Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Re-evaluating Safe Harbour Protections: Intermediary Liability and the Duty of Care in Regulating Cyberbullying through Comparative Analysis

Abrianna S[a] Nihanth Reddy. M[b]

[a]SASTRA deemed University, Thanjavur, India bSASTRA deemed University, Thanjavur, India

Received 07 September 2026; *Accepted* 07 October 2026; *Published* 12 October 2026

The fast growth of digital platforms has changed how people communicate, but it has also made cyberbullying easier, causing serious psychological, reputational, and social damage to those who are targeted. The safe harbour doctrine, which is part of Section 79 of the Information Technology Act, 2000 and further outlined in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, is meant to protect online platforms like Instagram and Facebook from being held legally responsible for content posted by others, as long as they follow certain due diligence rules. However, as cyberbullying becomes more common, it is important to ask whether the current laws are doing enough to protect victims or if they are giving too much protection to the platforms. This research looks into how much legal responsibility should fall on digital platforms for hosting content that involves cyberbullying under India's safe harbour laws and the duties of these platforms in dealing with such cases. Using a doctrinal research method along with a comparative legal analysis, the study reviews the legal framework, court decisions, and rules that govern what digital platforms are responsible for. It also compares India's approach with the laws of other countries, such as the European Union, the United Kingdom, South Korea, and Australia, which use different models like notice-and-takedown, actual knowledge, or conditional safe harbour. The research highlights problems in the Indian system, such as a lack of clear guidelines for dealing with cyberbullying content, inconsistent requirements for removing harmful content, and unclear rules about when a platform is considered to have knowledge or responsibility. It argues that while safe harbour is important for encouraging innovation and free speech, it should not protect platforms from being held accountable for not taking action when they know about or should know about ongoing

cyberbullying. The study aims to shape discussions about balancing the need to protect users, hold platforms responsible, and maintain free expression within India's developing digital laws.

Keywords: *harbour, protection, intermediary, cyberbullying.*

INTRODUCTION

The rapid growth in individuals' communication, access to information and engagement with the world through the internet and social media has transformed tremendously over the decades. This modern technology has both advantages and disadvantages. As a legal concern, the crimes that happen on social media and intermediary platforms include identity theft, financial fraud, cyberbullying, ransomware, malware, doxxing and harassment, etc. In the Indian regime, these crimes are being addressed through Bharatiya Nyaya Sanhita, Information Technology (IT) Act, 2000, Digital Personal Data Protection (DPDP) Act 2023. Official data from the Ministry of Home Affairs reveals that out of over 65 lakh cyber complaints submitted to the National Cyber Crime Reporting Portal (NCRP), fewer than 2 lakh advance to a formal First Information Report (FIR)[1]. Legal experts point out that a lack of technical expertise among local investigators leads to massive delays, allowing perpetrators to hide comfortably behind digital anonymity[2]. India uses the patchwork of laws where none of which truly address the core nature of cyberbullying[3].

Cyberbullying is intentional and repeated conduct carried out through digital communication tools that harasses, humiliates, threatens, or harms another person, resulting in emotional, psychological, or reputational injury. It can occur through SMS, Text, apps, online social media, forums, or gaming, where people can view, participate in, or share content[4]. The 'safe harbour' provision in section 79 of the Information Technology Act, 2000

[1] 'NATIONAL CYBER CRIME DATA' (*Press Information Bureau*, 21 July 2026) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2287039&reg=1&lang=1> accessed 16 September 2026

[2] Abhay Bora et al., 'Growing Incidence of Cybercrime in India: Causes and Remedies' (2026) 2(1) Journal of Applied Social Sciences and Humanities <https://www.researchgate.net/publication/408656165_Growing_Incidence_of_Cybercrime_in_India_Causes_and_Remedies> accessed 16 September 2026

[3] 'Cyberbullying and Legal Gaps Under Indian Law' (*Tax Guru*, 17 November 2025) <https://taxguru.in/corporate-law/cyberbullying-legal-gap-indian-law.html> accessed 16 September 2026

[4] 'What Is Cyberbullying' (*Stopbullying*) <https://www.stopbullying.gov/cyberbullying/what-is-it> accessed 16 September 2026

refers to the legal protection for the intermediaries that transmit and host third-party content online.

Under the provision, the intermediaries are not made liable for the third-party content as long as they comply with certain conditions. The conditions include transmission of content, compliance of due diligence, remove or disable access upon receiving actual knowledge through court or government order[5]. When the safe harbour provision was enacted under the Information Technology Act 2000, platforms functioned as the basic intermediaries. Over the years, it has evolved into diversifying participants like e-commerce, AI tools, etc., which makes the broader legal immunity outdated. Platform-led moderation policies would provide constitutional guarantees.

Hence, it is necessary to restrict the safe harbour provision by fine-tuning the boundary between curtailing digital disinformation and safeguarding user expression[6]. In December 2018, the Ministry of Electronics and Information Technology released the Intermediary Liability Guidelines (Amendment) Rules, which significantly alter the intermediary liability regime in India. The guidelines faced certain criticism and attention. Some of them are threats to End-to-End Encryption, Chilling Effect on Expression, Limitation of Automated AI tools, Disproportionate Financial Burdens, etc[7].

In the modern world, online platforms are the backbone of how we talk, buy things and share ideas. To shield these platforms from being blamed for what users post around the world, the 'harbour' rule was created. This paper looks at how different countries handle this. Comparing the rules, in India, the European Union, the United Kingdom, Australia and South Korea. While India's Section 79 of the IT Act and the IT Rules, 2021 impose stringent proactive compliance obligations, the EU's Digital Services Act establishes a systemic risk-management model. Concurrently, Australia prioritises administrative regulatory enforcement. By evaluating statutory provisions, judicial precedents, and regulatory updates across these jurisdictions, this paper examines how different legal systems rebalance

[5] 'What is the Safe Harbour Clause?' (*BYJU'S*) <https://byjus.com/free-ias-prep/safe-harbour-clause-in-it-law-upsc-current-affairs/> accessed 16 September 2026

[6] Aroon Deep, 'Center to reconsider 'safe harbour' clause in IT law' *The Hindu* (10 March 2023) <https://www.thehindu.com/news/national/centre-rethinking-safe-harbour-concept-in-it-act-revamp/article66599676.ece> accessed 16 September 2026

[7] Torsha Sarkar, 'Rethinking the intermediary liability regime in India' (*CyberBRICS*, 12 August 2019) <https://cyberbrics.info/rethinking-the-intermediary-liability-regime-in-india/> accessed 16 September 2026

platform accountability with user rights, offering actionable insights for reforming India's digital liability framework[8].

STATEMENT OF RESEARCH PROBLEM

India's safe harbour regime under section 79 of the IT Act, 2000, along with the IT Rules, 2021, was formulated for a relatively early era of intermediaries who operated as 'passive' entities. It has failed to keep pace with the magnitude and continuity of cyberbullying on contemporary platforms. In India's intermediary liability regime, immunity depends on intermediaries operating as 'passive' channels for information, and the regime neither incentivises proactive moderation to deal with persistent harassment, nor establishes a cyberbullying-specific due diligence standard, nor a calibrated notice-to-knowledge threshold, nor a tiered liability structure based on size or risk. This contrasts with the graduated, purpose-specific obligations in the EU's Digital Services Act, the UK's Online Safety Act, and South Korea's legislation after the tragedy of Sulli[9]. Thus, the research problem here is that India's intermediary liability regime neither incentivises responsible platform conduct nor provides victims of cyberbullying an adequate remedy.

RESEARCH OBJECTIVES

- To study the statutory and judicial parameters of intermediary liability under section 79 of the IT Act and the IT Rules, 2021, in the specific context of cyberbullying.
- Comparative evaluation of intermediary liability schemes of the European Union Digital Services Act, the United Kingdom's Online Safety Act, Ofcom's regulatory power, and South Korean network-utilisation and communications laws, highlighting features superior to India's regime.
- To determine if India's 'safe harbour' system is able to sufficiently deter the negligence of platforms, while protecting free expression and innovation.
- Proposing suggestions for a legislative framework in India, selectively borrowing features from the EU, UK, Australia and South Korean intermediary liability systems.

[8] Siddhant Samaiya, 'AN ANALYSIS OF INTERMEDIARY LIABILITY IN INDIA AND THE EUROPEAN UNION' (*Manupatra*, 02 September 2024) <https://articles.manupatra.com/article-details/an-analysis-of-intermediary-liability-in-india-and-the-european-union> accessed 16 September 2026

[9] 'After K-pop death, 'Sulli's Law' being considered to fight cyberbullying' *South China Morning Post* (29 October 2019) <https://www.scmp.com/lifestyle/entertainment/article/3035302/after-k-pop-death-sullis-law-being-considered-fight> accessed 16 September 2026

RESEARCH QUESTIONS

1. Is the 'passive intermediary' requirement of Section 79 a disincentive to proactively moderate cyberbullying content in India?

2. How do the risk management approach of the EU, the statutory duties enforced by Ofcom in the UK, and the post-tragedy reforms in South Korea solve the notice-to-knowledge gap left unresolved by Indian law?

3. How can legislation be crafted to address the issues of accountability for intermediaries, safety of victims and freedom of speech according to the constitution of the country?

LIMITATIONS OF THE STUDY

The research is based on documentary evidence and is focused on legal frameworks, subordinate laws and some judicial decisions made in India, the EU, the UK, Australia and South Korea relating to the liability of intermediaries for cyberbullying content. The limitations of the study prevent the examination of other forms of illegal content like terrorism or IP violations, unless they serve to clarify the issue of safe harbour. There are many limitations of the research like lack of access to South Korean language court, the speed of developing EU and UK laws compliant with the DSA and OSA (the issue of developing guidance from Ofcom and European Commission being still open) and the absence of any empirical or survey elements from the research.

RESEARCH METHOD

The method of this research is a doctrinal, comparative study. Primary data comes from legal texts, for instance, the IT Act 2000, IT Rules 2021, EU e-commerce directive and Digital Services Act, Australian Online Safety Amendment (Social Media Minimum Age) 2024, Australian Online Safety Amendment (Social Media Minimum Age) 2024 and UK Malicious Communications Act 1988 and Communications Act 2003, Online Safety Act 2023 and South Korean communications. Judicial decisions and regulatory guidance are considered primary data sources.

Secondary data includes academic commentaries and the results of surveys (NCRB/NCRP), governmental press releases (British White Paper on online harms). Data is analysed by

functional comparative analysis, and each jurisdiction's liability trigger, such as the distinction between active and passive liability, actual knowledge and the obligation of systemic risk and procedural security, is examined according to the firm standards of victim compensation efficiency, accountability of intermediary, and protection of freedom of speech. The matter of interpretation consists of the identification of transferable features of design in comparison with the Constitution of India and its use in case law.

LITERATURE REVIEW

Overview of Cyberbullying: Faye Mishna and others[10] in 2010 conducted a study that examined cyberbullying behaviours among school students. This research, which involved 2,186 participants, investigates how common cyberbullying is, its effects, and the different experiences people have with it. The study focuses on middle and high school students living in a major urban area. It looks at how students use technology, the types of cyberbullying they engage in, and the psychological effects of both being bullied and bullying others. Over half of the students, or 49.5%, reported experiencing online bullying, while 33.7% admitted to bullying others. Most of the bullying happened between friends, and many victims did not report the incidents. Students who were bullied often felt angry, sad or depressed. They carried those feelings with them for a long time. Those who bullied others said they did it because it made them feel powerful, funny or popular. Many of them also felt guilty or bad after doing it. That guilt didn't always stop them from doing it.

Cyberbullying affects people of all ages. It hurts children and teenagers the most. It can lead to problems like anxiety, depression and even suicide. The internet is everywhere now. Social media platforms are easy to use, and since many of them let people stay anonymous, it's easier for bullies to hide. That's why cyberbullying has become more common. People often don't understand how bad cyberbullying can be. Some don't care. Others don't know how to stop it. Authorities also don't pay attention, which makes the problem worse. Strong security measures are needed to protect identities and personal information. These can help reduce cyberbullying. Better laws and stricter penalties for those who bully online are also important.

[10] Faye Mishna et al., 'Cyber bullying behaviors among middle and high school students' (2010) 80(3) American Journal of Orthopsychiatry <https://psycnet.apa.org/doi/10.1111/j.1939-0025.2010.01040.x> accessed 16 September 2026

Reporting systems should be easier to use and more effective. Teaching people how to use the internet safely is key. Digital literacy should be part of school lessons. Governments, schools and tech companies must work together. Online safety campaigns, training programs and age-appropriate safety tools on media platforms can make a real difference. In conclusion, cyberbullying is a problem in India. It needs attention. By focusing on cybersecurity and taking steps like education, better laws and teamwork, India can build a safer digital space for everyone.

Concept of Independent Moderator: The article suggested that there should be a concept of an independent regulator, which was mentioned in the important UK white paper on harms[11], where the independent regulator would be responsible for drafting codes of conduct for online companies and responsible for their enforcement. This body is used to oversee and can be used to arbitrate disputes regarding content removal. The article also suggests that countries like the US, UK, and the EU, in Transatlantic Working Group Sessions, discussed the idea of an 'internet court' for illegal content regulation. It makes the norms of online content more transparent, which was previously done behind the closed doors of the government and tech incumbents, and employs trained professionals who dispose of the matter in an expeditious manner. India is familiar with the idea of specialised tribunals; for example, the government of India has passed the Commercial Courts Act in 2015 to deal with issues of larger value. There is no ultimate solution for the moderation of web content, but it is worth considering the compromise between complete government control and laissez-faire autonomy.

Shortcomings in Indian Law: The Indian Constitution ensures freedom of speech as outlined in Article 19(1)(a), but this right is subject to reasonable limitations. However, the nature of online speech introduces new challenges in interpreting these limits. The Information Technology Act, 2000 is the main legal instrument in this area. Initially, Section 66A was used to penalise cyberbullying, but it was struck down by the Supreme Court in the case of Shreya Singhal v Union of India (2015) due to being overly broad.

Now, the Act primarily addresses obscene content through Section 67 and sexually explicit material through Section 67A. The Information Technology (Intermediary Guidelines) Rules,

[11] *Online Harms White Paper: Full Government Response to the consultation* (UK Government 2020)

2021 impose additional responsibilities on social media platforms, such as tracing the origin of content and removing specific types of unlawful speech. However, concerns have been raised regarding excessive removals leading to censorship. The IT Act does not have rules for crimes such as cyberbullying of minors or revenge porn, so new laws are needed. The Juvenile Justice (Care and Protection of Children) Act 2015 gives protection to children who are victims of cyberbullying, including making it a crime to help cyberbullying and requiring social media companies to report child pornography. Experts say that because the rules are not followed well, the law does not work much. Both the IT Act and the Indian Penal Code address some parts of cyberbullying and hate speech, but the laws are old. Police do not get enough training about cybercrime. Many platforms avoid responsibility. The courts do not help victims heal. The legal system is patchy and only reacts when problems happen. We need police units for cybercrime and special courts everywhere with training and clear procedures.

On the side, it would help if victims could quickly get temporary orders from cyber tribunals and win damages fast, giving people easier ways to get help. Imposing liability caps by certain rules may encourage intermediaries to cooperate. Encouraging claims against perpetrators and intermediaries who fail to act on notice about unlawful speech can empower victims[12]. Inspired by the EU Digital Services Act, caps on liability can help balance the interests of different parties[13]. Proposed solutions include imposing a duty of care on intermediaries to moderate content, allowing the removal of anonymity to aid enforcement, setting up cyber courts and fast-track procedures for civil cases, and promoting mediation and restorative justice to give victims a voice.

EU Intermediary Liability: Both India and the European Union have remarkable legislation and judicial interpretations aimed at deciding the obligations and liabilities of intermediaries such as social media platforms, internet service providers and online marketplaces. The comparative analysis between India and European union gives the analysis of intermediary liability in the respective regimes. This study helps to elucidate the balance between

[12] Olivier Sylvain, 'Platform Realism, Informational Inequality, and Section 230 Reform' (2021) 131 Yale Law Journal <https://yalelawjournal.org/essay/platform-realism-informational-inequality-and-section-230-reform> accessed 16 September 2026

[13] K Prabavathy and Aswathi Sukumaran, 'An Analytical Study on the Legal Framework and Judicial Approach to the Cyberbullying' (2026) 9(2) International Journal of Law Management & Humanities <https://ijlmh.com/paper/an-analytical-study-on-the-legal-framework-and-judicial-approach-to-the-cyberbullying/?pdf=1> accessed 16 September 2026

innovation, free expression, and accountability in the online ecosystem. In the European Union, the e-Commerce Directive, enacted in 2000, governs the liability of intermediaries for third-party content. It established the minimum liability standards by introducing the safe harbour principles. Intermediaries are required to adhere to 'duty of care' and 'notice and take care' obligations to promptly remove illegal online content. It contains certain flaws like unclear scope of liability exemption and undefined concepts like passive and active roles of the intermediaries.

The European Commission later addressed these challenges in the upcoming Digital Services Act[14]. It included changes to existing provisions and introduced secondary liability for online intermediaries. The key elements of modern intermediary regulation, such as the introduction of a 'Good Samaritan' clause to encourage voluntary content moderation, new operational duties, defined platform regulator powers, and safe harbour protection for hosting, caching, and conduit providers, are areas where the EU legal framework maintains a clear advantage over India's regime.

Under Section 79 of India's IT Act and the IT Rules 2021, platforms must remain strictly passive technical intermediaries to retain immunity, and taking proactive steps to monitor or filter content risks stripping away their 'safe harbour' protection by making them 'active' actors.

In contrast, the EU's framework clearly handles this issue through its Good Samaritan provision. This allows platforms to voluntarily look for and take down content without losing their legal protection. Also, while India has one-size-fits-all rules like requiring content to be removed within 36 hours and demanding message traceability even for mid-sized services, the EU uses a more balanced and fair approach. It has a tiered system that matches the level of regulation to the size and role of the platform. It also clearly defines harbour categories for different types of intermediaries. It provides significantly greater legal certainty, user due process, and structural protection for platforms voluntarily cleaning up harmful content than India's current framework.

Australian Regulatory Framework: The authors discuss how the current regulatory framework in Australia addresses online harms by imposing responsibility on digital

[14] EU Digital Services Act 2022

platforms to police content through civil non-compliance measures rather than direct individual accountability. They argue that reliance on mechanisms such as strikes, takedowns, and bans creates a faulty framework that lacks common law due process, ignores procedural justice, and misses a critical opportunity to shape public digital citizenship through state-administered penalisation[15]. The Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024, which never passed, aimed to create penalties for any platform provider that failed to follow any misinformation code set by the Australian Communications and Media Authority. The bill in question intended to reach this goal by making platforms responsible for the quality of information they share and by requiring them to teach users, or else face consequences.

In a way, the Online Safety Amendment (Social Media Minimum Age) Act 2024, which received approval in December 2024, required platforms to stop young people in Australia who are under 16 years old from using certain platforms. This law placed penalties not on the users themselves or on parents or other people who help young people access the platforms but on the platforms that do not take 'reasonable steps to stop age-restricted users from having accounts, on the age-restricted social media platform' (63D). If it is necessary to send a removal notice to an end-user, not following this rule could result in a warning but not a penalty. The only exception given in the Act is a penalty for an end-user who fails to comply with a removal notice regarding shared intimate images[16].

UK and South Korea Approaches to Cyberbullying and Platform Responsibility: The UK has a system for dealing with cyberbullying. Under the Malicious Communications Act 1988 and the Communications Act 2003, sending messages meant to frighten, threaten or cause harm is against the law. Recently, the UK government passed the Online Safety Act 2023. This new law gives Ofcom, the communications regulator, the authority to act against platforms that allow harmful content like violence or bullying to spread online[17]. In addition to laws, the UK has set up education and support programs in schools. These are run jointly

[15] David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (Columbia Global Reports 2019)
[16] Rob Cover et al., 'Digital harms and penalties: Australian regulation, platform moderation and the figure of the perpetrator' (2025) 200(1) Media International Australia <https://doi.org/10.1177/1329878X251350727> accessed 16 September 2026
[17] Online Safety Act 2023 (UK)

by education departments, police and civil society groups. The combination of enforcement and prevention efforts makes the UK approach an example worth looking at.

Legal experts say that unlike laws, which focused only on individual offenders under Section 127 of the Communications Act 2003 or Section 1 of the Malicious Communications Act 1988, the current system now holds online platforms directly responsible by law. This means companies that connect users, like media sites, messaging apps and search engines, must take real steps to make their services safer. A big part of this change involves the Office of Communications, known as Ofcom. As a body, Ofcom can create Codes of Practice. It can also require companies to assess risks from their algorithms and follow rules to stay compliant. These can include fines of up to £18 million or 10% of a company's global yearly revenue, orders to disrupt business operations, and possible criminal charges against executives who fail to comply. Researchers agree that Ofcom's regulatory tools successfully push tech companies to implement strong notice-and-action systems, user-focused filtering options, and proactive reporting methods for issues like cyberbullying[18].

South Korea is one of the countries that has taken a very active approach to dealing with cyberbullying. After an increase in suicides among artists caused by online harassment, the country passed the Act on Promotion of Information and Communications Network Utilisation and Information Protection. This law includes rules that ban anonymous comments and allow South Korea to take a strong and active stance when it comes to fighting cyberbullying. The problem became serious after a rise in suicides among artists who were targeted by harassment. In response, the country passed the Act on Promotion of Information and Communications Network Utilisation and Information Protection. This law includes rules that ban anonymous comments and give authorities the power to quickly take down harmful content.

South Korea also created an online reporting system. It provides counselling services and an integrated online reporting system managed by government agencies. The strict enforcement and tight control over media platforms make South Korea a leading example of victim-centred regulation. Different countries handle cyberbullying in different ways. The way they

[18] Stephanie Law, 'Effective enforcement of the Online Safety Act and Digital Services Act: unpacking the compliance and enforcement regimes of the UK and EU's online safety legislation' (2024) 16(2) Journal of Media Law <https://www.tandfonline.com/doi/full/10.1080/17577632.2025.2459441#d1e775> accessed 16 September 2026

do it depends on their system, cultural values and technology policies[19]. In general, the UK and South Korea stand out with detailed legal frameworks. The UK focuses on making platforms responsible for the content they host. South Korea focuses on protecting victims.

EXISTING MEASURES FOR ADDRESSING CYBERBULLYING IN INDIA

The National Crime Prevention Council reports that the best method for preventing cyberbullying, as stated by teens, is to block the bully. Among teenagers who have experienced cyberbullying: 36 percent asked the bully to stop targeting them, 34 percent chose to block all communication with the bully, 29 percent took no action, and11 percent discussed the incidents with their parents. According to the Cyberbullying Research Centre, nearly two-thirds of tweens have attempted to assist someone who is being bullied online, and 30 percent have offered help multiple times[20].

- The Grievance Appellate Committee (GAC), established under Rule 3A of the IT Rules, 2021, is the closest functional mechanism, as it allows a user who is dissatisfied with an intermediary's Grievance Officer decision to appeal to the GAC, which operates as an online dispute-resolution mechanism and endeavours to resolve appeals within 30 days; however, it primarily functions as an appellate grievance mechanism rather than a specialised online-safety regulator[21].
- The Ministry of Electronics and Information Technology (MeitY) administers the IT Act and IT Rules and exercises broader regulatory functions over intermediaries and digital platforms, but it is a government ministry rather than an independent cyberbullying regulator[22]. The removal of the Good Samaritan Proviso under the 2025 amendment creates a regulatory challenge. Earlier, this clause protected intermediaries that voluntarily regulated content under Rule 3(1)(b). It recognised that intermediaries could manage material and keep their platforms decent on their own. Now, without the Good Samaritan Proviso, we must ask whether intermediaries

[19] 'Comparison of Intermediary Liability Safe Harbours of China, Japan, and Korea' (2020) 13(3) Journal of Northeast Asian Law <https://www.kci.go.kr/kciportal/landing/article.kci?arti_id=ART002556294> accessed 16 September 2026

[20] Justin W Patchin and Sameer Hinduja, *TWEEN CYBERBULLYING IN 2020* (Cyberbullying Research Center 2021)

[21] 'Grievance Appellate Committee' (*Grievance Appellate Committee*) <https://gac.gov.in/> accessed 16 September 2026

[22] 'About Us' (*Ministry of Electronics and Information Technology*) <https://www.meity.gov.in/ministry> accessed 16 September 2026

could be held liable under Section 79(2) when they perform moderation. The mismatch between the two frameworks causes ambiguity. This uncertainty may make intermediaries reluctant to moderate content. It is clear that MeitY must clarify its stance. Clarification will preserve platform autonomy. Help keep online content management responsible.

- The mismatch between the two frameworks causes ambiguity. This uncertainty may make intermediaries reluctant to moderate content. It is clear that MeitY must clarify its stance. Clarification will preserve platform autonomy. Help keep online content management responsible.
- CERT-In serves as India's national agency for responding to cybersecurity incidents, threats and vulnerabilities, but its primary mandate does not concern interpersonal online harassment or cyberbullying[23].
- Victims of criminal online conduct such as harassment, stalking, impersonation and threats may also use the National Cyber Crime Reporting Portal, but this is principally a criminal-law enforcement mechanism rather than a platform-regulation system. Thus, unlike Australia's eSafety Commissioner, India currently relies on multiple institutions and mechanisms rather than a single specialised authority dedicated to online safety and cyberbullying[24].

The Indian intermediary liability regime is primarily governed by Section 79 of the Information Technology Act 2000[25] and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[26]. Section 79 provides safe harbour to intermediaries for third-party information, while Rule 3 imposes due-diligence obligations. Rule 3(1)(d) requires an intermediary to remove or disable access to information upon obtaining actual knowledge through a court order or a reasoned government notification.

Various judicial decisions have laid down various measures to prevent cyberbullying. Some of them are:

[23] 'Indian Computer Emergency Response Team' (*CERT-In*) <https://www.cert-in.org.in/> accessed 16 September 2026
[24] 'Cyber Crime Related Complaint / Women & Children Related Cybercrime' (*Cyber Crime*) <https://cybercrime.gov.in/> accessed 16 September 2026
[25] Information Technology Act 2000
[26] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

In **Shreya Singhal v Union of India,** the Supreme Court has upheld Section 79 but read down Section 79(3)(b). It held that for the purposes relevant to Article 19(2), 'actual knowledge' is obtained by means of a court order or notification by the appropriate government/agency and not by every private complaint. The Court worried that asking intermediaries to judge the legality of millions of complaints themselves would impose too great a burden and might inhibit legal speech[27].

The Supreme Court of India in Google India Private Ltd v M/S. Visakha Industries, had to deal with the issue of intermediary liability for online defamatory content posted on a hosted forum. The Court noted that before the 2008 amendments to Section 79 of the Information Technology Act 2000, an intermediary could not rely on the safe-harbour provisions of the Indian Penal Code for criminal defamation unless it proved at trial that it had no knowledge of the offending material and had exercised due diligence. The Apex Court held that digital platforms cannot be passive to escape criminal liability when informed about the defamatory posts on their network. The verdict is an important precedent in the matter of platform liability in cases of cyberbullying and online defamation and makes it clear that hosting platforms have to take reasonable steps once notified to prevent further spread of defamatory content[28].

The European Union adopts a differentiated model under the Digital Services Act. Article 7 further protects investigations and measures undertaken by providers to detect, identify and remove illegal content, thereby reducing the risk that responsible moderation itself will destroy safe-harbour protection[29]. This is doctrinally important for India because proactive moderation should not necessarily be treated as inconsistent with neutrality. The CJEU's decision in Glawischnig-Piesczek v Facebook Ireland Ltd[30] demonstrates how this framework can permit intervention without creating a general monitoring obligation. The Court held that a hosting provider, following a finding of unlawfulness, could be required to remove identical information and information with an equivalent meaning. At the time, the Court maintained the prohibition on a general obligation to monitor under Article 15 of

[27] *Shreya Singhal v Union of India* AIR 2015 SC 1523
[28] *Google India Private Ltd v M/S Visakha Industries and Anr* AIR 2020 SC 350
[29] EU Digital Services Act 2022, art 7
[30] 'Glawischnig-Piesczek v. Facebook Ireland Limited' (*Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/glawischnig-piesczek-v-facebook-ireland-limited/> accessed 16 September 2026

the e-Commerce Directive. This creates a middle ground between India's largely reactive model and unrestricted proactive monitoring.

South Korea provides a victim-oriented notice-and-removal approach. Article 44 of the Information and Communications Network Act places an obligation on information and communications service providers to endeavour to prevent the distribution of information infringing another person's rights. Article 44-2 allows a person whose privacy or reputation has been infringed to request deletion or rebuttal of the information upon substantiating the infringement. The service provider must then take measures, including deletion or temporary measures, without delay and notify the relevant parties[31]. Korea Cyber Sexual Violence Response Centre offers help to victims of tech-facilitated violence through its helpline. The centre created a process for removing non-consensual sexual content such as videos and images that have been shared online. This deletion process became the model for the National Digital Sexual Crime Victim Support Centre, which started in 2018. The centre supports victims with counselling, legal assistance, psychological support and coordination for content deletion[32].

In **eSafety Commissioner v X Corp**, under provisions like Section 109 of the Online Safety Act, the eSafety Commissioner has the power to send binding removal orders to media and digital service providers. These orders require the platforms, under Section 111, to take all steps to remove harmful, violent or cyber-abuse content, such as Class 1 material that can be accessed by people in Australia. This must happen within a short time frame, just 24 hours. If a platform fails to follow these orders, it faces financial penalties and court-ordered performance injunctions under Section 121. These measures make it clear that both foreign and domestic platforms have a legal responsibility to actively moderate and block access to dangerous online content for Australian users[33].

India has established an appellate process for intermediary grievances, while Australia has created a specialised regulatory process for online safety with direct powers to investigate

[31] Act on Promotion of Information and Communications Network Utilization and Information Protection 2016 (South Korea)
[32] 'Korea Cyber Sexual Violence Response Center' (*Kering Foundation*) <https://keringfoundation.org/en/programs/korea-cyber-sexual-violence-response-center/> accessed 16 September 2026
[33] *eSafety Commissioner v X Corp* [2024] 303 FCR 354 (Australia)

cyberbullying complaints, require the removal of harmful material and pursue enforcement against non-compliant platforms.

SUGGESTIONS

The last chapters will state that India's implementation of reform must not use any foreign model but carry out the measured model legislation which contains a set of rules taking only those practices of the EU, UK, Australia and South Korea where the systems performed better than India:

From the EU (Digital Services Act): A legislative 'Good Samaritan' clause making proactive moderation possible without losing immunity, as well as a two-tiered system of responsibilities adjusted to the size of the platform and risk applied, replacing the rules existing in India where the same detailed responsibility rule is applied to all intermediaries alike, for example, the same rigid periods of shifting content.

From the UK (Online Safety Act): An independent sector regulator (like Ofcom), which can create obligatory regulations in relation to the content of cyberbullying and harassment, not relying only on a court order to block it. The watchdog, i.e.Ofcom, is encouraging the use of 'hash-matching' technology, which enables platforms to remove an image that has been reported as problematic. With this system, when a user reports an image or video, it is compared against a database of illegal images, such as revenge porn or explicit deepfakes, which have been turned into 'hashes,' or digital fingerprints. This process helps identify and eliminate harmful images from being shared online[34].

From South Korea: Sector-based legislative mechanisms initiated by harm show that legislation can be implemented in immediate response to observable damage, with victims at the centre of the legislation, and the current Indian approach is insufficient.

- Establish a specialised online safety regulator like Australia's eSafety Commissioner or the UK's Ofcom, which would have the authority to issue directly enforceable takedown orders. This would complement the existing Grievance Appellate Committee's limited jurisdiction.

[34] Dan Milmo, 'Ofcom urges social media platforms to combat abuse and limit online 'pile-ons'' *The Guardian* (25 November 2025) <https://www.theguardian.com/media/2025/nov/25/ofcom-social-media-platforms-online-abuse-measures-limit-pile-ons> accessed 16 September 2026

- Narrow and specify the 'actual knowledge' standard, building on South Korea's victim-centric approach, particularly with regard to cyberbullying.
- Finally, introduce victim support measures such as cyber tribunals, expedited civil remedies and counsellors, in addition to due diligence obligations for platforms.

CONCLUSION

Based on the comparative analysis, it is evident that India's safe harbour framework embodied in the IT Act, 2000, and the IT Rules, 2021, is built on an outdated theoretical foundation of 'passive intermediary'. While the safe harbour doctrine indeed promotes innovation and freedom of expression values, India's approach is currently failing to address the challenges of perpetual and repetitive cyberbullying by leveraging the opportunities provided by the evolving digital ecosystem. India's current rules are therefore counter-productive, as they fail to provide clarity, prevent abuse of the legal uncertainty and essentially rely on an overly broad 'actual knowledge' standard, which is ill-suited for the task of detecting cyberbullying. In contrast, the EU's Digital Services Act embodies a balanced approach, which builds on the principle of risk differentiation and introduces a 'Good Samaritan' clause.

The Online Safety Act of the UK builds on the separation of powers principle by empowering Ofcom to adopt directly enforceable industry codes of conduct. South Korea's experience with continuous cyberbullying of its celebrities (Sulli case) has led to the introduction of a victim-centric approach to online safety. Australia's model is notable for creating a specialist eSafety Commissioner with direct enforcement powers over social media companies.

While India cannot copy other jurisdictions' approaches, it can draw global inspiration in updating its rules to promote accountability without compromising the freedom of expression values enshrined in the Constitution (particularly Article 19(1)(a)).