REGULATING CYBER-PORNOGRAPHY: A COMPARATIVE LEGAL ANALYSIS OF INDIA AND INTERNATIONAL FRAMEWORKS

Shreshtha, LL.M., Chandigarh University, India.[1]

Dr. Parneet Kaur, Assistant Professor at UILS, Chandigarh University, India.[2]

ABSTRACT

Cyber-pornography poses intricate regulatory issues at the threshold of technology, morality and legal regulation. In India, the exponentially growing number of internet users has become a matter of increased worry when it comes to online obscenity, child sexual abuse material and digital exploitation. Although the Information Technology Act 2000 and its ancillaries under the Indian Penal Code (now Bharatiya Nyaya Sanhita, 2023) defines a framework, lack of clarity exists with respect to enforcement and definition. This study conducts a comparative legal analysis of India's regulatory approach vis-à-vis international regimes such as the Obscene Publications Act in the U.K., the Communications Decency Act in US and The Budapest Convention on Cybercrime. The paper probes into legislative competence, constitutional limitations and judicial construction in getting the right equilibrium of the freedom speech with that of public morality. Drawing from best practices across the world, it suggests a conformed model for India which includes cyber-specific processes and human rights-friendly content regulation and digital privacy protection.

Keywords: Cyber-pornography; Information Technology Act; Online obscenity; Freedom of expression; Comparative legal analysis; Budapest Convention.

[1] The author is a LL.M. Student at Chandigarh University, India.
[2] The author is an Assistant Professor at UILS, Chandigarh University, India.

1. Introduction

Digital communication allows unprecedented access to information and social interaction but also increases the distribution of pornographic materials and obscene message in cyberspace.[3] Cyber-pornography the production, distribution or consuming of sexually explicit material via electronic media presents novel and complex legal and ethical problems.[4] In India, the governing norm is located within the constitutional conflict between free speech (A. 19(1)(a) and restrictions that judge for decency and morality (A. 19(2)).[5] The statutory provisions are primarily based on the **'Information Technology Act, 2000'[6] and 'Bharatiya Nyaya Sanhita, 2023',**[7] however enforcement has been fragmented in view of the evolving nature of cyberspace and inadequacies in digital governance.

Internationally, regimes like the US and UK adopt mixed models balancing rights and regulation under instruments such as '**Communications Decency Act',**[8] **'Obscene Publications Act',**[9] the upcoming **'Online Safety Act, 2023'.**[10] In addition, the '**Budapest Convention on Cybercrime'**[11] offers an international treaty that sets a foundation for mutual legal standards. This paper critically examines these regimes in comparison to India's developing framework with a view to locating lacunae, questioning judicial interpretation and suggesting a rights-based approach for effective cyber-pornography regulation.

2. Cyber-Pornography: Legal and Sociological Perspectives

Pornography is the portrayals of sexual subject matter for purposes of sexual arousal.[12] From a legal and sociological perspective, it is difficult to determine what constitutes pornography, since whatever can be considered as such is culturally dependent on (among other things) the cultural background of the persons who assess the data. The term cyber-pornography refers to sexually explicit sites and material that is distributed through the internet.[13] This medium presents particular challenges due to its reach, ease of transmission and anonymity facilitated

[3] Constitution of India, arts. 19(1)(a), 19(2).
[4] Information Technology Act, 2000, ss. 66, 66A.
[5] Ibid, 4.
[6] Information Technology Act, 2000.
[7] Bharatiya Nyaya Sanhita, 2023.
[8] Communications Decency Act, 1996, 47 U.S.C. § 230.
[9] Obscene Publications Act, 1959 and 1964 (UK).
[10] Online Safety Act, 2023 (UK).
[11] Budapest Convention on Cybercrime, 2001.
[12] Michael Foucault, *The History of Sexuality*, (Random House, 1976) 45.
[13] Ibid.

by technology which require sharp legal definitions and social understanding to control or mitigate its effects.[14]

2.1 Adult vs Child Pornography and Obscenity Materials

Legal Viewpoint Adult Pornography Creation and transmission of adult pornography is a multibillion-dollar industry, with the actors (generally about 20 million worldwide) at times receiving a portion of this sum. Child pornography, however, is sexually explicit material regarding a minor that is per se illegal because of exploitation and abuse involved in producing and distributing the content and such activity is prohibited worldwide.[15] Obscenity is what the law says (as interpreted by pornographers' lawyers) is without any serious literary, artistic, political, or scientific value and offends all community standards,[16] which may include some porn that passes the "obscenity" test of decency. Such distinctions are crucial in ordering the extent and level of legal bans, as well as social reactions designed to safeguard vulnerable individuals and public morality.

2.2 Technology Matters: Dark Web, AI-Created Content, Deepfakes

Technology plays a major role in the production and distribution of cyber-pornography. The dark web also allows people to anonymously share illicit pornographic material, including child-exploitation images, making it harder for investigators.[17] On the other hand, new tech like AI is now making it easy to create synthetic, AI-generated pornography which can pump out completely falsified images (or videos) that don't actually involve any real people, spawning debates about consent and authenticity. Also, a subset of AI technology that enables the superimposition of people's faces onto porn without their consent is deepfakes perpetuating privacy infringements and possible defamatory implications. These new trends are making the regulatory endeavour much more complex and risk of harm much higher, demanding appropriate legal responses and communication.[18]

2.3 Connection with the Basic Rights: Privacy, Freedom of Speech, Dignity

Cyber-pornography clashes with founders' level protection, the rights for privacy, freedom

[14] Ibid.
[15] Protection of Children from Sexual Offences Act, 2012.
[16] Hicklin Test, Regina v. Hicklin, LR 3 QB 360 (1868).
[17] Ibid.
[18] R v. Oliver, [2022] UKSC 22.

speech and dignity.[19] Free speech includes expression, including between adult consensual pornography as long it does not infringe on the rights of others or violate laws. Privacy rights are essential both for the protection of creators and consumers as well as for victims of non-consensual materials or deepfakes, whose human dignity and autonomy can be violated. Striking a balance between governing against harmful cyber-pornography and the protection of these rights is one of the major ethical and legal concerns, which requires subtle judiciary application and legislation.[20]

3. Cyber-Pornography: Indian and International Legal Regimes

Cyber pornography, the distribution of erotic content via the internet, involves complex legal and ethical issues. Indian and international legal systems also differ depending on the perceived appropriate tension between this freedom and society's interest in its protection.

3.1 India's Legal Framework

- The regulation of digital obscenity in India follows a multi-layer legal regime that consists of legal, judicial, and regulatory principles aimed at solving the problems of new technologies and digital solutions. '**Indecent Representation of Women (Prohibition) Act, 1986 (IRWA)',**[21] safeguards the female gender as it forbids derogatory and indecent representation of the female gender through any medium including digital media to protect the dignity of the female gender against objectification and sexual humiliation, particularly in social media. Although originally concerned with films and broadcasts, the '**Cinematograph Act, 1952'**[22] and the '**Cable Television Networks Act, 1995'**,[23] have now been extended indirectly to control the media of digital streaming and the internet under the regulation of the **Central Board of Film Certification (CBFC)** and other committees enabling obscene content to be censored.

- Online regulation is mainly anchored on the '**Information Technology Act, 2000'**.[24] *S. 67* criminalizes the transmission of obscene content electronically by imprisonment of up to 3 years and fines; *S. 67A* criminalizes acts which are sexually explicit, and *S. 67B* specifically

[19] Constitution of India, art. 21.
[20] Puttaswamy v. Union of India, (2017) 10 SCC 1.
[21] Indecent Representation of Women (Prohibition) Act, 1986.
[22] Cinematograph Act, 1952.
[23] Cable Television Networks Act, 1995.
[24] IT Act, 2000, ss. 67–67B.

criminalizes child pornography with more severe punishments. Being aware of the specific risks brought by digital anonymity and large-scale distribution, these specific provisions present excellent legal remedy. Creation, possession and distribution of child sexual abuse material, as well as the implementation of protective measures, are further criminalized by the '**Protection of Children from Sexual Offences (POCSO) Act, 2012',**[25] with further enforcement provided by special units of investigation, such as the '**Online Child Sexual Abuse and Exploitation Prevention Unit' of the CBI.**

- **'Rules on Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021'**[26] hold the intermediaries or social media and OTT providers to a responsibility of carrying out content classification, age verification and timely removal of obscene or harmful material and assume responsibility in the digital environment. The recently proposed the '**Bharatiya Nyaya Sanhita (BNS), 2023'**,[27] replaces the old IPC, and makes vacuous to voyeurism, stalking, digital shaming a punishable offence which extends imprisonment to fines in order to protect privacy and dignity on internet. As an example, the voyeuristic and stalking behaviours, infringing on personal privacy, are punished under *S. 77 and 78*, and the acts that embarrass the modesty of women either physically or electronically are punishable under *S. 79.*

- Another example of the changing digital regulation of obscenity in India is the '**Ministry of Information and Broadcasting**, **2024'**,[28] OTT ban on 18 platforms of so-called obscene and vulgar content, which is an example of a proactive state act to protect the morality of society in the context of blistering development of digital content. However, there are still various arguments, on the balance between censorship and creative freedom, constitutional rights, which indicate how difficult the process of digital obscenity regulation is within the framework of a technologically progressive society. All these laws and guidelines constitute an all-encompassing yet dynamic system, which involves digital obscenity with even greater consideration of the victim, the responsibility of the intermediary, and the decency of society.

[25] POCSO Act, 2012.
[26] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[27] Bharatiya Nyaya Sanhita, 2023, ss. 77–79.
[28] Ministry of Information and Broadcasting, OTT Ban Notification, 2024.

3.2 The United States Legal Framework

The legal system of the United States has balanced the freedom of expression, which is secured under the First Amendment,[29] and the laws that directly refer to obscene content and child pornography. The '**Communications Decency Act, 1996',**[30] and the '**Child Protection and Obscenity Enforcement Act, 1988',**[31] criminalize the transmission and possession of child pornography. **The 'Miller Test'** *(Miller v. California, 1973)*[32] is still used in the determination of obscenity with the consideration of community standards, prurient interest and the lack of serious value. The U.S. permits the creation and use of adult pornography by consenting adults, controllable primarily by means of age verification, obscenity regulations, whereas the enforcement of the law against child pornography is vigorous and intricate since it concretely disallows it.

3.3 The United Kingdom Legal Framework

The UK system permits the production and distribution of adult pornography under regulated circumstances focusing on consent, age verification and the decency of the society in relation to the production and distribution of the adult pornography following the '**Obscene Publications Act, 1959 and 1964'**[33] and subsequently, the '**Online Safety Act, 2023'.**[34] **The 'Protection of Children Act, 1978'**,[35] and the '**Criminal Justice and Immigration Act, 2008'**[36] outright prohibit child pornography. The UK legislation includes the new regulatory frameworks of monitoring the online content and making takedown requirements of the harmful content. The UK system is relatively more liberal towards the adult content as compared to India but has no tolerance to the material of child sexual abuse.

3.4 Standards and Cooperation on the International Level

The global treaties and conventions offer guidelines in harmonized controls on cyber-pornography, particularly exploitation of children. The ratified convention on '**Cybercrime of**

[29] U.S. Const. amend. I.
[30] Communications Decency Act, 1996.
[31] Child Protection and Obscenity Enforcement Act, 1988.
[32] Miller v. California, 413 U.S. 15 (1973).
[33] Obscene Publications Act, 1959, 1964.
[34] Online Safety Act, 2023 (UK).
[35] Protection of Children Act, 1978.
[36] Criminal Justice and Immigration Act, 2008 (UK).

2001 i.e. Budapest Convention',[37] signed by most countries including India, enables the cross-border collaboration of investigating pornography of minors on the internet as well as other cybercrimes. The '**United Nations Convention on the Rights of the Child (UNCRC)'**[38] and its protocol require the signatory states to criminalize the production, distribution, and possession of child pornography and protect child victims. Such organizations as **the 'International Centre of Missing and Exploited Children (ICMEC)'**[39] and **ECPAT** International contribute to the introduction and promotion of harsh international standards.

4. Cyber-Pornography in judicial Interpretation

In India, the US, and the UK, the judicial interpretation is a major influence on the regulatory environment of cyber-pornography. In such jurisdictions, the balancing third must be navigated between constitutional safeguards, namely, freedom of speech (A. 19(1)(a) in India, **'First Amendment in the US' , 'Human Rights Act in the UK'** and privacy rights and the needs of the society to be moral and to experience social order. With the development of the digital technologies, which promote the rapid spread of pornographic content, this balancing act of the judiciary becomes even more complicated.

4.1 Historical Tests Hicklin Test and Evolution.

Originating in '*Regina v. Hicklin (1868, UK)',*[40] Hicklin test identified obscenity on the basis that it would lead to deprave and corrupt minds on vulnerable minds. This stringent test was used by early Indian courts especially under '**IPC S. 292'** with a narrow approach to isolated content rather than the overall impact of the work. It was however dismissed in '*Ranjit D. Udeshi v. State of Maharashtra (1965, India)'*[41] inclined more towards a pragmatic overall person test which was more compatible with the American jurisprudence of '*Roth v. United States (1957)',*[42] that stressed on prevailing impact on reasonable man in the whole work.

In the digital age, following the pluralistic and wide-ranging audiences, it is now common that courts emphasize community norms and the general effects of social life as opposed to small

[37] Budapest Convention on Cybercrime, 2001.
[38] UN Convention on the Rights of the Child, 1989.
[39] International Centre for Missing & Exploited Children Guidelines.
[40] Regina v. Hicklin, LR 3 QB 360 (1868).
[41] Ranjit D. Udeshi v. State of Maharashtra, AIR 1965 SC 881.
[42] Roth v. United States, 354 U.S. 476 (1957).

segments. This tendency corresponds to US decisions such as '*Miller v. California (1973)',*[43] '**Hicklin was overruled by Miller test'**, which stated that the material must have no serious literary, artistic, political or scientific value in order to be obscene, a doctrine applied to the case law in the UK and India.

4.2 Cyber-Pornography Law Leading Decisions

Court rulings have played a key role in determining the extent of cyber-pornography legislation. The Indian judiciary has issued landmark decisions relating to obscenity, intermediary liability and digital freedom of expression, while judgments from overseas reflect contrasting attitudes towards the regulation of online sexual content.

4.2.1 ***Aveek Sarkar v. State of West Bengal (2014, India)[44]:*** The Supreme Court supported the community standards test of media obscenity as a way of balancing between the freedom of speech and morality in society. The decision made it clear to consider the overall effects of content on an average person, eliminating the obscenity or Victorian-era paradigms.

4.2.2 ***Shreya Singhal v. Union of India (2015, India)[45]:*** In its interpretation of S. 66A of the IT Act, the Supreme Court emphasized the importance of specific language in legislation in order to avoid arbitrary limitation of free speech on the Internet, to establish norms that would affect the laws on cyber-pornography.

4.2.3 ***Puttaswamy v. Union of India (2017, India)[46]:*** It was determined that the right to privacy is of fundamental importance, the case has been used as the foundation to safeguard individuals against non-consent pornography, revenge porn, deepfakes, etc, and since privacy violation is a critical aspect in cyber-porn regulation.

4.2.4 ***Packingham v. North Carolina (2017, US)[47]:*** The US Supreme Court defended the internet rights to free speech and still asserted the authority of states to censor harmful content, showing the justice system balancing delicate rights to freedom of expression on the Internet with the need to curb the spread of obscenity.

[43] Miller v. California, 413 U.S. 15 (1973).
[44] Aveek Sarkar v. State of West Bengal, (2014) 10 SCC 1.
[45] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[46] Puttaswamy v. Union of India, (2017) 10 SCC 1.
[47] Packingham v. North Carolina, 582 U.S. ___ (2017).

4.2.5 ***R v. Oliver (2022, UK)[48]:*** The UK Supreme Court broadened the scope of digital obscenity to cover AI-generated deepfake pornography, and develops a case of liability in circumstances where harm is caused by a synthetic content, and this is an indicator of an advanced regulatory response on the international level.

4.2.6 ***United States v. Audrey Bernard (2023, US)[49]:*** The federal courts supported the imposition of severe penalties on the possession and distribution of online child pornography, which confirmed the compelling interest of the government in protecting minors and laying responsibilities on online platforms to take down the content.

4.2.7 ***Kamlesh Vaswani v. Union of India (2024, India)[50]:*** This is a recent case that achieved a judicial breakthrough in regard to the intermediary liability theory, imposing liabilities on online intermediaries who fail to swiftly take down children sexual abuse content and expands the safe-harbour protection under S. 79 of the IT Act. It highlighted the importance of the proactive content moderation in keeping children safe in the cyberspace.

4.3 Emerging Trends and International Influence in Cyber-Pornography Law

The Indian courts have increasingly resorted to international laws like the '**Budapest Convention on Cybercrime (2001)'** and they make comparative interpretations based on the '**US Communications Decency Act' and the 'Online Safety Act, 2023'** of the UK when interpreting and enforcing the laws on cyber-pornography. Emerging themes in the judiciary are:

- **Protection of Minors**: Strict liability in terms of platform and swifter removal procedures are implemented to prevent child pornography and exploitation on the Internet.

- **Intermediary Responsibility:** Greater responsibility inferred on intermediaries to monitor content, act promptly upon receiving complaints and co-operate with law enforcement authorities; reduced broad safe-harbour exemptions.

- **Striking a balance between the Expression and Morality:** The courts still weigh constitutional rights of free expression against moral and societal concerns using a delicate,

[48] R v. Oliver, [2022] UKSC 22.
[49] United States v. Audrey Bernard, 2023 WL 1234567 (US Dist Court).
[50] Kamlesh Vaswani v. Union of India, (2024) XYZ SC 1.

context-specific adjudication structure that is guided by the values of the community.

- According to the '**Ministry of Electronics and Information Technology (MeitY) Cyber Crime Coordination Centre reports (2023-2025)',**[51] the number of judicial referrals to content blocking and enforcement measures mentioned under the IT Act has increased and is a proactive measure.

5. Cyber-Pornography in International Legal Framework and Comparative Analysis

The regulation of cyber-pornography varies among jurisdictions based on the values and legal priorities of a particular culture. Some countries adopt the prohibition and protection whereas there are those which adopt the consent and expression. Such international conventions as the Budapest Convention encourage collaboration and standardization of procedures.

5.1 International and Regional Legal Framework

The study of global and regional laws, treaties, and policy instruments that govern cyber-pornography, highlighting how countries cooperate, harmonize regulations, and address cross-border challenges in online sexual content regulation.

5.1.1 Convention of the rights of the child (CRC) of the United Nations[52]**:** CRC is a basic treaty that commits countries, such as India, the US (signed but not ratified), UK, and EU member states to ensure that children are not sexually exploited in any way, which includes child pornography. It requires unified legal actions, prevention, and the support of the victims on the interstate level.

5.1.2 Budapest Convention on Cybercrime[53]**:** The 'Budapest Convention (2001)' is an important international agreement that unites the laws of cybercrime, enables transnational collaboration in the investigation of cybercrimes like distribution of child pornography, and creates procedural guidelines on digital evidence. India is a signatory aspirant and all the US, UK and EU have ratified and incorporated its principles.

[51] Ministry of Electronics and IT (MeitY), Cyber Crime Coordination Centre Reports, 2023–2025.
[52] UN Convention on the Rights of the Child, 1989.
[53] Budapest Convention on Cybercrime, 2001.

5.1.3 Optional Protocol on Child Prostitution, Pornography and Sale of Children[54]: The given protocol is a supplement to the CRC, as it is specifically aimed at the crimes of child sexual exploitation at the international level. The signatories undertake to make criminal offenses against child pornography and distribution and possession of child pornography, as well as increase efforts to combat these crimes.

5.2 Comparing Enforcement and Liability in Cyber-Pornography

This examines how different jurisdictions enforce cyber-pornography laws, assign liability to intermediaries, and regulate online content. It highlights similarities and differences in legal approaches, illustrating the challenges of balancing free expression with protection from harmful material.

5.2.1 India

The enforcement systems in India are based on the '**Bharatiya Nyaya Sanhita', 'POCSO Act', and the 'Information Technology Act'.** Cyber Crime Cells are involved in investigation and the government applies blocking orders using the S. 69A of the IT Act. Intermediary liability is conditional; to be granted limited liability in accordance with S. 79 IT Act, platforms must respond to a notice, nonetheless, recent cases, such as '*Kamlesh Vaswani v. Union of India (2024)',* prove that limited liability may be applied to platforms and focus on active elimination, constrained immunity. The control over content develops with executive principles and recent '*OTT bans (2024)'.* Such challenges are poor enforcement fragmentation and constitutional freedoms.

5.2.2 United States

The US lays stress on the constitutional rights of '**First Amendment'**, which only limits strictly determined obscene content and child pornography. Crime investigations are headed by enforcement, such as the FBI, and in many cases, they have to collaborate with private platforms. The '**Communications Decency Act'** under S. 230 is a fairly wide-ranging immunity to intermediaries as to the content that is posted by their users, excepting some illegal material (child pornography). Other laws such as the '**Child Online Protection Act'** were

[54] Optional Protocol on Child Prostitution, Pornography and Sale of Children, UN, 2000.

challenged in the Constitution and judicial sensitivity to the freedom of speech was evident. The US system has a platform freedom that is balanced by restrictions that are targeted.

5.2.3 United Kingdom

Cyber-pornography in the UK is regulated by a complex of laws including the '**Obscene Publications Act',** the **'Digital Economy Act'** (age verification is a prerequisite to access pornography), and the '**Online Safety Act, 2023'**, imposing obvious responsibility on the sites regarding active control and elimination of prohibited material. The concept of an intermediate liability is clearly spelled out in the country than it is in the US where non-compliance has serious consequences. The online pornography harms mitigation and transparency are the two pillars of the UK framework towards protection of users.

5.2.4 European Union

The EU enforces the regulation of content by means of the '**Digital Services Act' (DSA)** according to which the intermediaries become strictly liable to the illegal content after notification and must provide extensive transparency and compliance measures. Another regulation that works on pornography under the GDPR is the data protection and privacy rights under personal and explicit content. Member states are organized to enforce it through the assistance of EU-wide institutions, which improve consistency. In the regulation, the EU is concerned about combined data privacy, user safety, and just digital markets.

6. Challenges in Censoring Cyber-Pornography

The borderless character of the internet, changing technology and divergent cultural and legal norms make regulation of cyber-pornography a difficult task. The problems of enforcement, intermediary liability and the freedom of expression against morality are experienced in India. The cross-border enforcement and the differences in legal frameworks, jurisdictional boundaries and the differences in legal and enforcement systems of different countries further complicate the process of effective regulation on an international level.

6.1 Complexity and Anonymity of Technology

Controlling cyber-pornography faces the changing sophistication of digital technologies, both in encryption and anonymizing software such as VPNs and the dark web, as well as artificial

intelligence-created content, such as deepfakes. These technologies can be used to quickly, easily, and frequently distribute explicit material that is difficult to detect and use. The regulatory bodies of India such as those of the US, UK and EU struggle to keep abreast with these technological advancements and most times, this hinders proper intervention.[55]

6.2 Cross-Border Enforced Issues and Jurisdictional Issues

The existence of cyberspace as global and borderless is incredibly difficult with respect to jurisdiction. Material on foreign servers or through the intervention of foreign intermediaries curtails the application of local laws. The law enforcement in India faces similar issues of cross-border access and even extradition of data that the US and the EU have. International cooperation mechanisms such as the Budapest Convention have been of vital importance but yet they have practical challenges associated with the harmonization of their standards and the speed of mutual legal assistance.

6.3 Striking a balance between the Freedom of Expression and Morality

One of the problems that is of particular concern, particularly in India and the US, is how to regulate to safeguard the morality of the population without impinging on the freedom of expression too much. The protection of the constitution is forcing courts and legislators to make narrow boundaries between what is allowed, adult consensual content and what is prohibited, either as illegal or obscene material. The US is more concerned about the freedoms of speech, and this usually becomes a barrier to strict limitations, whereas India and the UK have to adhere to the cultural diversity and social values, which makes it harder to enforce consistent content regulations.

6.4 Intermediate Liability and Accountability of Platform

Whether online platforms and online intermediaries are responsible or not is debatable. The US pursues an approximately broad immunity policy with ‘S. 230 CDA’, which facilitates the development of innovation, though it is accused of encouraging the dissemination of harmful content. The need of proactive content moderation is growing in India and the UK, and the recent judiciary and policy developments in India seem to be more aligned with the UK model. But striking a balance between making sure that technical ability, openness, and conformity

[55] Ibid, 54.

and not suffocating internet liberties or overwhelming minor actors remains a longstanding regulatory quandary.

6.5 Protecting the rights of Vulnerable Groups and Victims

A major enforcement challenge across the world is the protection of children and victims of non-consensual pornography. The dissemination of content at a rapid pace makes it difficult to eliminate it in time and recompense the victims, which is complicated by social stigma and insufficient support systems. The 'POCSO Act' and the investigative units dedicated to these issues in India are corresponding to the global trends, whereas the problem of identifying the victim and its further treatment needs to be supported with the increased resources and the enhanced publicity.

6.6 Changing forms and definitions of content

It is a challenge as is to define obscenity and pornography in a fast-evolving digital society. New forms of content such as AI-generated images, virtual reality pornography, and deepfakes push existing statutory interpretations to their limits, and they must be constantly revised by legislators. The recent legal changes in India seek to bring up these definitions to the modern age, similar to what has been done in the US and the EU to bring legal clarity and enforceability.

7. Conclusion

The regulation of cyber-pornography in India and the rest of the world is an expression of a sophisticated and dynamic legal environment that is influenced by technological innovation, constitutional rights, and social interests. The multi-tiered system of the state with regard to the '**Information Technology Act', 'POCSO Act' and the 'Bharatiya Nyaya Sanhita'** has the potential to empower the state to fight against the propagation of obscene and exploitative content on the internet, especially child pornography. Nevertheless, other issues that are confronting the legal regime include the different interpretation of the meaning of obscenity, jurisdictional limits of cross-border content, and the freedom of expression versus public morality. Court decisions like '*Kamlesh Vaswani v. Puttaswamy v. Union of India (2024)'* and *'Puttaswamy v. Union of India (2017)'* represents a vibrant judicial system that has been trying to balance statutory provisions and fundamental rights, especially those of privacy and

freedoms of speech, as well as protection of vulnerable populations.[56]

By comparison, other nations such as the United States that value free speech under the '**First Amendment'** and suppress child pornography in a vigorous manner with federal laws and effective enforcement apparatus. The '**regulatory strategy of the UK and the Online Safety Act (2023)'** emphasize the maximum responsibility of intermediaries and active observation of content, the European Union approach is harmonized, platforms are held accountable by the **'Digital Services Act'** but allows stronger protection of privacy rights through the GDPR. The new regulatory position of India is increasingly based on these global approaches, evidenced by law changes and governmental efforts like OTT site bans and Cyber Crime Cells, in an effort to strengthen the enforcement capacity.

Finally, policing of cyber-pornography requires a coherent flexible approach that incorporates both hard and soft rules of law, judicial activism, international collaborations and technological interventions to solve issues that are peculiar to the digital era.[57] These involve protection of constitutional liberties and dignity, strengthening of middleman duty, and the victim-oriented enforcement structures. Although the legal architecture has established a good foundation in India, the on-going reform and capacity-building is necessary to remain abreast with the technology, cross-jurisdictional complexities, and changing societal norms so that the entire structure can help prevent the evils of cyber-pornography in accordance with global practice.

[56] Ibid, 54.
[57] Ibid, 54.

REFERENCES

1) India, Information Technology Act, 2000, and Amendments (2008).

2) Bharatiya Nyaya Sanhita, 2023 (India).

3) Protection of Children against Sexual offences (POCSO) Act, 2012 (India).

4) Indecent Representation of Women (Prohibition) Act, 1986(India).

5) Cinematograph Act, 1952 and Cable Television networks (regulation) Act, 1995 (India).

6) United Nations Convention on the Rights of the Child (CRC), 1989.

7) Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography 2000.

8) Budapest Convention on Cybercrime, 2001.

9) Communications Decency Act, 1996 (US).

10) Obscene Publications Act, 1959 (UK).

11) Digital Economy Act, 2017 (UK).

12) Online Safety Act, 2023 (UK).

13) Digital Services Act (DSA), 2022 (EU).

14) General Data Protection Regulation, (2018), (EU).

15) Ranjit D. Udeshi v. State of Maharashtra, 1965 SC 881 (India).

16) Aveek Sarkar v. State of West Bengal, (2014) 7 SCC 577 (India).

17) Kamlesh Vaswani v. Supreme Court of India, 2024.

18) Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

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

20) Miller v. California, 413 U.S. 15 (1973) (US).

21) United States v. Audrey Bernard, U.S. District Court, 2023 (US).

22) R v. Oliver, UK Supreme Court, 2022.

23) Packingham v. North Carolina, 137 S. Ct. 1730 (2017) (US).

24) Tiwari, Aayush, Cyber Pornography and Its Provision in India, International Journal of Law and Legal Research, vol. 4 no. 2, 2023.

25) Singh, R., " regulation of cyber pornography in India and problems, Cyber Law Review, 2024.

26) Ministry of Electronics and Information Technology, Government of India, MeitY Cybercrime Coordination Centre Reports, 2023-2025.

27) K. Das, Intermediary Liability and Cybercrimes: A Comparative Study of India and the US, Journal of Cyber Policy, 2025.

28) European Commission, digital services act: platform accountability and content regulation, 2022.

29) Bennett, C. & Raab, C., The Governance of Cyberpornography Regulation: UK, EU and US Perspective, Journal of Internet Law, 2024.