be used when the perpetrators threaten to publish intimate images for extorting money, sexual favours etc. Since article 152.1 of the Civil Code protects image rights, use of a citizen's image to create non consensual porn is illegal under the said provision, but mere content removal for copyright violation may not be sufficient deterrent for such dangerous acts.[81]

China

China also does not have a standalone law to address IBSA. It addresses cases on non consensual intimate images under existing criminal law provision on insult and

77 Law 11.340/2016.

78 Sergey Nikolaevich Klokov, Pavel Aleksandrovich Tikhonov, "Producing and/or Distributing Intimate Images of a Person without its Consent" 4(4) *Legal Issues in the Digital Age* (2023).

79 *See*, e.g.: Cassation Ruling of the Supreme Court of the Russian Federation No. 18-UDP20-36-K4. 10.06.2020/ *available at:* URL: http://vsrf.ru/stor_pdf.php?id=1893716 (last visited on Jan. 7, 2026).

80 Law (421-FZ) enacted in Nov. 2024.

81 *Supra* note 78.

defamation, Civil Code, 2021 and Cybersecurity Law. Within the Criminal Law, article 246 is applied when intimate images cause serious damage to the individual's reputation and qualify as insult or defamation.

Additionally, conduct involving pornographic material maybe prosecuted under provisions governing obscenity. Article 363 criminalises production, duplication, publication, selling or dissemination pornographic materials or profit purposes with penalties ranging from imprisonment upto three years and fine and upto ten years in serious circumstances. Article 364 punishes dissemination of pornographic materials including images, films or videos with imprisonment upto two years or three to ten years when circumstances are serious like at large scale or dissemination is to a minor under 18 years. For the purposes of these offences, article 367 defines pornographic material to include any content that explicitly portray sexual conduct.

Adult IBSA is generally grounded in the Civil Code of the People's Republic of China which acknowledges and protects right to privacy and right to image, enabling injunctive relief, taking down/erasure of the content and compensation for damages to the victims against the perpetrators and online platforms.

Administrative sanctions are available under the recently revised Public Security Administration Punishments Law, 2005(PSAPL)[82] which cover and penalize,[83] production, transportation, copying or renting any obscene content including picture, film and video recording through computer network, telephone or other telecommunication tools. These acts may attract administrative penalties outside the criminal justice system such as confiscation under article 11 or detention for 5-10 days depending upon the severity of the conduct.

Also, to address the emerging forms of IBSA, the Deepfake framework imposes obligation to label AI-generated or synthetic content to prevent deepfake and face swapping pornography-deepfake enabled sexual exploitation. Hence, China has adopted a fragmented and indirect response through provisions on defamation, pornography, privacy and cybersecurity instead of a direct and consent based dedicated framework.

Emerging trends

A comparative inquiry into the legal developments in the United States, Europe and BRICS countries highlight growing trends. The first being the global transition from a fragmented approach to a specific legal framework, recognising IBSA as a distinct legal wrong/offence rather than treating it under general offences like obscenity or defamation. Earlier countries like Australia, South Africa, Brazil and many states of US depended on laws relating to privacy, defamation or pornography which were

82 Public Security Administration Punishments Law, 2005, *(w.e.f.* Jan. 1, 2026).

83 Public Security Administration Punishments Law, art. 68.

found lacking on covering harms exclusive to IBSA. They have now enacted specific provisions targeting NCDII. Though countries like Russia and China have not come up with dedicated provisions/legislations and still rely on indirect regulation of IBSA.

Older legal approaches focussed on this conduct as obscene and pornography- of public morality. The shift from morality-based approach, modern laws on IBSA recognise as violation of constitutional right to dignity and privacy (South Africa), sexual autonomy and bodily integrity (Australia and Brazil), reflecting a broader human rights-based approach. Further countries like Australia, Brazil and US States Illinois and New Jersey base prosecutionon lack of consent to distribution, recognising that consent to create an image does not extend to the act of distribution. Some other countries like United Kingdom, South Africa and state of California make proof of malicious intention on the part of perpetrator mandatory, *i.e.,* he intended to cause distress or harm, being criticised for placing a heavy burden of proof on the victims. Motive based offences have been replaced by a more modern consent-based approach. Stricter penalties are imposed in instances of child/minor victims by almost all the jurisdictions to CSEM, and has become a global trend.

Another emerging trend is the availability of civil remedies in addition to criminal prosecution, providing a multi-layered approach allowing victims to choose civil remedies over lengthy criminal proceedings, claim monetary compensation and obtain take down and content erasure orders from civil courts. The Violence Against Women Reauthorization Act of 2022 in US, compensation claims under the Brazil Civil Code and privacy based civil actions under the Chinese Civil Code.

There are an increasing attention and acknowledgement of the role of online platforms in the spread of harmful content like non consensual intimate images. Jurisdictions like China through Cybersecurity regulations have imposed content monitoring and removal obligations and South African regulation obligates disclosure of identities of perpetrators who share prohibited content. In Australia, state laws like Australian Capital Territory and New South Wales include retraction provisions empowering the eSafety Commissioner to order content removal in such instances, addressing persistent nature of digital harm.

Lastly, there is growing tendency to respond to the concern related to emerging instances of deepfakes and AI-generated sexual imagery and AI manipulated pornography. Though many countries are yet to come up with specific legislations or provisions to cover AI generated intimate images or synthetic pornography, China has introduced deepfake labelling regulations. This technological development is projecting new regulatory challenges before countries.

VI India's legal framework on image-based sexual abuse

IBSA has been a persistent problem since the genesis of portable cameras and more recently smart phones. The infamous *DPS MMS*[84] case involving capturing/creating a video of the private sexual act between minors and its illegal distribution and bid to auction at *Bazee.com* (eBay now) highlighted first the perils of non-consensual sharing of intimate images and consequent IBSA for the first time and the inadequacy of legislative and inefficiency of the regulatory framework in India in dealing with such cyber-crimes. Since the video was created and circulated first by a minor(s), no criminal proceedings were initiated against them, but Avnish Bajaj, then Director of *Bazee.com*, was booked under IPC and then Information Technology Act, 2000 for facilitation and transmission of the obscene material but was acquitted later as the prosecution failed to establish the requisite *mens rea* and liability under the existing framework. In the amendments made subsequent to this case, intermediaries were put under an obligation to take down unlawful content hosted/uploaded within 36 hours of receiving 'actual knowledge'. In *Shreya Singhal,*[85] however, the court read down "actual knowledge" under section 79(3)(b) to mean receipt of a court order/notification directing intermediaries to remove or disable access to content expeditiously. In *re Prajwala Letter,*[86] it directed auto-deletion of content be put in place to deal with videos, imagery, sites and other similar content in relation to child pornography, rape and gang rape.[87]

Despite the exponential surge in the incidents of IBSA post COVID, even today, the issue of IBSA is explicitly not addressed by a single dedicated statute in India; rather, it can be addressed through a combination of laws- criminal law, Information Technology Act, 2000 (IT Act), Protection of Children from Sexual Offences Act, 2012 (POCSO) and Digital Personal Data Protection Act, 2023 (DPDP ACT, 2023), with each law covering some specific aspects of the abuse.

Section 354C (Voyeurism) under the Indian Penal Code, as amended in 2013, was particularly focused on the dissemination of consensually captured images without consent. The new provision, section 77 under the Bhartiya Nyaya Sanhita (BNS), though in substance has retained the offence of voyeurism, it has adopted a gender-

84 Anurag, "DPS MMS Scandal: India's first MMS scandal where a video of 2 students was sold online"(20 September 2020) *available at:* https://www.opindia.com/2022/09/dps-mms-indias-first-mms-scandal-where-the-video-was-sold-on-ebay/ (last visited on Jan. 8, 2026).

85 (2015) 5 SCC 1.

86 MANU/SCOR/45933/2017 date of order: Oct. 23, 2017.

87 Deepa Kharb, "Cyber Law" 53 *Annual Survey of Indian Law* (2017) 297.

neutral approach with respect to the perpetrator, not the victim.[88] It penalises any person, regardless of gender, who captures or circulates such image. The law now explicitly states that consent to take picture does not amount to consent for circulation of it, thereby addressing all instances of nonconsensual intimate image abuse where images are initially taken/captured/shared with consent but circulated/transmitted without consent later. However, the provision, unlike UK and Scotland laws, does not cover photoshopped or morphed images where the victim's face is transposed onto another's naked body with similar consequences and harm as unaltered images. The language of the section is not gender-neutral and applies only when the victim is a female. An explanation could be inserted in the section to address both the inadequacies.

Stalking and sexual harassment under sections 78 and 75 BNS respectively complement IBSA. Stalking involves repeated monitoring, contacting or tracking the movement through electronic means, goes hand in hand with IBSA, often in the form of harassment, threatening to publish intimate images and controlling behaviour. Sexual harassment involves using digital platform to make unwelcome physical advances, making sexually suggestive remarks or asking for sexual favours or showing pornography against will.

Where a person utters any word, makes any sound or gesture or exhibits any object in any form with the intention that it should be seen or heard, or to evade the privacy of a woman commits the offence of outraging the modesty of a woman under section 79 BNS, whether it is in physical, electronic or digital medium.

Section 292 IPC[89] penalised generally all the act of distributing obscene content that is lascivious or appeals to the prurient interest or tends to corrupt or deprave persons watching.[90] The equivalent offence under section 294 BNS incorporates the same ingredients but explicitly includes electronic materials.

Provisions under IT Act like sections 67 and 67A are broad in application and address the publication and distribution of any kind of pornographic content (text, image, painting.[91] audio, video *etc.*) in electronic form, also covering photoshopped and

88 The Bhartiya Nyaya Sanhita, s. 77-Whoever watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.

89 Corresponding S. 294 of the Bhartiya Nyaya Sanhita, 2023.

90 Raghav Mendiratta, "Non-consensual sharing of intimate images online: Solutions in Criminal, Media & Technology Laws"*Socio-Legal Review* (Oct. 19, 2020) *available at*: https://www.sociolegalreview.com/post/non-consensual-sharing-of-intimate-images-online-solutions-in-criminal-media-technology-laws (last visited on Nov. 15, 2025).

91 *Maqbool Fida Hussain* v. *Raj Kumar Pandey,* 2008 SCC OnLine Del 562.

morphed images. Section 67B is applicable where the content involves depicting children in sexually explicit acts.[92] in electronic form. It applies to the creation of digital images and recordings in any electronic form, even the abuse of others pertaining to sexually explicit acts with children.

Section 66E of the Information Technology Act, 2000, titled 'punishment for violation of privacy', is the most notable provision which punishes the 'intentional or knowing capture, publication, or transmission of images of 'private area' without consent. This section emphasises the violation of privacy of a person as a sexual offence and extends to public as well as private dissemination. The section also penalises non-consensual transmission and publication of images of a person's private area. As per the explanation attached to the section, 'capture' with respect to an image means to videotape, photograph, film or record by any means.[93] The provision has a wide approach and does not restrict liability to 'capture' by the perpetrator but also applies to cases where 'selfies' are taken by the victim and transmitted with the implied consent or in expectation of privacy but are shared further where consent is implied. When such photos are further transmitted/published by the receiver without the consent of the sender, this offence will apply.

In *Animesh Boxi,*[94] District court judge Gautam Nag made a landmark decision by applying section 66E, though superficially, marking the first conviction in India for revenge porn. Judge Nag termed the non-consensual posting of intimate images of his girlfriend by the accused on pornhub as '*virtual rape*'. The court interpreted the harm to the victim's mind and reputation under section 44 IPC, emphasising the continuous abuse the girl was to face because of the online permanence of her images. Though the judgment does not have a precedent value as a lower court judgment, the stringent punishment of five years conferred sends out a strong message to the perpetrators. The accused was convicted under multiple charges though, including sections 354C&D, 509 IPC and sections 66C, 67, 67A along with section 66E of IT Act.

The Intermediary Guidelines and Digital Media Ethics Code of 2021[95] notified by the MEITY created stringent timelines for the social media intermediaries with over five million registered users- the 'significant social media intermediaries', and were obligated to identify and moderate content depicting rape or child sexual abuse through act or simulation and deploy auto block tools.[96]

---

92 Information Technology Act, 2000, s.67B.

93 *Supra* note 28.

94 *Supra* note 9.

95 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

96 The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, GSR 139(E), 2021, s. 4 ('The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules') cited in Kabra, *supra* note 59.

The POSCO Act, 2012 (POCSO) criminalises all forms of sexual abuse including penetrative[97] and non-penetrative assault,[98] harassment[99] and pornography.[100] It expanded, particularly post 2019 amendment, the definition of pornography to cover computer generated or manipulated images, adults portraying as children as well as pornographic cartoons and anime involving children in sexually explicit act/sexual intercourse *etc.*[101] POCSO generally conforms to global practices in protecting children from sexual abuse covering wide range of sexual offences, a broad definition of pornography expressly covering pornography in electronic form[102] as computer generated and manipulated images/content even cartoons and anime depicting pornography, aligning with Budapest Convention,[103] and mandatory reporting after 2019 amendment[104] and 2020 Rules[105] for proactive protection.

Gaps and challenges

IBSA is prosecuted under a mix of IPC, IT Act and POCSO. Each of these statutes has been designed for a different context and not IBSA. The patchwork leads to inconsistent definitions of offences, posing problems for victims and enforcement agencies. Unlike South Africa FAPAA and Brazil's revenge porn law there is no dedicated/ standalone statute for countering IBSA. Though POCSO is relatively stronger and conforms to global practices, it is applicable only to child related IBSA, not adults. The 2019 Amendment expands already broad definition of pornography to include computer simulated/synthetic pornography, sufficient to address deepfakes and makes this legislation more advanced than most jurisdictions. However, there is no equivalent provision to address the same in case of adult pornography and IBSA.

VII Judicial approaches to image based sexual abuse in India

Judicial response to IBSA in India has been cautious but evolving.Courts have relied upon the provisions of IPC/BNS, IT Act and POCSO and tried to curb the menace imposing the obligation to take down or block such content on the intermediaries. Section 67 and 67A of IT Act have a broad connotation and address obscenity and

97 Protection of Children from Sexual Offences Act, 2012 s. 3-6.

98 *Id.,* s.7.

99 *Id.,* s.11.

100 *Id.,* s. 13.

101 The Protection of Children from Sexual Offences Act, 2012 s.2 (da)-
"Child pornography" means any visual depiction of sexually explicit conduct involving a child which include photograph, video, digital or computer-generated image indistinguishable from an actual child and image created, adapted, or modified, but appear to depict a child.

102 *Ibid.*

103 The Convention on Cybercrime, 2001, art.9- offences relating to child pornography; also known as the Budapest Convention on Cybercrime or the Budapest Convention.

104 The Protection of Children from Sexual Offences(Amendment) Act, 2019.

105 The Protection of Children from Sexual Offences Rules, 2020.

sexually explicit content, whereas section 66E is focused on consent and preventing violation of bodily privacy, which is more individual-centric. Courts have tended to prioritise obscenity even though arguments from the victim's side were centred on violation of privacy until the landmark *K S Puttaswamy* case.[106] which recognised the right to privacy as a constitutionally protected right under article 21, and that right to privacy also arises in varying contexts from other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III of the Constitution of India.[107] The apex court went ahead to identify the 'right to be forgotten'- in physical and virtual mediums like the internet under the umbrella of informational privacy in this judgment.[108]

In the first case on 'revenge porn' in India, *State of West Bengal* v. *Animesh Boxi* [109] where the accused uploaded the intimate and nude photographs and videos of a girl with whom he was in relationship for a long time on the website 'pornhub', disclosing her and her father's identity when she refused his demands of sexual favours. He was charged with sexual harassment (section 354A), stalking (section 354D), voyeurism (section 354C) and criminal intimidation under sections 354(A, C, D) and 509 (outraging the modesty of a woman) of IPC and sections 66C (identity theft) 66E (violation of bodily privacy), 67, 67A (transmitting obscene and sexually explicit material online) of the IT Act. The trial court held that the prosecution sufficiently proved all the charges against the accused with the help of electronic evidence, and injury to reputation is sufficient as per section 44 in the absence of physical injury. It held that non-consensual sharing intimate images, is a 'virtual rape' leading to psychological trauma and permanent injury to the victim's reputation. The case though historic, lacks precedent value being a lower court judgment, still being cited in later judgments. The ruling is in line with countries like UK, Canada, Scotland and Israel which have legislations against revenge porn and image based sexual abuse. It highlighted the need for a victim centric approach in cases of dissemination of non-consensual intimate images similar to the cases of sexual violence and sets a case for considering victim as rape survivor for being considered for compensation.[110]

---

106 *K.S. Puttaswamy* v. *Union of India,* (2017) 10 SCC 1.

107 Deepa Kharb, "Cyber Law" 56 *Annual Survey of Indian Law* 213(2020).

108 *Id.,* para 635.

109 *Supra* note 9.

110 Arnav Mathur, "Justice in the Digital Age: Addressing Non-Consensual Dissemination of Intimate Images in India's Penal Code"*The P39 Criminal Law Blog*, NLU Delhi, May 22,2023 *available at:* https://p39ablog.com/2023/05/justice-in-the-digital-age-addressing-non-consensual-dissemination-of-intimate-images-in-indias-penal-code/ (last visited on Oct. 2, 2025).

In *Shubhranshu Rout @ Gugul* v. *State of Odisha*,[111] the accused raped his classmate and recorded the incident on his mobile phone to blackmail her and coerce her to continue a physical relationship. Later, he created a fake Facebook account in her name and posted objectionable pictures and videos of her. Though the photographs were deleted from the Facebook account after police intervention, the court observed that the information in the public domain is like toothpaste; once it is out of the tube, one can't get it back in, and once the information is in the public domain, *it will never go away*. [112] The court highlighted the absence of a legal right to be forgotten as available in Europe under the General Data Protection Regulation (GDPR). The victims under GDPR have the right to have their personal data erased without undue delay. The high court also observed that the Indian criminal justice system focuses more on sentences than on the victim's loss and suffering and violation of modesty and privacy.[113]

Recently, in *X* v. *Union of India*[114,] the High Court of Delhi addressed the issues of intermediary liability and obscenity when victim's intimate images were posted on certain pornographic websites. Though not charged under section 66E, the court ruled that non-consensual dissemination of private images is a privacy violation due to the instant and pervasive nature of the internet, covered it under section 67 even when the pictures were not sexually explicit per se. It emphasised the need for immediate remedies for the same, allowing the application of obscenity laws to mitigate the harms of non-consensual dissemination, even for non-intimate images, recognising the similar impact as that of sexually explicit content.[115]

Relying upon High Court of Delhi judgment *X* v. *Union of India,*[116] the High Court of Madras in *X* v. *Union of India*,[117] directed the respondent to take immediate measures to block/remove/issue take down orders to all the intermediaries, websites, telecommunication service providers and apps to detect, remove and block all the content containing non-consensual intimate images of the victim advocate within 48 hours in case they were uploaded/ re-uploaded, shared, transmitted or disseminated over the internet or digital platforms. The court felt that the fundamental right to privacy and right to dignity guaranteed under article 21 of the Constitution to the victim was being violated every second and the State was obligated under the Constitution to safeguard to protect the same.

Significant developments have occurred in the judicial landscape after the recognition of the new-age concept of informational privacy in *Puttaswamy*[118] judgment and right

111 *Subhranshu Rout* v. *State of Odisha*, 2020 SCC OnLine Ori 878.

112 *Id.,* para 5.

113 Deepa Kharb, *supra* note 107.

114 (2023) 3 HCC (Del) 6.

115 *Ibid.*

116 *Ibid.*

117 2025 SCC OnLine Mad 3310.

118 *Supra* note 68.

to be forgotten in *Sri Vasunathan*,[119] particularly in sensitive cases involving the modesty and reputation of individuals. Additionally, the adoption of 'auto-block measures' by the apex court in *Sabu Mathew George* case[120] and *Re Prajwala Letter*[121] (though decided in different contexts) further underscores the evolving legal landscape in protecting privacy and preventing harm from the non-consensual dissemination of intimate images. These advances align with the need to shift the focus from mere obscenity to a more comprehensive protection of individual privacy and dignity. The recent DPDP Act, 2023 mentions penalties for failing to protect an individual's data, but it does not specifically provide for the 'right to be forgotten.' The Intermediary Guidelines, 2021[122] include a process for removing personal information gathered without consent, reflecting ongoing efforts to enhance privacy protections.

The Supreme Court recently[123] overturned a decision of the High Court of Madras in *S.Harish* v. *Inspector of Police*[124] wherein the criminal proceedings under POCSO were quashed. As per the High Court of Madras, in the absence of any material to indicate any transmission or publication of pornographic content involving children, no offence could be said to have been committed under the POCSO or IT. While broadening the scope of 'possession' under section 15(1) of POCSO to include constructive or digital possession covering digital storage(downloading) and cached files even when the same is without intention to publish or circulate or use for commercial purposes. The Court also observed that the term 'child pornography' is misleading hence directed to substitute the term with 'Child Sexual Exploitative and Abuse Material (CSEAM)' to more correctly reflect the nature of the crime and the victimisation of the child. It also held that the intermediaries must exercise due diligence by promptly removing CSEAM content and 'reporting it to the appropriate authorities', as mandated under sections 19 and 20 of the POCSO Act read with Rule 11 of the POCSO Rules. Failure to comply disentitles intermediaries from immunity. *Just Rights for Children Alliance* v. *S. Harish*[125] is a landmark judgment in India's IBSA jurisprudence as it advanced India's conformity with global child protection practices, especially aligning with CRC[126] and the Optional Protocol and partially with Lanzarote[127] and substantively with Budapest Convention[128] without

119 *Sri Vasunathan* v. *The Registrar General*, 2017 SCC OnLine Kar 424 decided on Jan. 23, 2017.

120 *Sabu Mathew George* v. *Union of India*, 2016 SCC OnLine SC 681 para 6.

121 MANU/SCOR/45933/2017 date of order: Oct. 23, 2017.

122 Information Technology(Intermediary Guidelines and Digital Media Ethics Code) Rules,2021.

123 *Just Rights for Children Alliance* v. *S. Harish* (2024 INSC 716, decided on Sep. 23, 2024).

124 2024: MHC:5769 decided on 11/1/2024.

125 *Supra* note 96.

126 UN Convention on the Rights of the Child, 1989.

127 Lanzarote Convention, 2007.

128 Budapest Convention on Cyber Crimes, 2001.

formal accession. However, critical gaps still exist for adult IBSA in the absence of a dedicated law to harmonise India's legal framework with global standards.

VIII Conclusion

The comparative analysis of legal responses to IBSA across different jurisdictions affirm a gradual but inconsistent evolution of legal frameworks in response to this digital sexual violence. The earlier legal systems relied upon general provisions dealing with obscenity, defamation, invasion of privacy or harassment, the perusal of modern systems adopted in countries like Australia, South Africa, Brazil and several states of US reveal that IBSA has been recognised as a distinct form of harm which violates an individual's dignity, privacy and sexual autonomy. These countries have come up with dedicated legislations/ provisions penalising nonconsensual creation, sharing and distribution of intimate images, highlighting their acknowledgement of seriousness of such conduct and the potentiality of causing unique harm to the victim involved. The legal mechanisms also vary in different countries. Earlier civil remedies under torts law

The shift towards consent-based approach in legal systems where absence of consent forms the basis of prosecution. This approach is beneficial to the victim in two ways- recognising victim's sexual agency and avoiding placing heavy burden to prove malicious intention. Though in United Kingdom and California State, law requires the proof of intention to cause distress complicate and hamper the prosecution.

Availability of civil remedies, platform accountability and content removal and erasure mechanism across countries in addition to criminal remedies, provide a multifaceted response that delivers punishment as well as harm mitigation. However, despite these developments and movement towards harmonised modern global approach, significant gaps persist. Russia and China lack dedicated provisions and still depend on fragmented legal mechanisms to cope with IBSA.

India partly aligns with the global trends, particularly in recognising IBSA as violation of privacy, dignity and sexual autonomy, as well as in imposing obligations on internet intermediaries. The statutory provisions like section 66E of IT Act, section 354C IPC/ BNS demonstrate recognition of non-consensual capture and circulation of IBSA as a form of sexual harm as highlighted through the judicial interpretation in *Animesh Boxi*. India also conforms to global standards and aligns with international norms under Budapest Convention on Cybercrime in relation to child protection against online sexual exploitation through POCSO, 2012 which was recently amended to incorporate a broad definition of child pornography, explicitly covering computer generated and manipulated images.

Even though the judiciary has played an instrumental role in expanding the legal framework to curb IBSA, moving beyond a narrow focus on obscenity to embrace

broader protection of individual privacy and dignity, there is more to be done on the legislative front. The absence of a dedicated statute means victims must rely on a patchwork of criminal, information technology, and data protection laws, each addressing different facets of IBSA. Recognising informational privacy and the right to be forgotten by the Indian judiciary marks a significant step needed in safeguarding victim's rights in the digital age. Making the laws gender-neutral, and to include morphed images as well under Section 354 IPC, is also worthy of attention. Additionally, continued legislative and judicial efforts are necessary to fully address the complexities of IBSA and ensure comprehensive privacy protections.

While the judiciary has played an important role in the interpretation of existing laws and recognising the constitutional dimensions of privacy, dignity and informational autonomy, the current framework still remains fragmented. Victims of IBSA have to rely on multiple legislations and statutory provisions which were not originally perceived to address the harms peculiar to non consensual dissemination of intimate images. Comparative experiences from countries like Australia, South Africa, Brazil and several states of US highlight the requirement of a coherent and victim centric approach recognising IBSA as a separate offence, focusing on consent rather than proof of malicious intent, and provide effective and expedited removal mechanism for such content. A dedicated statutory framework integrating criminal liability with civil remedies is what India would benefit from. The jurisprudence evolved around section 79 of the IT Act in *Avneesh Bajaj, Shreya Singhal and Prajwala* reflect global shift towards focus on regulation through digital platforms from older trend of chasing individual perpetrator, an approach harmonious with Australia,China,South Africa. To ensure speedy and effective removal of IBSA content, intermediary guidelines must be strengthened so that victims can obtain relief without court's intervention. Finally, victim support mechanisms coupled with awareness campaigns to educate the public about IBSA, consent, and available legal remedies will add significant value to India's evolving digital rights framework.