CYBERBULLYING AND MENTAL HEALTH: LEGAL DIMENSIONS OF SOCIAL MEDIA'S IMPACT ON EMOTIONAL WELL-BEING

Rakshit Aggarwal & Ananya Singh, LL.M., Gujarat National Law University, Gandhinagar

ABSTRACT

The prevalence of cyberbullying is rising in the digital era, and it poses serious risks to psychological integrity and mental health that are frequently disregarded. Indian legal systems are still fragmented when it comes to addressing the emotional and social trauma that comes from online abuse, which is at par with conventional forms of violence. This paper underscores a doctrinal analysis of cyberbullying through the lens of constitutional rights, statutory protections, and mental health jurisprudence. The study examines relevant constitutional protections under Articles 14, 19, and 21 of the Constitution of India, advocating for a broader recognition of psychological injury as a violation of digital dignity. The paper identifies key enforcement challenges, including anonymity, jurisdictional barriers, evidentiary limitations, and underreporting. It also encompasses a multi-tiered legal reform strategy encompassing codification of cyberbullying as a distinct offense and mental health-informed redress mechanisms. Therefore, the paper delves into the realm of cyberbullying that must be recognized not merely as a behavioural or technological issue but as a significant legal and human rights concern requiring urgent and comprehensive reform.

Keywords: Cyberbullying, Mental Health, Digital Rights, Constitutional Law, Platform Accountability

1. INTRODUCTION

The widespread influence of social media platforms has made cyberbullying one of the most complicated and crucial issues of the digital age. Cyberbullying differs from traditional bullying such that it occurs in a 24/7 setting where damaging content may be quickly amplified, permanently stored, and extensively distributed. Due to features that promote anonymity, virality, and algorithmic amplification, social media platforms like Instagram, Facebook, Twitter (now X), and Snapchat have created interactive spaces that also facilitate harassment, public shaming, and psychological targeting while encouraging expression and connectivity. This dynamic type of online abuse may manifest in numerous forms, such as doxing, impersonation, trolling, and the unapproved sharing of private information. Its effects are extensive, and victims frequently suffer from long-term mental health issues like suicidal thoughts, anxiety, sadness, and self-harm. Despite these negative effects, India's traditional legal systems have been slow to acknowledge the unique nature and seriousness of cyberbullying.

The prerequisite for a doctrinal legal analysis stems from the realization that the current statutory and constitutional instruments cannot adequately capture the psychological and emotional harm caused by these digital environments. Without explicit, enforceable, and platform-specific legal rules, it is becoming more and more unacceptable that vulnerable people, particularly women, children, and disadvantaged groups, continue to be targeted in virtual spaces. The identification of doctrinal and institutional deficiencies, evaluation of the effectiveness of Indian legal protections, and proposition of comprehensive reforms that prioritize mental health and digital dignity within cyberlaw are the objectives of this research. Through social media, it aims to portray cyberbullying as a severe legal injury that requires immediate legislative, constitutional, and regulatory action, rather than just a behavioural or technological dilemma.

The scope of this study is limited to Indian laws and legal principles governing cyberbullying, while drawing comparative insights from select foreign jurisdictions such as the UK, USA, and the European Union. The focus is on legal instruments that directly or indirectly address the intersection of cyber abuse and emotional harm. The significance of this research lies in its attempt to frame mental health damage as a legally cognizable harm within the realm of cyber regulation. In the wake of increasing suicides and psychiatric disorders linked to online abuse,

the law's silence on psychological injury becomes untenable. By critically examining legislative and judicial approaches, the study seeks to fill the normative gap in legal scholarship and offer actionable recommendations for a victim-centric, rights-based regulatory framework. It urges lawmakers, courts, and platforms to treat cyberbullying not as trivial or inevitable, but as a serious violation of human dignity and constitutional values.

2. CYBERBULLYING: A LEGAL DIMENSIONAL OUTLOOK

2.1 Definitions and Characteristics

Cyberbullying lacks a uniform definition across jurisdictions, which creates a significant obstacle for consistent legal interpretation and enforcement. Generally, it refers to any intentional and repetitive conduct carried out using electronic means to harass, threaten, humiliate, or harm another individual. Unlike traditional bullying, it often includes elements of anonymity, permanence of content, viral dissemination, and public visibility, which make its impact more severe and long-lasting.

Legal definitions of cyberbullying vary. In India, the Information Technology Act, 2000, does not define "*cyberbullying*" per se, although various provisions may apply to cyber abuse. Courts have interpreted online harassment within the broader framework of cybercrime, but without specific terminology or coherent jurisprudence. In contrast, countries like the United States have state-level statutes that define and criminalise cyberbullying explicitly, while the United Kingdom addresses it under laws related to malicious communications and harassment.

The key characteristics that set cyberbullying apart as a distinct legal harm include -

- Permanence and Dissemination: The harmful content, once posted, may be difficult or impossible to erase.
- Anonymity of Perpetrators: Abusers often operate behind pseudonyms or fake profiles, complicating prosecution.
- Amplification Through Technology: The speed and scope of online platforms can turn a single comment into mass humiliation.
- Psychological Targeting: Cyberbullying often aims to exploit vulnerabilities such as body

image, sexuality, gender identity, caste, or religion.

These traits necessitate a legal framework that recognizes the digital environment's unique properties. The laws designed for physical-space harm are inadequate in addressing the diffuse, asynchronous, and borderless nature of online abuse. Therefore, there is an urgent need to codify cyberbullying as a standalone offense, with definitional clarity that captures its distinct dimensions.

Cyberbullying differs substantially from traditional harassment, not only in its methods but also in the depth and breadth of harm caused. In traditional settings, bullying is often confined to physical spaces like schools, workplaces, or neighbourhoods, and usually ends when the victim is physically removed from the environment. In cyberspace, however, the abuse follows the victim into their private and personal spaces, rendering escape nearly impossible.

Some key legal and psychological distinctions include -

- Spatial and Temporal Ubiquity: Cyberbullying occurs 24/7, often invading victims' homes and personal time.
- Evidentiary Complexity: Screenshots, metadata, and digital forensics are often required for proof, complicating legal processes.
- Lack of Witnesses or Interveners: Traditional bullying might be witnessed and stopped; cyberbullying is often hidden.
- Public Shaming and Viral Content: The reputational damage in cyberbullying is extensive due to the potential virality of posts.
- Platform Mediation: Unlike in physical settings, digital intermediaries (like Facebook, X, or Instagram) play a role, raising questions of platform responsibility.

While harassment laws under the Bhartiya Nyaya Sanhita, 2023 (BNS), cover several forms of verbal and physical abuse, they fall short in addressing these online-specific nuances. For instance, the concept of “outraging the modesty of a woman” under Section 354 of the IPC

1860[1](*now section 74 BNS*) may apply in some cases, but the lack of gender-neutral platform-aware provisions reveals a vital gap. Legislators must be aware of these distinctions to create legislation that not only makes harmful conduct illegal but also offers victims easily available remedies that are appropriate for the digital age.

2.2 Mental Health Impact as Legal Injury

Cyberbullying inflicts psychological harm that can be as debilitating as physical injuries. However, the law has been slow to treat mental health impairments as actionable harms in themselves, especially when caused by non-physical conduct. Emotional trauma, anxiety, depression, post-traumatic stress, and suicidal ideation have all been linked to sustained online abuse, yet the Indian law has limited provisions that recognize these outcomes as grounds for civil or criminal liability.

The legal treatment of mental health injury typically depends on proving causality, foreseeability, and intent. This can be particularly challenging in cyberspace, where abuse is often perpetrated anonymously and cumulatively, rather than through a single identifiable act. Moreover, the stigmatization of mental health itself deters victims from seeking legal redress.

Several international jurisdictions have begun to shift this narrative. For example, the UK's Online Safety Act[2] mandates that platforms assess psychological harm risks to users and design moderation systems accordingly. In Canada, civil liability can arise from the intentional infliction of mental suffering. Indian jurisprudence, however, remains tentative. Article 21 of the Constitution has been expanded to include mental health as part of the right to life and dignity.[3] However, the application of this principle to cyberbullying cases remains underdeveloped.

The explicit recognition of emotional and psychological trauma as a separate legal tort under Indian law is now required. In addition to supporting criminal penalties, this acknowledgement also needs to make it possible for victims to pursue civil remedies like injunctions and compensation. To assess harm and provide victim support, mental health specialists ought to

[1] Indian Penal Code, § 354 (1860) (India).
[2] Online Safety Act 2023, c. 50 (UK).
[3] Francis Coralie Mullin v. Administrator, Delhi, (1981) 1 SCC 608

be included in legal proceedings. A significant amount of the suffering experienced by victims of cyberbullying goes unnoticed since mental health problems are not recognized by the law.

2.3 Role of Social Media Platforms in Enabling Cyberbullying

Social media platforms are dynamic online environments where users can produce, disseminate, and interact with information in a variety of media, including text, photos, videos, and audio. These platforms, which are mostly accessed through mobile apps and web browsers, serve as virtual communities that facilitate social networking, real-time collaboration, and communication. The well-known websites like Facebook, Instagram, Snapchat, YouTube, LinkedIn, Twitter (now X), and others each have different purposes, ranging from microblogging and visual storytelling to professional networking.

Social media makes connections simpler, but it also creates conditions that encourage cyberbullying. The design of algorithm-driven visibility, quick material sharing, and anonymity makes it possible for destructive conduct to proliferate and endure. It has become common practice to use tactics including doxing, impersonation, meme-based shaming, targeted abuse, and distributing private content without consent. This conduct, in contrast to offline bullying, is ongoing, international, and frequently humiliating in public, which exacerbates psychological injury. There is a substantial impact on mental health. Poor self-esteem, anxiety, and body dissatisfaction have all been related to repeated exposure to idealized imagery, particularly in young people. When people contrast their lives with well-manicured online representations of others, FOMO intensifies this feeling of inadequacy. In addition, the dopamine-reward loop that social media provides through likes, comments, and shares promotes obsessive use, which can result in digital addiction, sleep disturbances, and poor performance at work or in school. Overuse of social media, being the victim of cyberbullying, and psychological consequences, including depression and self-harm, are strongly correlated. These patterns highlight the pressing need for legislation that requires platforms to implement preventive, transparent, and trauma-sensitive design and moderation procedures in addition to criminalizing online abuse.

3. LEGAL FRAMEWORK GOVERNING CYBERBULLYING IN INDIA

3.1 IT Act, 2000 and its Amendments

The Information Technology Act, 2000 (IT Act) serves as India's foundational statute for

governing cyber activities, including offences related to cyberbullying. While the Act does not use the term "*cyberbullying*" explicitly, several of its provisions address behaviours that fall within its scope. Section 66A[4], which criminalised sending offensive messages via communication services, was initially used to prosecute online harassment cases. However, the Supreme Court struck it down in ***Shreya Singhal v. Union of India (2015)***[5] for being vague and violative of Article 19(1)(a)[6].

Despite the striking down of Section 66A, other sections remain relevant. Section 66E penalises the violation of privacy by capturing or transmitting images of private areas without consent.[7] Sections 67 and 67A deal with the publishing or transmission of obscene material in electronic form, which can apply to the circulation of non-consensual intimate images, a common tactic in cyberbullying.[8] Section 72 criminalises the breach of confidentiality and privacy by those who have access to personal data under a lawful contract.[9]

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, significantly modified the regulatory landscape. These rules place due diligence obligations on intermediaries (social media platforms), including grievance redress mechanisms and timelines for content takedown. Rule 3(2)(b) mandates the publication of grievance redressal mechanisms by intermediaries and the appointment of grievance officers.[10] For significant social media intermediaries, the rules require the identification of the first originator of the message in cases related to security and public order provision potentially useful for cyberbullying investigations.

Yet, there are still gaps. The IT Act does not include non-sexual types of cyberbullying including doxing, trolling, or social exclusion; instead, it focuses on pornographic and sexually explicit content. The victims frequently lack clear legal redress due to the scattered application and enforcement of the absence of a comprehensive statutory definition of cyberbullying.

[4] Information Technology Act, No. 21 of 2000, § 66A, India Code (2000).
[5] 2015 AIR SCW 1989
[6] India Const. art. 19(1)(a).
[7] Information Technology Act, No. 21 of 2000, § 66E, India Code (2000).
[8] Information Technology Act, No. 21 of 2000, § 67, India Code (2000).
[9] Information Technology Act, No. 21 of 2000, § 72, India Code (2000).
[10] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(2)(b), Gazette of India, Extraordinary, Part II, Sec. 3(i) (Feb. 25, 2021) (India).

3.2 Data Protection and Emotional Harm under DPDP Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, which emphasizes individual rights and data fiduciary duties, is a major development in India's legislative environment. The Act's elements pertaining to permission, purpose limitation, and the right to erasure make it relevant to cyberbullying even if its primary focus is informational privacy. Individuals (data principals) are empowered by the DPDP Act to access, update, and remove their sensitive personal data. In circumstances of cyberbullying, particularly when there is non-consensual sharing of private information or photographs, these rights are extremely important. Theoretically, the right to erasure might enable victims to request that material upsetting them be taken down.

The Act does not, however, specifically acknowledge emotional injury as a justification for exercising these rights. Additionally, enforcement measures are weak and mostly depend on the data protection board, which has not shown that it has the institutional competence to do so. Although the DPDP Act's conceptual scope includes the sharing of personal information that results in harassment, there is no direct correlation between it and negative effects on mental health. Lack of child-specific safeguards is another issue. The Act does not address the potential negative effects of internet exposure on children's emotional health, even though it establishes age limits and parental consent for minors. Conversely, the GDPR of the EU takes into account the child's best interests as well as possible risks, such as psychological injury. The guidelines that acknowledge emotional harm as a type of data harm could be added to the DPDP Act to provide a basis for such reform.

3.3 Juvenile Justice and Online Safety Laws

When minors are the targets of cyberbullying, complicated legal issues arise. The Juvenile Justice (Care and Protection of Children) Act of 2015 established a dual mandate of protection and rehabilitation by acknowledging both juvenile offenders and child victims. The Act isn't, however, adjusted for the digital environment. When it comes to children, cyberbullying presents unique legal issues. Although the Juvenile Justice (Care and Protection of Children) Act of 2015 acknowledges both juvenile offenders and victims, it has not been modified for the digital age. Due to their heavy reliance on internet platforms, children are particularly at risk, although non-sexual cyberbullying is not specifically addressed by Indian legislation. The 2012 Protection of Children from Sexual Offences (POCSO) Act excludes more general forms of digital abuse and only addresses sexual offenses.

There is no centralised system for reporting or addressing cyberbullying against minors, and recommendations from organizations such as the National Commission for Protection of Child Rights (NCPCR) are still non-binding. Minors are more vulnerable in the absence of obligatory reporting, grievance redressal procedures, and coordinated school-level interventions. Models such as Australia's e-Safety Commissioner serve as a model for other countries, providing specialized online safety oversight and quick resolution procedures. India does not have this kind of control over digital dangers unique to children. In the absence of comprehensive legislation, existing provisions must be interpreted purposively using Article 15[11] to support affirmative protections and Article 21A[12] to assert that digital safety is integral to the right to education. These institutional and normative weaknesses must be filled immediately through legislative change or a specific Online Child Safety Act.

4. CONSTITUTIONAL AND HUMAN RIGHTS DIMENSIONS

4.1 Right to Privacy and Psychological Integrity

The right to life and personal liberty is guaranteed by Article 21 of the Indian Constitution, a provision interpreted broadly by the judiciary to encompass many aspects of human autonomy and dignity. The right to privacy was upheld as a basic right enshrined in Article 21 in the historic ruling in ***Justice K.S. Puttaswamy (Retd.) v. Union of India***.[13] The decision's underlying principle encompasses psychological integrity and mental autonomy, despite its primary focus on informational privacy.

This acknowledgement is important in the context of cyberbullying. The frequent online harassment, public humiliation, or the unapproved sharing of private information compromises people's mental and emotional well-being in addition to their informational boundaries. Cyberbullying weakens the victim's ability to express themselves freely, causes worry, and erodes their sense of security. These impacts are inextricably tied to one's mental space, which needs to be taken into account under Article 21's protective provisions.

Indian constitutional jurisprudence has not yet specifically acknowledged emotional or psychological safety as a fundamental privacy issue, notwithstanding this broad meaning.

[11] India Const. art. 15.
[12] India Const. art. 21A.
[13] (2017) 10 SCC 1

Courts must affirmatively recognize the extension of privacy rights to digital mental well-being. When thinking about mental integrity as a crucial aspect of human dignity, comparative examples are helpful, such as the German Federal Constitutional Court's jurisprudence on personality rights. The constitutional doctrine must expand the definition of privacy to include emotional and psychological injury as a violation that can be brought to justice under Article 21 in order to successfully address cyberbullying. This would also establish a foundation for holding state and non-state actors accountable for creating or facilitating toxic digital environments.

4.2 Freedom of Speech vs. Protection from Harm

While the right to freedom of speech and expression is guaranteed by Article 19(1)(a) of the Constitution, Article 19(2) allows the State to impose reasonable limits for a variety of reasons, including public order, decency, morality, and defamation. Since it has become harder to discern between damaging information and acceptable expression in the digital sphere, this balance becomes even more fragile. The invoking of protections under free speech, cyberbullying frequently poses as opinion, parody, or critique. However, jurisprudence has acknowledged that communication that advocates discrimination, incites hatred, or harms someone psychologically is not protected by the right to free speech. In ***Shreya Singhal v. Union of India***[14], the Court recognized the State's authority to control speech considered defamatory or inciting, even as it invalidated Section 66A of the IT Act for being ambiguous.

Insofar as the intervention is appropriate and well-targeted, this suggests a constitutional framework that can support regulatory action in cyberbullying cases. For instance, the reasonable limits provision may be used to restrict online content that degrades, threatens, or shames people, especially when it is done anonymously. The "reasonable" criterion needs to be recalculated in digital domains, where the effects are serious and far-reaching even though they are not always immediate or tangible. Digital platforms must stop online hate and abuse without unreasonably restricting free speech, according to international human rights organizations like the UN Human Rights Council. India must carefully balance its constitutional obligations through law and jurisprudence in order to fulfill these twin responibilities.

[14] Supra note 5.

4.3 Substantive Equality in the Digital Space

Article 14 of the Constitution guarantees equality before the law and equal protection of the law. Over time, this has evolved to mean not just treating everyone the same, but treating people differently when needed to ensure genuine fairness. In the digital world, especially when addressing cyberbullying, this means recognising that some groups, like women, LGBTQ+ individuals, children, and marginalised communities, face more harm than others.

Online spaces often mirror and amplify social prejudices, enabling unchecked misogyny, casteism, and homophobia. Applying general laws equally to all can miss the deeper, unequal impact on vulnerable groups. For instance, harassment of LGBTQ+ creators or Dalit voices often includes identity-driven hate, not just random trolling. Ignoring this context hides the power imbalances at play. To truly uphold equality, the law must recognise these differences and respond with tailored safeguards. Article 14 can support targeted protections such as mandatory grievance redressal systems for high-risk users, bias checks on platform policies, and transparent algorithms, to better protect those more likely to be harmed online

5. MENTAL HEALTH AND THE LAW: NEED FOR INTEGRATION

5.1 Legal Recognition of Emotional Distress

The recognition of emotional distress as a legal harm has long been marginal in Indian jurisprudence. Tort law in India, based on common law traditions, allows claims for mental anguish under specific conditions often as part of damages in defamation, breach of privacy, or custodial abuse. However, emotional or psychological injury is rarely treated as a standalone basis for legal action. In the context of cyberbullying, this poses a substantial barrier to justice, as much of the harm inflicted manifests as mental health deterioration rather than physical injury

Some recognition exists through judicial precedents. For example, in ***R. Rajagopal v. State of Tamil Nadu***[15], the Supreme Court upheld a right to privacy that includes the emotional space of individuals. In ***State of Maharashtra v. Madhukar Narayan Mardikar***[16], the Court acknowledged the right to dignity and mental peace, even in the absence of physical harm.

[15] (1994) 6 SCC 632.
[16] (1991) 1 SCC 57.

However, these acknowledgements are not consistently translated into actionable legal standards. As a result, victims of cyberbullying must often stretch existing doctrines or combine multiple legal avenues to seek redress.

The recognition of emotional distress as an autonomous injury would require legislative reform. Statutes governing cyber offenses, defamation, and personal data protection must incorporate mental harm as a compensable and punishable outcome. Additionally, procedural rules should be modified to allow for expert testimony from mental health professionals to substantiate claims of psychological impact. These changes would align Indian law with countries such as the UK and Canada, where mental distress is becoming more widely recognized in both civil and criminal cases.

5.2 Role of Mental Health Legislation

The Mental Healthcare Act, 2017 (MHCA), which places a higher priority on patient rights, dignity, and access to care, marks a significant change in India's mental health legislation. It recognizes that mental health is a spectrum that includes both well-being and sickness. In fact, though its connection to cyber-related hazards is still mostly unknown. The MHCA's Section 18 ensures that everyone has the right to receive mental health care and treatment from government-run or funded programs.[17] When combined with the State's obligations under Article 21, this clause provides a strong basis for arguing that victims of cyberbullying are entitled to therapeutic assistance. A mental health evaluation is also required for those who attempt suicide, many of whom may have been victims of cyberbullying, and Section 115 of the Act decriminalizes suicide.

The MHCA and cybercrime law enforcement do not have an institutional link despite this forward-thinking architecture. Police officers looking into cybercrimes hardly ever recommend psychological assistance to victims. Similarly, in cases of cyber harassment, mental health specialists are not included in the grievance redressal or adjudicatory processes. The end effect is a disjointed strategy in which the healthcare system functions independently while the legal system seeks responsibility. The institutional procedures that connect MHCA frameworks with IT Act investigations are necessary to close this gap. Cybercrime cells could have dedicated mental health officers assigned to them. When cyberbullying causes observable mental harm,

[17] Mental Healthcare Act, No. 10 of 2017, § 18, India Code (2017).

courts may order counselling or a psychiatric examination. In tackling online abuse, this would signal a paradigm shift away from punitive justice and toward reparative justice.

A victim-centric framework is lacking in current legislation, such as the IT Act and IPC, and courts hardly ever order psychological treatment or compensation for emotional injury. Public interest litigation, though helpful, cannot address individual trauma. To close this gap, a rights-based framework must include -

- Mental health services as part of legal redress
- Compensation for emotional distress
- Platform-level psychological support mechanisms
- Judicial standards for evaluating mental harm

6. COMPARATIVE JURISPRUDENCE

6.1 UK's Malicious Communications Act and Online Safety Act

The United Kingdom has taken a proactive stance on regulating online abuse through both statutory provisions and evolving regulatory models. *The Malicious Communications Act, 1988* criminalizes the sending of letters, electronic communications, or articles with the intent to cause distress or anxiety. *Section 127 of the Communications Act 2003* penalizes offensive, indecent, obscene, or menacing messages transmitted via public electronic communications networks.[18]

While these laws have provided a framework for penalizing cyberbullying conduct, criticism regarding vagueness and overreach led to a rethinking of legal design. This culminated in the drafting of the *Online Safety Act (OSA) 2023,* which aims to impose a duty of care on digital platforms. The OSA mandates risk assessments, content moderation protocols, and algorithmic transparency, particularly concerning harms affecting children and mental health. It introduces the concept of "*legal but harmful*" content, obligating platforms to proactively manage risks, even where the content does not cross criminal thresholds.

[18] Communications Act 2003, c. 21, § 127 (UK).

The UK's approach offers two key lessons: Firstly, platform liability and regulatory oversight are essential complements to criminalization. Secondly, through impact assessment and systemic preventative requirements, mental health considerations can be incorporated into digital governance. While some of these concepts are reflected in India's IT Rules 2021, they do not have the institutional enforcement mechanisms or the explicit mental health regulations that the OSA envisioned.

6.2 US Federal and State Cyberbullying Statutes

A number of state-level laws offer strong regulatory capabilities, but the US lacks a comprehensive federal law that addresses cyberbullying. Forty-eight states have passed anti-bullying laws that specifically address cyberbullying, with a special emphasis on educational settings. The Education Code of California, for example, requires school districts to create policies to prevent and deal with student cyberbullying, including restorative justice programs and cognitive therapy.

The Children's Online Protection Act, 1999 (CIPA) ties federal funding to adherence to online safety regulations. Although not specific to cyberbullying, CIPA highlights the federal government's indirect regulatory influence. The civil lawsuits for intentional infliction of emotional distress or defamation offer remedies in the absence of direct federal statutes. The US jurisprudence maintains a strict boundary between free speech and harmful content that is grounded in the First Amendment. Courts are reluctant to criminalize online expression unless it meets clear tests for incitement, threats, or targeted harassment. In ***Elonis v. United States (2015)***, the Supreme Court overturned a conviction for online threats due to a lack of proof of subjective intent, demonstrating the high threshold for criminal sanctions.[19] India can learn from the decentralized, education-integrated response in the US, especially in applying restorative and therapeutic remedies. However, care must be taken not to overprotect speech at the expense of victims' mental health, especially given differing constitutional frameworks.

6.3 EU Approaches: Digital Services Act and GDPR

The European Union (EU) has adopted a holistic regulatory architecture to govern online safety, combining user rights, platform obligations, and mental health protections. *The Digital*

[19] 575 U.S. 723 (2015).

Services Act (DSA), effective from 2024, imposes significant responsibilities on online platforms to prevent systemic risks, including psychological harm caused by cyberbullying. It mandates annual risk assessments, independent audits, and crisis protocols to mitigate harm to users' fundamental rights, especially among vulnerable populations.

The DSA is facilitated by the *General Data Protection Regulation (GDPR),* which safeguards users' control over personal information, which is frequently used as a conduit for cyberbullying. The GDPR gives users the right to request that content be removed (right to be forgotten), that inaccurate information be corrected, and that data processing be limited. These resources give victims of cyberbullying the ability to take back control of their online persona. The GDPR acknowledges that emotional harm can result from data misuse, unlike India's DPDP Act, which focuses more narrowly on consent and processing. The GDPR's Recital 75 recognises "*psychological harm*" and "*loss of control over personal data*" as hazards that data protection regulations need to mitigate.

The EU approach provides a thorough combination of remedial, punitive, and preventative measures. This raises the possibility that comprehensive legal reform that unifies data protection, online safety, and mental health requirements into a unified framework for digital rights could be beneficial for India. According to a comparative study, legal remedies vary depending on the setting, even though cyberbullying is a worldwide issue. India stands to gain by implementing -

- Clear statutory definitions and standalone cyberbullying offenses (UK, US)
- Mandatory content moderation and platform duty of care (UK OSA, EU DSA)
- Restorative justice and educational interventions (US State laws)
- Legal recognition of emotional distress and psychological harm (EU GDPR)
- Special protections for children and marginalized communities (all jurisdictions)

These observations highlight the necessity for Indian cyber legislation to adopt a preventive, participatory, and reparative strategy rather than a punitive one. When creating laws and policies, mental health must be a primary issue rather than an afterthought.

7. CHALLENGES IN ENFORCEMENT AND REDRESSAL MECHANISMS

7.1 Anonymity, Jurisdiction, and Platform Liability

The structural nature of digital communication presents one of the biggest obstacles to the enforcement of laws against cyberbullying. The anonymity provided by internet networks gives offenders more confidence, making it very challenging to identify and hold them accountable. Pseudonymous accounts, VPNs, and offshore platforms are frequently used by criminals to hide their identities. The law enforcement organizations frequently lack the cross-border collaboration procedures and technological capability necessary to successfully track down such actors.

The enforcement is made more difficult by jurisdictional concerns. State and national borders are often crossed by cyberbullying, which leaves legal problems regarding the prosecutorial jurisdiction. Mutual Legal Assistance Treaties (MLATs) are frequently unresponsive, cumbersome, and unprepared to handle urgent online harms. Because of this, a large number of cyberbullying cases are either dropped or never looked into because of unclear jurisdiction. Another unresolved problem is platform liability. The "safe harbor" provision under Section 79 of the IT Act[20] remains to protect intermediaries unless they wilfully aid or abet or fail to act upon a particular notification, even though India's IT Rules 2021 establish due diligence obligations. When there is no proactive obligation to keep an eye on or stop cyberbullying, damaging content can continue to exist and frequently causes irreversible harm. India needs more precise laws requiring proactive flagging systems, speedier takedowns, and legally enforceable collaboration agreements between law enforcement and platforms. The bilateral and multinational treaties that more effectively handle jurisdiction and data-sharing must also improve cross-border coordination.

7.2 Underreporting, Evidentiary Barriers and Platform Moderation

A prevalent issue in situations of cyberbullying is underreporting. Because of societal stigma, fear of reprisals, or skepticism about the system's responsiveness, victims frequently hesitate to come forward. This hesitation is made worse in vulnerable areas, where legal redress is discouraged by cultural taboos, a lack of computer literacy, or a fear of institutional reprisal.

[20] Information Technology Act, No. 21 of 2000, § 79, India Code (2000).

Evidentiary difficulties occur even when cases are disclosed. Typically, screenshots, chat logs, or metadata are used to document cyberbullying instances; however, without verified forensic validation, these records may be edited or deemed inadequate. Furthermore, a lot of platforms only keep user data for a short period of time, which makes it challenging to collect admissible evidence following delays.

Prosecution is hampered by the absence of standardized procedures for gathering, storing, and authenticating digital evidence. Furthermore, courts may not always have the qualified staff to evaluate the psychological effects of cyberbullying. A large percentage of injuries go unrecorded in court records because mental health testimony is rarely requested or accepted. While social media platforms have made strides in moderation, most rely heavily on automated content filters and user-flagging systems. These mechanisms, though efficient at scale, lack contextual judgment, often failing to capture subtle or targeted harassment. Moreover, platforms have limited incentive to police abuse proactively, as doing so may conflict with engagement-driven business models. The "safe harbor" protection under Section 79 of the IT Act, 2000 shields platforms from liability as long as they do not initiate the transmission or fail to act upon specific notice. This reactive model has proven inadequate in addressing fast-moving and psychologically damaging forms of abuse. Even after complaints, content removal can be slow, appeals opaque, and account bans inconsistently enforced. India needs a revised safe harbor framework that distinguishes between passive and active intermediaries. Platforms that algorithmically amplify harmful content or repeatedly fail to act on credible complaints should face penalties, including monetary fines or operational restrictions. The grievance officers must be made legally accountable, with enforceable standards for transparency, responsiveness, and victim engagement.

India lacks a centralized, coordinated institutional framework to deal with cyberbullying comprehensively. Jurisdiction is fragmented across ministries, law enforcement agencies, and educational institutions. This often leads to blame-shifting, bureaucratic inertia, and policy overlap. Unlike jurisdictions such as Australia (e-Safety Commissioner) or the UK (Ofcom under OSA), India does not have a single public authority tasked with ensuring digital safety. Consequently, there is no consolidated registry of complaints, no unified training protocols, and no national policy on cyberbullying awareness and redressal mechanisms.

8. CONCLUSION AND SUGGESTIONS

Cyberbullying is one of the most pervasive harms emerging from our hyper-connected digital era, with deep implications for dignity, mental health, and social justice. Though non-physical in form, its psychological toll is severe, amplified by the very architecture of social media platforms that allow anonymity, rapid dissemination, and algorithmic amplification of abuse. These platforms are no longer passive hosts but active participants in shaping online discourse, and thus cannot be excluded from legal accountability.

This paper has proposed in favor of a comprehensive, rights-based framework that prioritizes emotional well-being as a fundamental constitutional priority, replacing India's disjointed and reactive legal system. It is evident from doctrinal examination of Indian legislation, constitutional jurisprudence, and comparative international practices that current frameworks do not adequately require platforms to prevent, identify, and respond to abuse, and therefore underrecognize psychological injury. While digital platforms continue to function under extensive "safe harbor" protections, victims encounter several obstacles, such as underreporting, evidential difficulties, and institutional indifference. The legal remedies are meaningless in the absence of platforms' affirmative obligations to protect victims and properly control content.

India must enact a dedicated statute or amend the IT Act to define and criminalize cyberbullying explicitly to address the fragmented nature of existing laws. The definition should be inclusive of different forms of textual, visual, impersonation, exclusion, and data-based bullying and cover both adult and child victims. This codification should recognize psychological injury as a principal form of harm and include both criminal and civil remedies. A statutory definition will bring clarity for law enforcement, simplify evidentiary standards, and increase public awareness. The guidelines on sanctions, grievance procedures, and victim protection measures should be included, together with model rules for execution.

The study advocates a multifaceted approach, including creating a National Digital Safety Authority, enforcing platform regulations, integrating mental health into cyber legislation, and classifying cyberbullying as a separate crime. In order to combat cross-border abuse and conform to international best practices, legislative harmonization and international cooperation are also crucial. In conclusion, it is no longer optional to acknowledge cyberbullying as a type of digital violence, particularly when it occurs through social media. For the rights to privacy,

dignity, and mental health to be protected online, the law must change along with technology. The legal frameworks that protect human dignity in virtual environments are just as important to the future of digital citizenship as advancements in technology.