CYBERBULLYING AND ONLINE HARRASMENT: LEGAL CHALLENGES

Aryawat Khandelwal, Amity University, Noida

Dr. Niharika Singh, Amity University, Noida

Introduction

1.1 Defining Cyberbullying and Online Harassment:

Intentional and persistent harm caused by electronic devices, including computers, smartphones, and other gadgets, is known as cyberbullying. Usually, this behaviour consists of violent acts meant to threaten, degrade, or embarrass those who are unable to defend themselves.

The term "online harassment" refers to a wider variety of actions carried out through digital platforms, such as rude and unwelcome emails, threats, stalking, and the spread of misleading information. Online harassment can impact people of all ages and in a variety of settings, such as public spaces and workplaces, in contrast to cyberbullying, which frequently includes peers and is common among teenagers.

In the contemporary digital landscape, the widespread use of the internet has led to the emergence of new types of interpersonal aggression, particularly cyberbullying and online harassment. Although these terms are frequently used synonymously, they represent different behaviours that carry unique legal and social consequences.

Cyberbullying is defined as the act of using electronic communication to intimidate or harass an individual, typically through the transmission of threatening or distressing messages. This behaviour is often characterized by its repetitive nature, with the intent to instil fear, provoke anger, or induce shame in the victim. Common venues for cyberbullying include social media platforms, messaging applications, gaming sites, and various online discussion forums.

Online harassment refers to a wide range of abusive behaviours carried out through digital platforms. This term includes actions such as sending threatening communications,

disseminating false information, doxing (the act of revealing private information), and engaging in cyberstalking. In contrast to cyberbullying, which typically involves young people and peer relationships, online harassment can impact individuals of all ages and can take place in numerous settings, including workplace environments.

1.2 Forms and Manifestations:

Cyberbullying and online harassment manifest in diverse forms, each with distinct characteristics:

- **Harassment:** Persistent sending of malicious messages intended to distress the recipient.
- **Denigration:** Spreading false or harmful information to damage an individual's reputation.
- **Impersonation:** Unauthorized use of someone's identity to deceive or harm others.
- **Outing and Trickery:** Sharing personal or sensitive information without consent, often leading to embarrassment or vulnerability.
- **Exclusion:** Deliberately ostracizing individuals from online groups or activities, impacting their social interactions.
- **Cyberstalking:** Intense and repeated online monitoring or harassment that induces fear or concern for safety.

These behaviours are prevalent across various digital platforms, including social media networks, forums, and messaging services. For instance, a study highlighted that 68% of young individuals reported receiving malicious private messages, and 41% experienced social anxiety due to online abuse.

1.3 Psychological and Social Impacts:

The effects of cyberbullying and online harassment are significant, influencing victims on both psychological and social levels:

- **Mental Health Effects:** Individuals targeted by cyberbullying face a heightened risk of experiencing depression, anxiety, and suicidal thoughts. Studies show that adolescents who endure cyberbullying are more than twice as likely to display symptoms of depression and contemplate suicide compared to their peers who have not been victimized.

- **Academic and Professional Challenges:** Victims of cyberbullying often experience a decline in academic achievement, increased school avoidance, and lower job satisfaction in adulthood. The constant presence of digital harassment makes it difficult for victims to escape their tormentors, resulting in ongoing stress.

- **Physical Health Concerns:** Victims frequently report psychosomatic issues, including headaches and sleep problems, which arise from the chronic stress and anxiety linked to online harassment.

- **Social Isolation**: The public and lasting nature of online content can lead to significant embarrassment, causing victims to withdraw from social engagements and activities. This withdrawal can intensify feelings of loneliness and isolation.

The widespread nature of digital communication ensures that the consequences of cyberbullying reach far beyond the online environment, profoundly impacting victims' real-life experiences and overall well-being.

The conceptual framework of this dissertation is grounded in the intersection of law, technology, psychology, and human rights, aimed at understanding the evolving phenomenon of cyberbullying and online harassment. At its core, cyberbullying is not just a technological misdeed; it is a manifestation of harmful behaviour that uses digital mediums to exert psychological, emotional, or reputational harm on individuals. This research adopts a multidisciplinary lens, combining legal doctrines, constitutional principles, and sociobehavioural theories to explore how existing laws interact with modern-day digital abuse.

The primary conceptual foundation lies in understanding cyberbullying as a violation of fundamental rights, particularly the right to life and personal liberty under Article 21 of the Indian Constitution, which encompasses the right to dignity, privacy, and mental health. The framework draws on the theory of legal positivism and natural law principles, acknowledging

that legal systems must adapt to technological realities to remain just and relevant. Additionally, the Harm Principle by John Stuart Mill serves as a guiding moral compass, suggesting that individual liberty can be curtailed when it causes harm to others—a critical justification for regulating online behaviour.

Another key component of this framework is the theory of deterrence in criminal law, which assumes that strict legal sanctions can prevent harmful behaviour. This theory is applied to examine whether current Indian cyber laws, despite their fragmented structure, are adequate in deterring cyber offenders. The framework also integrates elements of routine activity theory from criminology, which argues that crime is likely to occur when a motivated offender and a vulnerable target converge without a capable guardian. In the digital space, this "guardian" could be the legal system, content moderators, or even algorithmic surveillance.

Further, the framework assesses the jurisdictional challenges and limitations of domestic laws in the face of borderless cybercrimes. It questions the applicability and enforcement of Indian statutes against offenders operating from foreign territories, thus inviting a comparative inquiry into the legal systems of countries like the United States, the United Kingdom, and Australia. These international case studies provide a contextual benchmark to identify global best practices and regulatory gaps.

Incorporating victimology into the framework is essential to highlight the lived experiences of those affected by cyberbullying, especially women, children, and marginalized groups who face disproportionate risks online. It also evaluates the role of platform governance and intermediary liability, particularly under Section 79 of the Information Technology Act, 2000, which grants safe harbour to digital platforms while simultaneously expecting them to enforce due diligence.

The conceptual framework ultimately supports a rights-based and victim-centric approach, advocating for reforms that protect the mental and emotional well-being of internet users while ensuring due process and legal clarity. It underscores the need for legal modernization, international cooperation, and digital literacy, not only to respond to cyberbullying but to prevent it through education, awareness, and systemic safeguards. By anchoring this study in such a comprehensive theoretical base, the research aspires to offer actionable insights for law reform, policy enhancement, and social change in the realm of online safety.

Building on the foundational ideas of legal theories and rights-based approaches, this research further integrates the **doctrine of proportionality** and **the principle of legal certainty**, both of which are central to constitutional and cyber jurisprudence. The doctrine of proportionality, which requires that state actions (like regulating online content) must not be excessive and must be balanced against fundamental rights, is essential in evaluating the **constitutionality of legal restrictions** on online expression, particularly in democratic societies like India. Simultaneously, the principle of legal certainty mandates that laws must be clear, predictable, and not open to arbitrary interpretation—a significant issue in India's current cyber laws, where vague definitions of terms like "offensive," "obscene," or "threatening" have led to misuse and inconsistent enforcement.

The conceptual framework also borrows from psychological and behavioural science, particularly in understanding the mental health implications of cyberbullying. According to the World Health Organization, cyberbullying is now recognized as a public health issue, with victims reporting increased rates of anxiety, depression, suicidal ideation, and emotional trauma. The Cognitive Behavioural Theory (CBT) model is referenced to explain how repeated exposure to online abuse can negatively alter an individual's thought processes, leading to selfblame, withdrawal, or even retaliatory behaviour. These psychological impacts justify the need for not only legal remedies but also psychological intervention, digital counselling, and traumainformed care.

A critical axis of this framework is the role of digital intermediaries, such as Facebook (Meta), Instagram, X (formerly Twitter), and YouTube, which are often the platforms where cyberbullying occurs. Under Section 79 of the IT Act, these intermediaries enjoy conditional "safe harbour," meaning they are not liable for third-party content unless they fail to act upon government directives or user complaints. However, the lack of a robust grievance redressal mechanism, noncompliance with takedown timelines, and inadequate moderation, especially in Indian regional languages, have made these platforms complicit in sustaining online harm. Therefore, the framework critiques the current self-regulatory model and examines international shifts toward co-regulation, where tech companies are held accountable through independent regulators or compliance frameworks—as seen in the EU's Digital Services Act or Australia's eSafety laws.

The framework also emphasizes the importance of digital citizenship and literacy as preventive

tools. A digitally literate society can better recognize, report, and resist cyberbullying. The UNESCO Digital Citizenship Education (DCE) model offers valuable insights into building safe online spaces by equipping users, especially children and adolescents, with critical thinking, empathy, and reporting skills. In India, however, digital literacy remains uneven, particularly among women, rural populations, and non-English-speaking users. This digital divide contributes to both increased victimization and decreased awareness of available legal remedies.

Another conceptual layer is the global vs. local dichotomy. While cyberbullying is a global phenomenon, legal responses must consider local values, societal norms, and constitutional boundaries. Hence, this research situates India's legal response within a global context—adopting global standards but customizing them to Indian realities. The comparative framework used herein will analyse how international best practices, such as the UK's Online

Safety Act 2023, California's anti-cyberbullying statutes, or New Zealand's Harmful Digital Communications Act 2015, can inform Indian legal reforms without compromising on civil liberties like freedom of speech.

Lastly, this conceptual framework embraces a multi-stakeholder ecosystem model. Addressing cyberbullying effectively requires synergy between the judiciary, legislature, executive, civil society, educational institutions, parents, and tech companies. The "whole-of-society" approach, as endorsed by the United Nations Office on Drugs and Crime (UNODC) in its 2021 cybercrime strategy report, supports this inclusive governance model. This approach not only strengthens enforcement but fosters a culture of digital responsibility and empathy.

In essence, this research adopts an integrative and forward-looking conceptual lens—one that is not confined to punitive law alone but extends to platform ethics, victim rehabilitation, digital literacy, constitutional values, and comparative jurisprudence. It provides the scaffolding to critically assess where India currently stands and how it can shape a progressive, inclusive, and enforceable legal architecture for online safety.

To gain a comprehensive understanding of cyberbullying and online harassment, this conceptual framework employs a socio-legal lens, acknowledging that legal measures cannot function independently of societal contexts. The presence of legal statutes alone is inadequate if they fail to address the social issues of discrimination, stigma, and marginalization.

Cyberbullying has a disproportionate impact on specific groups, including women, LGBTQ+ individuals, religious minorities, and persons with disabilities, necessitating a focus on social justice. However, the

Indian legal framework frequently neglects these intersecting factors. Consequently, this research critically examines whether India's policies on cybercrime and their enforcement effectively tackle the imbalances of power and identity-based targeting inherent in online abuse.

Additionally, this framework addresses the technological shortcomings in legal enforcement. While technology can facilitate abuse, it also possesses the capability to prevent and trace such actions. Nevertheless, law enforcement agencies in India often lack the necessary cyber forensic resources, AI-driven content monitoring systems, and adequately trained digital personnel, resulting in ineffective or delayed investigations and prosecutions. A report by the Data Security Council of India (DSCI) revealed that over 70% of police stations in India are ill-equipped to handle cybercrime investigations efficiently. This gap between technology and legal enforcement represents a significant barrier, highlighting the critical need for enhancing the skills and capabilities of law enforcement officials in the digital realm.

2. International Legal Perspectives

2.1 United States:

In the United States, cyberbullying and online harassment are primarily addressed at the state level, with each state enacting its own legislation. As of recent data, all 50 states have laws that address bullying, and most include provisions related to cyberbullying.

- **State Laws**: Many states have specific statutes that define and prohibit cyberbullying, especially within educational settings. These laws often mandate schools to implement policies addressing cyberbullying incidents.

- **Federal Laws**: While there is no federal law that specifically addresses cyberbullying, certain federal statutes may apply in severe cases, such as the Computer Fraud and Abuse Act (CFAA) and the Children's Online Privacy Protection Act (COPPA).

- **Enforcement Challenges**: The decentralized nature of legislation leads to inconsistencies in definitions, protections, and penalties across states. Additionally, jurisdictional issues arise when cyberbullying crosses state lines.

2.2 United Kingdom

The UK addresses cyberbullying and online harassment through a combination of legislation:

- **Protection from Harassment Act 1997**: This act criminalizes harassment, including that conducted online.
- **Malicious Communications Act 1988**: Prohibits sending electronic communications that are grossly offensive or threatening.
- **Communications Act 2003**: Section 127 makes it an offense to send messages that are grossly offensive or of an indecent, obscene, or menacing character over public electronic communications networks.
- **Online Safety Bill**: Introduced to impose a duty of care on online platforms to protect users from harmful content, including cyberbullying.

2.3 Canada

Canada has taken legislative steps to address cyberbullying, particularly following high-profile cases:

- **Protecting Canadians from Online Crime Act (2015)**: Also known as Bill C-13, this law criminalizes the non-consensual distribution of intimate images and empowers courts to order the removal of such content.
- **Criminal Code Provisions**: Sections addressing harassment, defamatory libel, and uttering threats are applicable to online conduct.
- **Provincial Initiatives**: Provinces like Nova Scotia have enacted specific laws targeting cyberbullying, mandating educational programs and providing support for victims.

2.4 Australia

Australia addresses cyberbullying through both federal and state laws:

- **Criminal Code Act 1995**: Contains provisions against using a carriage service to menace, harass, or cause offense.
- **Enhancing Online Safety Act 2015**: Established the eSafety Commissioner, who has the authority to investigate complaints about cyberbullying and can issue takedown notices to social media platforms.
- **State Laws**: Various states have enacted laws that criminalize stalking and harassment, which can encompass online behaviors.

2.5 European Union

The European Union (EU) promotes a coordinated approach among member states:

- **General Data Protection Regulation (GDPR)**: Provides individuals with rights over their personal data, which can be invoked in cases of online harassment involving personal information.
- **EU Strategy on the Rights of the Child (2021-2024)**: Includes measures to protect children from cyberbullying, emphasizing the role of digital education and online safety.
- **Member State Legislation**: Countries like France and Germany have specific laws criminalizing online harassment, with penalties ranging from fines to imprisonment.

2.6 China

China addresses cyberbullying through broader cybercrime laws:

- **Cybersecurity Law (2017)**: Mandates network operators to prevent and stop the transmission of illegal information, which can include cyberbullying content.
- **Criminal Law Amendments**: Certain amendments criminalize online defamation and

the spread of false information, which can be applied to cyberbullying cases.

- **Enforcement Mechanisms**: The government exercises strict control over online content, and platforms are required to monitor and remove harmful content proactively.

2.7 United Arab Emirates (UAE)

The UAE has enacted laws to combat cyberbullying and online harassment:

- **Cybercrime Law (Federal Decree-Law No. 5 of 2012)**: Criminalizes acts such as online threats, defamation, and invasion of privacy.
- **Penalties**: Offenders can face imprisonment and substantial fines, with stricter penalties for offenses involving minors or public officials.
- **Preventive Measures**: The government conducts awareness campaigns and has established cybercrime units to handle complaints.

2.8 Comparative Analysis

A comparative analysis reveals both commonalities and differences in international approaches:

- **Commonalities**: ₀ Recognition of cyberbullying as a serious issue requiring legal intervention.
    - Utilization of existing criminal laws to address online harassment.
    - Implementation of educational programs to raise awareness.
- **Differences**:
    - Divergence in penalties and enforcement mechanisms
    - Variations in definitions and scope of cyberbullying across jurisdictions.
    - Differences in the role and responsibilities assigned to online platforms.

Cyberbullying and online harassment transcend national boundaries, emerging as transnational issues that flourish within the interconnected global digital landscape. Consequently, numerous countries have implemented specific legislation and preventive strategies to combat these challenges, with these international legal advancements serving as vital references for the development of cyber law in India.

In the United States, the legal framework addressing cyberbullying is decentralized yet comprehensive. At least 48 states have enacted laws specifically targeting cyberbullying, many of which are incorporated into school policies. This integration allows educational authorities to intervene in online incidents occurring off-campus that disrupt the school environment. A significant case that influenced this legal landscape is that of Tyler Clementi, a college freshman who tragically took his own life following cyber harassment. His case prompted the creation of the Tyler Clementi Higher Education Anti-Harassment Act, underscoring the importance of federal legislation in promoting digital accountability within educational institutions. While the U.S. Constitution prioritizes freedom of speech, courts have sought to strike a balance by criminalizing threatening speech, online stalking, and image-based abuse—areas that Indian courts are just beginning to investigate under Article 19(2).

Conversely, the United Kingdom employs a more centralized and proactive legal approach. The Malicious Communications Act of 1988 and the Communications Act of 2003 make it illegal to send electronic communications that are threatening, offensive, or distressing. In 2021, the UK introduced the Online Safety Bill, which establishes a "duty of care" for social media platforms, requiring them to eliminate harmful content or face substantial penalties. This legislative framework emphasizes accountability for platforms, a strategy that India has started to adopt through its IT Rules of 2021, albeit without a robust independent regulator akin to the UK's Ofcom.

Throughout the European Union, the General Data Protection Regulation (GDPR) serves a crucial function in preventing the misuse of personal data, a common factor in online harassment. Additionally, the Digital Services Act (DSA), which was implemented in 2024, introduces new regulations for online platforms concerning content moderation, algorithm transparency, and the swift removal of harmful material. These regulatory frameworks are fundamentally supported by the European Convention on Human Rights, which seeks to balance the right to privacy with the freedom of expression. In contrast, India’s Digital Personal

Data Protection Act of 2023 reflects some terminology from the GDPR but falls short in providing enforceable rights or a robust data protection authority, leading to concerns about its implementation and the availability of justice.

In Australia, laws addressing cyberbullying are enforced through a mix of federal and state regulations. The Enhancing Online Safety Act of 2015 resulted in the creation of the e-safety

Commissioner, the first independent regulatory body of its kind globally, which possesses the authority to remove harmful content, respond quickly to incidents, and support victims. Their

Cyberbullying Scheme allows minors or their parents to directly contact the commissioner's office, which collaborates with online platforms to ensure content removal within 24 hours.

Australia's approach, which emphasizes direct assistance for victims, educational resources, and legal options, is recognized as one of the most comprehensive and sensitive frameworks in the world. This model presents a valuable example for India, illustrating how a centralized cyber oversight body could enhance the effectiveness of the judiciary and law enforcement.

When comparing international benchmarks to India's framework for addressing cyberbullying, several deficiencies become apparent. Although India has implemented measures such as establishing intermediary guidelines, revising the IT Act, and advancing digital literacy initiatives like Digital India, it still lacks specific legislation targeting cyberbullying, a centralized regulatory body, and a publicly accessible grievance redressal mechanism similar to those found in Western democracies. Furthermore, India's approach tends to be more punitive rather than preventive, with insufficient emphasis on rehabilitation, counselling, or training in digital citizenship.

Nevertheless, India is increasingly collaborating with countries such as the U.S., Australia, and Japan on bilateral cybercrime initiatives, exchanging knowledge in areas like digital forensics, cloud evidence collection, and cyber threat intelligence. Additionally, India's involvement in forums like the G20 Digital Economy Working Group indicates its growing alignment with global standards in digital governance. However, to establish itself as a global leader in online safety, India must convert these discussions into domestic legislation, particularly laws aimed at safeguarding women, children, and LGBTQ+ individuals from online harassment.

In summary, international legal frameworks concerning cyberbullying provide India with both warnings and successful models. Nations that have adopted comprehensive strategies—combining legal enforcement, accountability for platforms, education, and support for victims— are significantly more effective in combating digital abuse. India must transcend its fragmented legal landscape and leverage these global best practices to create a cohesive, inclusive, and enforceable legal framework suitable for the digital citizens of the 21st century.

Across the globe, nations have adapted to the rise of digital harassment by establishing legal frameworks that vary significantly in scope, execution, and enforcement. While cyberbullying is generally defined in a manner that allows for content removal, civil lawsuits, and criminal prosecution, distinct regional priorities and cultural considerations shape each nation's response.

India's response, in comparison, continues to evolve, and the country looks at these international models to inform its strategies and legislative goals.

In Canada, for instance, the Criminal Code of Canada criminalizes harassment and defamatory libel through provisions such as Section 264 (Criminal Harassment) and Section 372 (Defamatory Libel), which cover online communications as well. In 2014, Ontario's AntiCyberbullying Act became the first to allow victims of cyberbullying to seek restraining orders against perpetrators, a solution that has inspired discussions on implementing similar provisions in Indian law. Notably,

Canada's approach is unique in its integration of educational measures, with schools being legally mandated to develop anti-cyberbullying policies. India, on the other hand, has yet to integrate such mandates at the school level, and the concept of school-based legal intervention remains underdeveloped.

In New Zealand, the Harmful Digital Communications Act (2015) is a pioneering piece of legislation aimed specifically at cyberbullying. It empowers the Communications Tribunal to issue orders for the removal of harmful digital content and offers victims a civil remedy for compensation. This legislation is a fine example of the public-private cooperation model, where internet service providers and platforms are compelled to remove harmful content promptly. New Zealand's system has been effective in curbing incidents of online harassment, but it also raises questions about freedom of expression versus privacy—concerns that India

must consider as it refines its regulatory mechanisms. Notably, Section 66A of the Information Technology Act, which was struck down in 2015, has been regarded as a failed attempt to regulate online speech too broadly, showing the delicate balancing act between regulation and freedom.

Cross-Border Legal Tensions and Jurisdictional Issues

A significant issue in combating cyberbullying is jurisdictional ambiguity, particularly when offenders operate across national borders. The extraterritorial application of laws becomes complex when the platform (such as Facebook or Instagram) is based in one country (e.g., the U.S.), but the victim resides in another (e.g., India). Unlike in physical crimes, where territorial boundaries are clearer, cybercrimes transcend these limitations, leading to frequent conflicts between domestic and international legal systems.

For instance, while the European Union's General Data Protection Regulation (GDPR) allows EU citizens to bring complaints against international companies, India lacks such a uniform extraterritorial data protection mechanism. Intermediary liability provisions under Section 79 of the IT Act require platforms to comply with Indian laws, yet these platforms are often based in jurisdictions where enforcement is weaker or unavailable. As a result, it remains a significant challenge to hold platforms accountable for harassment that originates from other countries. This discrepancy was particularly highlighted in the 2018 Supreme Court case of Shreya Singhal v. Union of India, which struck down Section 66A of the IT Act, emphasizing the need for clearer guidelines on platform responsibility and jurisdictional boundaries.

Moreover, global cooperation frameworks like the Budapest Convention on Cybercrime have encouraged member countries to collaborate on combating cyberbullying, but India's nonsignatory status limits its engagement with this mechanism. This leaves India in a precarious position when cyberbullying crosses into foreign jurisdictions, as there is no clear international procedure to address crimes that span multiple borders. The lack of an international standard for online harassment laws exacerbates the challenge for India in developing its legal approach.

United Nations' Efforts and Multilateral Cooperation

At the international level, organizations such as the United Nations and Interpol have worked

to establish broad frameworks to address the threat of online harassment and cyberbullying. The UN's Resolution A/RES/70/1 (Transforming Our World: The 2030 Agenda for Sustainable Development) calls for inclusive, peaceful societies and acknowledges the role of cybersecurity and online safety in creating such societies. The UN Human Rights Council has also recognized that online harassment undermines the right to privacy, freedom of expression, and equal participation in public life.

While the UN has issued guidelines, including UN Human Rights Council Resolution 29/16 (2015), which affirms the need to balance freedom of expression with the prevention of harm in the online space, these remain recommendatory rather than binding. As India continues to align its legal framework with international human rights norms, it can draw from these resolutions and frameworks to build stronger safeguards for digital safety and online freedom.

Role of International Treaties and Agreements

Countries with strong cross-border cooperation frameworks, such as the United States and European Union, have created mechanisms that directly impact how international digital harassment cases are handled. These agreements emphasize cross-border information sharing, the role of digital platforms in moderating content, and the protections for vulnerable users. For India, being **part of the G20 and BRICS nations opens up opportunities to engage in multilateral dialogues regarding global digital security, privacy rights, and harassment protections. These forums allow India to learn from international best practices, collaborate on drafting uniform cyber regulations, and ensure accountability for multinational tech companies operating within Indian borders.

The OECD (Organization for Economic Cooperation and Development) has also worked on drafting guidelines related to online safety and cybercrime, many of which India can incorporate into its policymaking. For example, the OECD Guidelines on Child Online Protection (2019) offer recommendations that can guide India in drafting a comprehensive child-specific cyberbullying policy, which is currently lacking.

International Enforcement Mechanisms and Global Jurisdictional Challenges

As cyberbullying and online harassment are inherently cross-border phenomena, they often involve offenders, victims, and platforms that operate in multiple jurisdictions, which can

create significant challenges in the enforcement of laws. The lack of global legal coherence has led to situations where victims in one country are left without legal recourse when the perpetrator operates in another country. In many cases, victims find themselves caught between conflicting national laws with varying standards for content removal, harassment definitions, and platform liability.

Case Example: Cross-Border Legal Conflicts

A noteworthy case that underscores the complexities of international jurisdiction in cyberbullying is the case of "Google v. Oracle" in the U.S., where issues of data protection and copyright infringement were brought to the forefront due to the international nature of the companies involved. In a similar context, if a person in India is harassed by a user based in the U.S. through platforms like Facebook or Instagram, Indian authorities may face difficulties in obtaining evidence or pursuing criminal charges due to the extraterritorial reach of U.S. law. The process of international mutual legal assistance (MLA) can be slow and cumbersome, and it often requires extensive diplomatic efforts to secure cooperation between jurisdictions.

The Role of Digital Platforms in Cross-Border Enforcement

Many social media platforms are global in nature, and as such, they face significant challenges in managing content moderation and responding to legal requests across various jurisdictions. For example, the Global Internet Forum to Counter Terrorism (GIFCT), a coalition of companies, government agencies, and international organizations, addresses harmful online content, including cyberbullying and online harassment, on a global scale. However, despite efforts to improve content moderation across borders, the lack of a global regulatory framework to hold platforms accountable for user-generated harassment remains a major gap.

Indian Perspective on Jurisdictional Issues

India’s Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 have made progress in regulating digital platforms, but they still face challenges in enforcing laws against cross-border harassment. Section 79 of the Information Technology Act (2000), which provides a safe harbor for intermediaries (such as social media platforms), has been criticized for being insufficient in holding platforms accountable for user-generated content. While the government has been pushing for stricter compliance measures and quicker

removal of harmful content, the jurisdictional reach of Indian law remains limited when offenders are located in countries with less stringent regulations.

To tackle these issues, India must push for global cooperation on cybercrimes, drawing on successful models such as the European Union's Digital Services Act (DSA), which requires platforms to take responsibility for the content they host. The Global Forum on Cyber Expertise (GFCE) and initiatives like the International Telecommunication Union (ITU) are also creating forums for global cooperation on these issues, but India's involvement in these discussions remains fragmented.

Global Standards and India's Alignment

While there is no single global convention on cyberbullying, several international bodies have developed soft law instruments—such as guidelines, frameworks, and resolutions—that India can incorporate into its domestic law. The OECD's Guidelines on Internet Policy provide a global standard for addressing harmful content online, encouraging member countries to introduce content moderation measures and stronger victim support systems. These guidelines align with the principles set out in the Universal Declaration of Human Rights, which emphasize the need for protection from harm without stifling freedom of speech.

The Role of Global Human Rights Bodies

At the global level, human rights organizations such as Human Rights Watch and Amnesty International have called for stronger regulations to curb online harassment and bullying, particularly against vulnerable groups such as women, children, and minority communities. These organizations have highlighted the need for global frameworks that protect digital rights while ensuring online safety. India, as a signatory to several UN treaties, including the Universal Declaration of Human Rights (UDHR), should take steps to align its national laws with international standards for online protection. Furthermore, India's National Human Rights Commission (NHRC) can collaborate with international bodies to ensure that online harassment laws are compatible with global human rights standards.

Challenges in Victim Access to Redress and Remedies

Another key issue in the international legal landscape is that victims of cyberbullying often face significant barriers in seeking legal redress, especially when the offenders are located in

other jurisdictions. The extraterritoriality of online harm means that victims might face delays in obtaining justice or limited access to support due to the complexity of international law enforcement. For instance, if an Indian citizen faces online harassment by a person in another country, they must go through the process of requesting legal cooperation under frameworks like Mutual Legal Assistance Treaties (MLATs) or extradition treaties, both of which are time consuming and not guaranteed to succeed.

In many instances, victims may not even be aware of the legal routes available to them, particularly when the harassment occurs on social media platforms or unregulated digital spaces. This lack of awareness is compounded by the complexity of international law, which varies between jurisdictions and may provide differing levels of protection. India's National Cyber Crime Reporting Portal (2020) is a step forward in allowing victims to report incidents of cyberbullying, but it is still limited in addressing cross-border cases, as the portal does not have the resources or international coordination mechanisms needed to tackle such offenses at a global level.

International Cooperation: Moving Towards a Global Framework

While there are varied national responses to cyberbullying, there is an increasing global consensus on the need for cooperative frameworks to address online harm. Bilateral and multilateral agreements, such as the Global Forum on Cyber Expertise (GFCE) and Interpol's Cybercrime Division, are leading efforts to facilitate cross-border cooperation in investigating and prosecuting cybercrimes, including online harassment. However, many of these efforts are still in their early stages and need greater coordination to be effective in the long term.

To advance the global fight against cyberbullying, India must continue to strengthen international partnerships, such as through its participation in the G20 and BRICS forums, which can help shape global digital policies and encourage greater cooperation on issues such as cybersecurity and victim protection. India can also look to international treaties and conventions—such as the Budapest Convention—as models to create a national cyberbullying law that complies with global digital governance standards while protecting the fundamental rights of its citizens.

3. Recommendations and Reforms

3.1 Enactment of Specific Cyberbullying Legislation:

- **Current Gap**: India lacks a dedicated law that specifically addresses cyberbullying. Existing provisions under the Information Technology Act, 2000, and the Indian Penal Code are often inadequate to tackle the nuanced forms of online harassment.

- **Recommendation**: Introduce comprehensive legislation that clearly defines cyberbullying, delineates various forms (e.g., doxing, trolling, cyberstalking), and prescribes proportionate penalties. This law should also outline procedures for swift redressal and victim protection mechanisms.

3.2 Strengthening Law Enforcement Capabilities:

- **Current Gap**: Law enforcement agencies often lack the technical expertise and resources to investigate and prosecute cyberbullying cases effectively.

- **Recommendation**: Establish specialized cybercrime units equipped with advanced forensic tools and trained personnel. Regular training programs should be conducted to keep officers abreast of evolving cyber threats and investigative techniques.

3.3 Enhancing Digital Literacy and Awareness:

- **Current Gap**: A significant portion of the population remains unaware of the legal remedies available against cyberbullying, leading to underreporting and prolonged victimization

- **Recommendation**: Implement nationwide digital literacy campaigns focusing on safe online practices, recognizing cyberbullying, and understanding legal rights. Educational institutions should integrate cyber safety modules into their curricula to sensitize students from an early age.

3.4 Promoting International Collaboration:

- **Current Gap**: Cyberbullying often transcends national boundaries, complicating jurisdiction and enforcement.

- **Recommendation**: Foster international cooperation through treaties and mutual legal assistance agreements to facilitate cross-border investigations and prosecutions. Participation in global forums can also aid in sharing best practices and harmonizing legal standards.

3.5 Encouraging Responsible Behaviour on Digital Platforms:

- **Current Gap**: Social media platforms sometimes lack robust mechanisms to prevent or address cyberbullying, and users may not be fully aware of the impact of their online behaviour.

- **Recommendation**: Encourage platforms to implement stringent community guidelines, employ AI-driven content moderation, and provide clear reporting channels. Additionally, public awareness campaigns should promote empathy and responsible digital conduct among users.

3.6 Establishing Support Systems for Victims:

- **Current Gap**: Victims of cyberbullying often face psychological trauma and may lack access to counselling or legal assistance.

- **Recommendation**: Create dedicated support centres offering psychological counselling, legal aid, and guidance on navigating reporting mechanisms. Collaborations with NGOs and mental health professionals can enhance the support network for victims.

To effectively combat cyberbullying and online harassment in India, a multi-pronged approach involving legislative reform, policy innovation, technological intervention, and societal transformation is urgently needed. Firstly, the current legal framework under the Information Technology Act, 2000 and sections of the Indian Penal Code is fragmented and outdated in addressing the sophisticated nature of digital abuse. A comprehensive, standalone Cyber Harassment Prevention Law, modelled on global best practices like the UK's Online Safety Act (2023) or Australia's Online Safety Act (2021), could offer clarity, procedural ease, and stronger victim protection. Such legislation should include clear definitions of cyberbullying, doxxing, morphing, deepfake creation, revenge porn, and online stalking — areas often

underregulated or misunderstood in current jurisprudence.

Furthermore, procedural reforms are crucial to make law enforcement more responsive and sensitive. Police officers, particularly in rural or semi-urban areas, often lack the technical training or gender sensitivity required to handle digital harassment cases effectively. Regular capacity building workshops, integrated with human rights and digital forensics training, should be institutionalized through agencies like the Bureau of Police Research and Development (BPRD). The creation of special cyber response units at the district level with a dedicated female officer could also improve accessibility and trust, especially for women and LGBTQ+ victims.

On the preventive side, school and university curricula must integrate digital citizenship education, emphasizing online behaviour, consent, emotional intelligence, and cyber laws.

Programs like Cyber Smart Schools initiated in Delhi, and Maharashtra's Digital Literacy Mission, serve as effective prototypes. These need to be scaled nationwide with collaboration from the Ministry of Education and state education boards. In addition, higher education institutions must establish cyber grievance redressal cells, much like anti-ragging or POSH (Prevention of Sexual Harassment) cells, to ensure timely and discreet handling of digital complaints.

Technology companies and social media platforms must also be held accountable through stronger enforcement of platform-level regulations. Amendments to India's Intermediary Guidelines (2021) should require platforms to provide clearer, faster, and more victim-cantered complaint redressal mechanisms. Appointing resident grievance officers, maintaining transparent takedown policies, and offering tools for content moderation and user blocking are essential reforms that need better oversight by the Ministry of Electronics and Information Technology (MeitY). Penalties for non-compliance, such as those proposed in the Digital India Bill (Draft 2023), should be implemented with seriousness to deter platform negligence.

Moreover, India must prioritize the mental health dimension of online harassment. Victims often suffer from depression, PTSD, or social withdrawal, but legal mechanisms rarely address the psychological aftermath. Establishing state-funded cyber trauma helplines, in collaboration with mental health organizations like NIMHANS and Power, can offer immediate

psychological first aid. Schools and colleges should also partner with psychologists to conduct regular workshops on coping strategies and online self-care.

Another necessary reform is the adoption of data privacy laws that better safeguard users' personal information from exploitation and misuse. India's newly passed Digital Personal Data Protection Act, 2023, while a step forward, needs tighter enforcement to prevent the sale or leakage of sensitive data that fuels doxxing or identity-based harassment. Provisions for "right to be forgotten" and "right to withdraw consent" should be practically implementable for survivors who wish to erase harmful traces of abuse online.

Finally, India should establish a centralized cybercrime reporting dashboard with multilingual interfaces, streamlined FIR filing, and real-time tracking of complaints — much like the Cybercrime Reporting Portal (cybercrime.gov.in), which exists but is under-utilized due to lack of awareness and complex navigation. A mobile app version, integrated with AI-based chat support and quick legal aid access, can dramatically improve reporting rates, especially for tech-challenged or rural populations.

In essence, the reform agenda must move beyond punitive legalism to a victim-cantered, digitally literate, and empathetic cyber ecosystem. Legal reforms, when aligned with educational initiatives, tech accountability, mental health support, and community resilience, can create a robust framework capable of addressing the evolving challenges of cyberbullying in India.

An urgent reform area in India is the harmonization of cyber laws across central and state jurisdictions. Due to federal legislative structures, cybercrime cases often face delays because of confusion between state police authority and central law provisions. A clear division of cyber jurisdiction, along with the empowerment of state-level cyber regulatory bodies, can streamline complaint registration, investigation, and prosecution. States like Telangana, Maharashtra, and Kerala have already developed Cyber Security Policies tailored to their local needs — these should be emulated nationwide with a standard compliance matrix from the Ministry of Home Affairs.

Another critical recommendation involves empowering the judiciary with digital literacy and cyber law specialization. Most judicial officers, especially at the district level, lack specific training in understanding evolving cybercrimes like virtual blackmail, digital extortion,

deepfakes, or cyber-flashing. Establishing Judicial Academies with specialized modules on cyber jurisprudence, and assigning dedicated cyber benches in High Courts, would ensure speedy and knowledgeable adjudication. A fast-track cyber court system for cases involving online harassment — similar to the Fast-Track Special Courts (FTSCs) under POCSO and rape cases — could drastically reduce pendency and improve victim confidence in the legal system.

Additionally, India must focus on inclusive reforms, especially considering the disproportionate impact of online harassment on minorities, Dalits, LGBTQ+ individuals, and people with disabilities. Policies should require inclusive language in online safety tools, regional dialect support in cyber complaint platforms, and representation from marginalized groups in digital policy consultation panels. This ensures that reforms do not follow a one-sizefits-all model but respect intersectionality — a concept strongly supported by research from The Internet Democracy Project and Point of View (POV India).

On the technical reform front, the government must incentivize the development of indigenous AI moderation tools that reflect Indian sociolinguistic and cultural contexts. Imported algorithms used by global platforms often fail to detect harassment in Hindi, Tamil, Bengali, or mixed-language text, allowing abusive content to circulate unchecked. Research grants to IITs, IIITs, and AI startups can spur the creation of contextualized content flagging systems. These tools could be mandated via MeitY's policy framework as part of the Responsible AI in India initiative. There's also scope for a structured whistleblower protection mechanism for content moderators and ethical hackers who help report abusive accounts, child exploitation content, or coordinated harassment networks. These individuals often face backlash from tech platforms or online mobs and deserve legal and institutional backing similar to anti-corruption whistleblowers.

Beyond individual solutions, macro-level reforms such as including cyberbullying metrics in the National Crime Records Bureau (NCRB) annual reports can help shape future policy. As of 2022,

NCRB reports still aggregate many forms of cyber violence under vague categories like "others." A disaggregated dataset for cyberstalking, impersonation, and online sexual harassment — along with gender and age-wise breakdowns — would provide data-driven insights for reform.

Finally, India needs to champion digital rights in its foreign policy. By participating more actively in global forums like the Internet Governance Forum (IGF), Freedom Online Coalition, and UNESCO's Internet for Trust initiative, India can shape international norms while also benefiting from best practices. This can include cross-border data sharing agreements to tackle transnational cyber harassment — a growing issue due to social media's global nature.

Strengthening the Role of Civil Society Organizations (CSOs) and NGOs

One of the most significant, yet underutilized, reforms for tackling cyberbullying and online harassment in India is the active involvement of Civil Society Organizations (CSOs). These organizations can play a pivotal role in both preventive and post-incident recovery phases by organizing awareness campaigns, peer support networks, and community outreach programs. Well-established organizations like The Digital Empowerment Foundation (DEF), Sambodhi, and Breakthrough India are already working on ground-level interventions that equip individuals with digital literacy and mental health support. However, a formalized partnership model between the government and these organizations should be established, which would allow for joint projects in cyber education, training for online safety, and victim empowerment.

Moreover, community-led activism can go a long way in shifting the public perception around online harassment. Large-scale campaigns led by CSOs could take advantage of India's strong social media presence, particularly leveraging platforms like WhatsApp and Instagram to engage youth in conversations about safe online spaces and reporting channels. The #SheThePeople campaign, which advocates for women's digital safety, is an example of how collective social media movements can influence policy discussions and media narratives.

Technological Advancements in Cyber Safety

The role of emerging technologies, such as Artificial Intelligence (AI), machine learning (ML), and natural language processing (NLP), is pivotal in shaping the future of digital safety in India. AI-based solutions could be used to automatically detect and flag abusive content, including hate speech, cyberstalking, and explicit material, even in regional languages. These technologies could be further enhanced by integrating emotion recognition algorithms that can identify distress signals from victims who may not explicitly mention harassment but display other psychological signs.

One promising initiative is Google's Jigsaw, which uses AI to detect harmful content in real time. India could partner with tech giants like Google, Microsoft, and Amazon to scale these solutions specifically for local languages, cultural contexts, and harassment patterns. AI-based monitoring systems can be deployed to provide instant alerts to both users and platforms when harmful behaviour is detected, significantly improving the timeliness of intervention.

Moreover, integrating blockchain technology to ensure privacy and anonymity for cyberbullying victims could offer victims more control over their data while ensuring their safety. A blockchainbased incident registry could securely store abuse-related information and allow victims to have access to verifiable records, should they decide to take legal action in the future.

Public Education Campaigns on Digital Literacy and Safety

It is essential to move beyond school-based digital education and launch nationwide public awareness campaigns. Research indicates that many young people, especially in India's smaller towns and rural areas, are unaware of the severity of online harassment or their rights in the digital world. For instance, a study by the Centre for Internet & Society (CIS) found that nearly 40% of youth in smaller towns are unaware of how to report harassment on social media platforms. To bridge this gap, the government should collaborate with television channels, mobile service providers, and popular influencers to disseminate educational content about cyber safety, digital ethics, and reporting mechanisms.

Programs like the Digital Shakti initiative should be expanded to include offline workshops and mobile app interventions that provide real-time guidance on navigating digital safety. These programs must also include gender-sensitive content, particularly for women and children, who remain the primary targets of online harassment in India.

Specialized Helplines and Support Systems for Victims

Currently, there is a lack of comprehensive helplines that are equipped to deal with the psychological trauma and legal guidance that victims of cyberbullying face. While the National Helpline for Cybercrimes (155260) is an important step, it lacks immediate psychological counselling services, which are essential in addressing the emotional consequences of online abuse. Establishing a nationwide cyberbullying-specific helpline, available in multiple

languages, could provide immediate emotional and legal support. This helpline could serve as a first point of contact, offering confidentiality and legal advice, as well as mental health counselling for victims.

Additionally, creating community centres for online harassment victims in both urban and rural areas could provide face-to-face support, where individuals can safely report incidents and access necessary resources like mental health services and digital privacy advice.

Fostering Digital Empowerment Through Youth Participation

It is crucial to foster youth-driven movements that advocate for cyber rights and online safety. Young people are often the most vulnerable to online harassment but are also best positioned to lead initiatives on cyber self-defence, safe internet practices, and digital wellness. The Indian government can encourage youth-led cybersecurity camps, competitions, and ambassador programs to raise awareness. Programs such as TechGirls India, which targets young women to become future leaders in the tech and cybersecurity space, could be expanded to include selfdefence digital tactics — such as blocking abusive users, protecting online privacy, and counteracting hate speech.

Incorporating digital wellness and online etiquette modules in high school and college curriculums will equip the next generation with the skills to navigate online spaces safely and responsibly. Students can be trained as peer educators who share their knowledge with others, fostering a digital community of support.

International Collaboration for Cross-Border Data Protection

As cyberbullying and online harassment often occur across borders, international cooperation becomes crucial. India must play an active role in shaping global cyber standards, particularly in the G20 and United Nations forums, by promoting comprehensive cross-border data protection agreements. Such agreements would create frameworks to handle cases of international harassment, online defamation, and revenge porn that might involve platforms operating in multiple countries.

India should also collaborate with international organizations such as INTERPOL to ensure crossborder cybercrime tracking and victim protection, ensuring that perpetrators cannot escape accountability by simply operating from other jurisdictions.

Incentivizing Corporations to Build Safer Online Ecosystems

Lastly, an essential recommendation is to incentivize tech companies to design safer online spaces through corporate social responsibility (CSR) initiatives. The government should offer tax benefits or other rewards to companies that implement robust anti-harassment policies, enhance platform security, and regularly engage with users about online etiquette and safe conduct. Social media giants should be required to regularly audit their policies, user reports, and harassment prevention measures, ensuring they are effective in addressing the unique issues faced by Indian internet users.