

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi-Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

LEGAL REASSESSMENT OF SAFE HARBOUR AND GENDER NEUTRAL LAWS THROUGH THE LENS OF ONLINE SAFETY IN INDIA

AUTHORED BY - AAYANSH THAKUR
Symbiosis Law School, Nagpur

ABSTRACT

India has been expanding its digital ecosystem but there have been several issues in relation to online safety also raising questions on the accountability of intermediaries and the amount of cyber crimes it inflicts. The outline of safe harbour mentioned as per Section 79 of the Information Technology Act, 2000 which provides intermediaries with conditional immunity. However, various digital crimes ranging from AI-generated deepfakes as well as morphing of non-consensual pornography along with gender neutral abusive speech have revealed its shortcomings in relation to the current legal framework. The case of Shreya Singhal v/s Union of India has provided a judicial outreach so as to lessen the widespread of harmful or abusive content on digital platforms. India's legal system has been recently embracing the gender neutral approach with respect to cyber crimes whereas also acknowledging the fact that abusive content affects individuals across all gender identities. Though the legal landscape tends to remain with many conceptual ambiguousness as well as inadequate harmonious construction between gender neutral protections and along with the liabilities of intermediaries reduce the effects of an existing safeguard. Victims that face various digital sexual exploitation and technology related harassment often encounter many procedural delays and also plays as a role in the problems with evidence which are mainly due to the wide scope of safe harbour and also the limited mandatory obligations imposed by the platforms. This research is in correlation to a legal reassessment of the doctrine of safe harbour through the lens of gender neutral laws and also providing a means for online safety concerns. Using doctrinal analysis and using a comparative review of international models such as the "U.S. Section 230 and the EU Digital Services Act", this study highlights the systemic gaps in India's current legal framework that are particularly in relation to platform related design choices and also raises questions on the algorithmic of harmful content, anonymous abuse, and also to counter the absence of certain mechanisms that are required to address AI-driven harms. Overall, the findings undermine the

requirement of constructing an adaptive and gender neutral regulatory framework that is capable of ensuring online safety while also balancing it with innovation, accountability within the digital landscape.

Keywords: Safe harbour, Liability of Intermediaries, Gender Neutral Laws, Online safety, Cyber crime, Artificial Intelligence.

Introduction: -

The evolving nature of India's digital framework has increased many debates around the liabilities of intermediaries also considering the safe harbour and its scope and the dire need for gender neutral laws so as to ensure online safety. As per section 79 of the Information Technology Act, 2000 was initially designed in order to protect the intermediaries from any liability for such third-party content which has undergone significant changes after the case of *Shreya Singhal v. Union of India*¹ and in addition to the 2021 Intermediaries Guidelines and the Ethics Code of Digital Media. In current time, the landscape of such grave online harm has grown and proved to be more complex, where issues that are raised such as portrayal of intimate images without consent along with deepfakes morphing, abusive language, and harassment is also to be considered. These harms are caused across all the individuals despite different gender identities making it an important issue to reassess. There are many instances where people tend to use typing symbols in place of cuss words like (*,#,!, \$ etc) also called as grawlix. These are used so as to avoid or to bypass automatic content filters and also to protect them against community guidelines and its violation and is not detected by the application.

Though there have been many legal reforms, but these existing laws are often gender biased in nature with many provisions listed down for protecting women particularly while leaving the consideration of males, transgenders, and even non-binary victims. This kind of system creates many complications in relation to the platform level for certain safety measures, particularly in the context involving the content of sexual content, morphing by use of AI or deepfakes, and also verbal abuse. Digital platforms that have a range from social media to that of content sharing and also using the messaging services where there is a struggle with the requirements of balancing of free speech on digital platforms and infringement of user privacy.

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

This research paper re-evaluates India's safe harbour and its architecture with respect to gender neutral laws by analyzing their overlapping with online safety. It also evaluates whether the current legal system is adequate enough to address the harm caused by cyber crimes and also explores the need for any such reforms that are required in the field of technology and is within the jurisdiction of the Constitution of India.

Research Methodology:-

This research provides a reassessment of India's safe-harbour legal and digital framework and considering the cyber crimes and the related provisions which are to be addressed in relation to online safety across genders and if the principles from the EU Digital Services Act can be used for a gender neutral reform. Key questions to be discussed are:

1. How does India's statutory laws and regulatory frameworks (Section 79 IT Act, Intermediary Rules 2021) tend to operate in reality with regards to online safety and gender based harms?
2. What are the loopholes that exist in the protection of victims across all genders?
3. Which regulatory framework from the EU's Digital Services Act can be used in the Indian framework which is not violative of laws instilled by the Constitution of India?

Doctrinal Analysis:-

The first step of the research methodology requires a **doctrinal examination** of existing Indian statutes and rules that are primarily in use which involves use of "**Section 79 of the Information Technology Act, 2000**" also known as safe harbour and the use of "**The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**". It also analyzes the relevant statutory provisions, case laws, and the regulatory framework in order to gain a understanding of **how these laws function in real life**, particularly in relation to online harassment, sensual images, deepfakes and its morphism, and targeting based on gender. This research methodology also involves a comparative study which examines the fundamentals mentioned under the **EU Digital Services Act which involves a requirement of:**

- i. Due diligence and classified requirements for online platforms
- ii. Mandatory evaluation of risk analysis
- iii. Regulation of algorithm and its regular inspection
- iv. A medium of transparency for content control

This comparative analysis provides us with the requirements which may be practically and constitutionally suitable with conditions in India.

Qualitative Analysis:-

This study relies on use of **secondary data** through a qualitative content analysis for its approach by using academic articles, policy papers, blogs and expert commentary that are reviewed to understand the reality of online gender based harms. Key sources of secondary data includes:

- I. Centre for Communication Governance, *Report on Intermediary Liability in India*** (Jan. 18, 2023), CCG Blog²
- II. Chinmayi Arun, *Intermediary Liability in India*, Centre for Communication Governance (2013)**³
- III. Indranath Gupta & Lakshmi Srinivasan, *Evolving Scope of Intermediary Liability in India*, 37 *Int'l Rev. of L., Computers & Tech.* 294 (2023)**⁴

These sources helped us to identify the structural gaps in India's current legal regulatory model and also the limitations faced by all the victims across all gender identities.

Analysis of Legal Framework:-

This analysis takes a note of the understanding of the current legal framework in India which evaluates various statutory provisions and laws in correlation to the court interpretations, and platforms behaviour on basis of gender. It also tends to state the gender based harms that are caused online that are inconsistent with its application. It also has identified various structural loopholes where there have been delays in bringing down harmful content due to weak redressal and also the approach is limited on gender recognition thus causing harm to victims irrespective of their gender. It can also be considered that transparency is essential on the digital platforms, which can be used in risk analysis which are in derogation to the transparency rules where algorithm is set usually to be women centric which can be considered as a violation of Article 19 (1) (a) freedom of speech and expression and also violative of Article 14 Right to Equality and Article 15 Prohibition of discrimination on grounds of religion, race, caste, sex or place of birth.

2. <https://ccgnludelhi.wordpress.com/2023/01/18/report-on-intermediary-liability-in-india/>

3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566952

4. <https://pure.jgu.edu.in/id/eprint/5413/1/Evolving%20scope%20of%20intermediary%20liability%20in%20India.pdf>

Case based study with statutory guidelines:-

The statutory provisions involves the use of

1. Section 79 of IT Act, 2000 safe harbour clause
2. Due diligence requirements
3. The 2021 Rules' obligations: Tracking, a cool down period of 24 hours takedown for sexual or harmful content, Grievance officer mechanisms involves the appointment of a grievance officer for all digital platforms, Dynamic monitoring for gender based harms and harmful content.

Case Laws to consider:-

1. *Shreya Singhal v. Union of India* (2015):

The Court in this case held safe harbour Section 79 but with a 24 hours limited takedown to **actual knowledge via court or by government order**. In reality, these digital platforms still abide by these rules to avoid liability. Gender based harms like morphing, revenge porn are often removed only after significant delay.

2. Delhi High Court v/s *Union of India* (2021, Pornographic Content Circulation case)⁵:
This case is about a woman whose morphed sexual intimate video was circulated on meta platform of WhatsApp where the digital platform struggled a lot to remove duplicates of the content. The Court directed the term of "global takedown" which revealed various gaps where the intermediaries lacked the technical ability to remove re-posts effectively due to which the victim faced repeated harm due to inability to take quick action for taking down the content.

- *Men & Other Genders Facing Harms:- There are many instances where the Delhi High Court & Karnataka cybercrime rulings were where men faced the threat of extortion through the medium of honey trap or blackmailing by sexual means. It also addressed the issue of transgenders facing targeted deepfakes circulation. These cases highlight the loopholes in the legal framework where Indian statutes tends to recognise harm based on gender and not on the factor of gender diverse victims equally.*

5. X v. Union of India, W.P.(C) 648 of 2021 (Del. HC Jan. 29, 2021) (India)

Loopholes in Digital Platforms Protection:-

1. Absence of a gender neutral definition in context of sexual harm mentioned under IT laws.
2. There is no such mandated time bound resolution which are in exception in severe sexual content cases.
3. Weak regulation of duties of grievance officers.
4. No victim compensating mechanism provided through the liability of digital platform.
5. Re-uploads and the content being viral not being technically addressed at instance.
6. Various enforcement agencies often misinterpret the real idea of cyber laws leading to delay.
7. Lack of obligations by digital platforms required in order to preserve evidence for all victims of unbiased on basis of genders.

These cases and loopholes help us to uncover the **practical gaps or loopholes in reality, where issues** such as slow takedown processes, lack of gender based grievance procedures, and also an inconsistent application of safe harbour protections for intermediaries, and even involving cyber laws to be misinterpreted.

Review of Literature:-

This particular review is surrounded in relation to India's safe harbour provisions, liability of intermediaries, and also considering online safety which presents a crucial picture of legal evolution with challenges in its application with gaps in gender based protection. Early analysis primarily focused on Section 79 of the Information Technology Act, 2000 which introduced the concept of safe harbour legal framework in order to shield the intermediaries from liability for any such user generated content.

Chinmayi Arun⁶ provides a major insight into these doctrinal loopholes of Section 79 further highlighting that the law has been offered a broad protection to those of its intermediaries while leaving any significant discretion to courts for its interpretation with due diligence and its obligations. This also notes that those laws which are inconsistent with these judicial interpretation has led to a point of uncertainty in its enforcement, thus causing gaps in its timely protection for those victims who suffered any such online harms through any harmful content.

6. Chinmayi Arun, *Intermediary Liability in India*, Centre for Communication Governance (2013)

Gautam Bhatia⁷ has interrogated many of these constitutional dimensions in many aspects, also arguing that Indian liability laws for intermediaries particularly when they were interpreted as a need for an active monitoring it can be a part of conflict with the freedom of speech as provided as per Article 19(1)(a) of the Constitution of India. It also highlights that platforms often perform an error on the side of caution and when it comes to removal of harmful content which can also lead to impact women and all those of users of all genders whose digital expressions are suspected to be more frequently targeted and falls under the cyber crimes faced by all genders.

This literature on gender based harms reinstates this rising concern. Arvind Narrain⁸ has critically examined the Indian Penal Code's (IPC) based on factor of treatment of gender and sexual crimes that are related to it also primarily revealing that the law remains largely based on social stigma. Narrain's analysis has also indicated that these limitations are in regards to that with online contents as cyber crimes and their reporting mechanisms as well as the platform policies usually rely on based of conventional legal definitions due to which it's interpretation turns out to be faulty when it comes to all genders suffering from cyber crimes on digital platforms. For instance, leaving transgender along with non-binary victims unprotected. Though there are many new age crimes with the backing of technology posing severe threat such as non-consensual deepfakes and also use of morphing of intimate or harmful content which undermines their inefficiency with current legal frameworks so as to respond to quickly evolving new age digital harms or crimes. Scholars also noted that the reactive takedown procedures for taking down these harmful content often fails to address the speed and spread range of such content, highlighting the urge for a proactive regulatory measure so as to avoid these issues in near future.

These comparative analysis also suggests various potential pathways for any of these reforms. Research on the EU Digital Services Act further demonstrates that any such structured obligations pose the requirement of analyzing of these risk assessments along with a timely algorithmic updates based on rising crimes and their variety through a medium of transparency in reporting of these crimes and also clearly defining notice and action mechanisms which can enhance these measures in case of online safety without ignoring the constitutional rights.

7. Gautam Bhatia, *Intermediary Liability and Online Speech*, Oxford Human Rights Hub (Mar. 7, 2016)

8. Arvind Narrain, *Gender and the Indian Penal Code: A Critical Appraisal*, Alternative Law Forum (n.d.)

Gupta and Srinivasan's⁹ recent work on the study of evolving liabilities faced by intermediaries in India requires the need to adopt the EU Digital Services Act mechanisms which could strengthen India's regulatory framework and also serve as a great improvement in its current laws in India. It is also to be seen that they are adopted based on laws mentioned in the constitution of India and with that of social contexts.

These academic studies forms the basis of a comprehensive legal reassessment of India's liability in relation to that of intermediaries also highlighting the need for such reforms that are both gender neutral in nature and it also curbs down the risks raised in today's digital world.

Methods:-

This research has adopted a **qualitative and doctrinal approach in research methodology**, which is also supported by their comparative analysis in close correlation to India's socio-legal issues faced by all genders and to further re-evaluate the relationship between India's safe harbour legal framework and to that of gender neutral laws in regards to that of emerging online harms suffered by the people in its entirety.

Firstly, this research relies on the factor of a **doctrinal examination** of statutory texts including Section 79 of the Information Technology Act, 2000 which talks about the Guidelines for intermediaries and that of Ethics Code with digital media also reviewing the provisions relating to sexual content as well as all those relevant penal provisions based on privacy, voyeurism, stalking, and defamation. Significant judicial decisions such as the case of *Shreya Singhal v. Union of India* (2015), *Google v. Visakha Industries* (2020)¹⁰, and recent High Court judgments based on the circulation of pornographic or obscene content and the use of deepfakes form a crucial role in their textual analysis. These cases often help to trace the evolution of liabilities for intermediaries and the shifting concern placed on all these online platforms.

Secondly, this research employs a **comparative approach while** referencing the global regulatory digital legal frameworks such as the EU Digital Services Act. This globally jurisdictional aspect helps us to identify these regulatory mechanisms that are required to balance safe harbour law and its protections with that of their accountability, particularly in

9. Indranath Gupta & Lakshmi Srinivasan, *Evolving Scope of Intermediary Liability in India*, 37 *Int'l Rev. L., Computers & Tech.* 294 (2023)

¹⁰

areas which involves gender based harms like uploading of intimate imagery and AI generated deepfakes.

Thirdly, this study engages in a **literature based review** and **analysis** on basis of policies and academic articles and publications by Indian and international organizations such as CCG. These materials provides us with deep insights into the governance of these digital platforms. They also help us to identify the conceptual gaps between all the legal provisions to that of digital abuse in reality faced by the people.

Finally, this research instills a **socio-legal lens** to understand how gender neutral laws function within an environment where online harms disproportionately affect women and marginalized groups while the rest are not considered under this like males, transgenders and non-binary people.

Suggestions:-

A. Reforming the Safe Harbour laws on basis of harm

India should adept a harm based safe harbour model. While all the intermediaries should not lose protection for the content that they have no knowledge of being circulated on these platforms must be undertaken as a part of their duties in cases involving gender based image harms. This is inclusive of faster takedown of such content while also dedicating reporting tools for an immediate detection of unlawful content.

B. Uniform Takedown Procedures based on timeline

A standard notice period of 24 hours is to be maintained despite gender for all these online platforms to be considered as a takedown period. A user-friendly complaint dashboards is a necessity and their regular transparency reports can help to build their user trust and ensure any such future accountability.

C. Gender Neutral Laws to be implemented

Although the certain laws remain gender neutral but their enforcement must be accounted for gender based impact. This also requires a specialized training to be given to all law enforcement agencies when handling sensitive complaints, and prioritizing these harms that often target women and minors.

D. Institutional establishment for Online Safety

A special Commission for protection against digital harm could coordinate with these digital platforms and help them to address such appeals and also in conducting weekly

or monthly audits. This will certainly reduce their reliance on courts and will strengthen their systemic enforcement and it will also be of help when it comes to pendency of cases in courts.

Conclusion:-

India's safe harbour framework, designed in the early 2000s, now confronts unprecedented challenges arising from AI-generated content, intimate-image abuses, and digital gender-based violence. Simultaneously, gender-neutral statutory drafting, though theoretically egalitarian, often falls short of addressing the disproportionate vulnerabilities faced by women and marginalised users online. This research finds that strengthening accountability, standardising takedown procedures, reforming deepfake regulations, and adopting a harm-centric approach can significantly enhance online safety without undermining innovation or constitutional speech rights. A balanced recalibration—rooted in proportional platform duties and sensitive implementation—can help India shift towards a digital ecosystem that is safer, more equitable, and more responsive to evolving technological harms.

