VIOLATION OF CHILD RIGHTS IN THE DIGITAL ERA WITH SPECIAL REFERENCE TO CYBER CRIMES

Aapthi Srivatsa* **Khushi Suresh***

ABSTRACT

Children represent the group that consumes technology at the highest rates during the present time. Children experience unprecedented life changes through the digital era because it gives them complete access to education, together with entertainment and social possibilities. Multiple positive aspects exist during the digital wave, yet the rights and safety of children remain endangered through digital risks. Adults acknowledge that children understand technology well, yet they remain among the most susceptible groups. Financial fraud, together with cyber bullying, online grooming, identity theft, and exposure to pornography, represent the principal forms of cyber abuse that children encounter while using computers. Children without the necessary digital literacy experience have increased exposure to digital risks because of their insufficient skills. Children frequently expose personal details while using the internet through unsafe behaviours, which puts them at risk for cybercriminal attacks. Children from different economic backgrounds experience increased social and educational gaps since they lack digital resources, which intensifies their disadvantage in the modern world. Youngsters who suffer from these crimes develop trust problems as well as anxiety and depression, affecting both their academic work and social relationships. Stigmatization from such incidents leads children to shun reporting their experiences. When individuals create false online profiles to fabricate attacks or humiliation against children, it leads to enduring emotional damage during their development. The term "sharenting" now identifies parent behaviour of sharing child content online and represents a major violation of child rights. The practice of sharenting, which parents undertake with pure motives, actually makes children more susceptible to dangerous internet crimes such as stalking and exploitation. Criminals can use minimal details posted by parents to discover and reach out to children. The priority must

*BBA LLB (HONS), SECOND YEAR, PES UNIVERSITY.
*BBA LLB (HONS), SECOND YEAR, PES UNIVERSITY.

be the development of digital literacy knowledge between children and their guardians. Maintaining child safety on the internet demands a common effort that protects both their digital rights and their welfare throughout the digital age.

Keywords: Children, Sharenting, Digital Literacy, Cyberbullying, Online Grooming.

INTRODUCTION

Online platforms feed cyberbullying, which presents itself as a widespread digital threat in the digital age by targeting weak individuals, especially children and adolescents. The harassment method systematically breaks through physical limits by using technology to spread intimidation and humiliation while causing psychological suffering. Cyberbullying functions in an anonymous environment, which gives bullies more confidence to harm people and persevere through digital records, which expand the network and make harassment last indefinitely. Several forms of cyberbullying exist since digital interactions present numerous targets that bullies can use for their purposes. The practice of impersonation targets victim' identities by establishing bogus accounts or taking control of their profiles for harmful communications, whereas cyberstalking represents constant supervision and dangerous tendencies that create threats to physical safety. Abusers maintain their harassment campaign by sending nonstop messages filled with threatening or demeaning language to strip a victim of their self-worth. Doxing and outing consist of unauthorized disclosure of private data, such as personal dialogues and sensitive content and photographs, to harm victims in public scenarios.

Some types of cyberbullying develop gradually when attackers establish false trust to obtain private information that later becomes weaponized online and when perpetrators actively remove people from their digital peer groups. When disputes escalate through flaming, users engage in brutal arguments that consist of offensive language and insults, after which trolling occurs as perpetrators use inflammatory statements to trigger emotional responses. The actions of dissing and fraping involve spreading damaging rumours and hacking social media accounts to create offensive posts, respectively. The creation of fake online profiles through catfishing makes it difficult to trust others because people fabricate identities to obtain emotional connections or steal money. Such behaviours result in severe psychological damage to victims. People who experience cyber-attacks feel anxiety and depression alongside social withdrawal when they worry that abusive information will remain available forever. Children become more

vulnerable because inadequate knowledge about privacy protection leaves them exposed through digital inequality. Educational institutions, along with parents, face opposite needs of preserving digital connections while creating security measures to protect young users from dangerous online threats. The solution to cyberbullying requires collaboration between several initiatives that incorporate digital education with caring online habits and reliable protection systems. The development of technology requires corresponding improvements in prevention methods for its misuse to establish digital spaces where all users feel safe and included. All users must actively work together to create respectful online relationships because this approach effectively prevents our present-day digital problems.

ANALYSIS OF THE EXISTING LEGAL FRAMEWORK

The advancement of child digital rights protection evolved substantially because of essential legal decisions and parliamentary legislative changes. These laws have been better defined through recent developments, which provided clarity about their application throughout different territories. In September 2024, the Supreme Court of India delivered a pivotal judgment in the case of Just Rights for Children Alliance v S. Harish.[1], expanding the interpretation of Section 67B of the IT Act and Section 15 of POCSO. The Court ruled that merely viewing, storing, or possessing child sexual abuse material constitutes an offense, overturning the Madras High Court's narrower interpretation. This decision established that Section 67B comprehensively criminalizes not only electronic dissemination but also the creation, possession, and consumption of such material. The UK's Online Safety Act 2023[2] has introduced stringent enforcement mechanisms, with Ofcom(The Office of Communication)[3] Gaining powers to impose fines up to £18 million or 10% of annual turnover on platforms failing to protect minors. The Act requires platforms to implement safety measures by March 2025, including senior accountability protocols and enhanced content moderation systems. Notably, the Act extends globally to services with significant UK users or those targeting UK audiences.

The European Court of Justice (CJEU) has refined the interpretation of the GDPR's compensation framework through several 2023-2024 judgments. In the VB case[4], the Court established that fear of potential data misuse alone doesn't warrant compensation without

[1] Just Rights for Children Alliance v. S. Harish, 2024 INSC 716 (India).
[2] Online Safety Act 2023.
[3] UK Online Safety Act: Enforcement Framework, OFCOM (Oct. 17, 2024).
[4] VB v. Natsionalna agentsia za prihodite, Case C-340/21.

demonstrable harm. This ruling particularly impacts how platforms must handle children's data breaches, requiring evidence of actual damage rather than speculative harm. COPPA (Children's Online Privacy Protection Act)[5] enforcement in the US has intensified, with maximum penalties increasing to $50,120 per violation. Recent cases demonstrate stricter application, such as the enforcement action against major toy companies, including Viacom, Mattel, and Hasbro, for allowing advertising partners to track children's online activities without parental consent[6]. India's Digital Personal Data Protection Act 2023[7] has introduced substantial penalties up to ₹250 crore for breaches involving children's data. The Act mandates data fiduciaries to implement specific safeguards for processing children's information, though implementation timelines remain pending. A significant development is the requirement for verifiable parental consent, addressing a critical gap in previous legislation.

The Kerala High Court's 2024 ruling[8] The accidental downloading of prohibited content has added nuance to enforcement, holding that unintentional possession requires evidence of specific intent for prosecution. This decision highlights the complexity of applying traditional legal frameworks to digital behaviours, particularly regarding minors' online activities. Recent cases have also addressed the intersection of privacy rights and platform accountability. The GP v Juris GmbH case[9] Before the CJEU established that multiple GDPR violations from a single processing activity cannot be "double-counted" for compensation, affecting how platforms must structure their child protection measures. The protection of digital rights progressed from basic prohibitions to complete defensive strategies, which combine preventative measures under strict responsibility systems.

INITIATIVES BY THE GOVERNMENT

The digital revolution in India has brought 830 million internet users online, including 250 million children and adolescents. While this connectivity offers unprecedented opportunities, it has also exposed young users to cyberbullying—a menace affecting 33% of Indian children, the highest rate globally, according to McAfee (2024)[10]. India's legal and institutional response

[5] Children's Online Privacy Protection Act.
[6] In re Viacom, Inc., Mattel, Inc., Hasbro Inc., & JumpStart Games, Inc., No. 16-CV-1-1 (N.Y. Att'y Gen. Sept. 13, 2016).
[7] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
[8] Sebin Thomas v. State of Kerala, CRL.REV.PET NO. 610 OF 2024 (Kerala H.C. June 19, 2024).
[9] GP v. juris GmbH, Case C-741/21.
[10] Maria Giulia Conti et al., Sharenting: Characteristics and Awareness of Parents Publishing Sensitive Content of Their Children on Online Platforms, 50 Ital. J. Pediatr. 135 (2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC11290302/.

has evolved significantly since 2020, blending legislative reforms, judicial interpretations, and grassroots initiatives. However, persistent gaps in enforcement, digital literacy, and platform accountability continue to challenge progress. The Indian approach to cyberbullying employs various laws instead of creating one unified cyberbullying statute.

Information Technology Act, 2000 (IT Act)[11]:

- Section 67: A person faces imprisonment of up to three years for sending obscene materials.
- Section 67B: Targets child sexual abuse material (5+ years imprisonment).
- Section 66E: penalizes acts of privacy violation, which include the unauthorized sharing of images.

The Supreme Court eliminated Section 66A through its verdict in Shreya Singhal v. Union of India (2015)[12] Due to its restrictions on offensive message regulation. Free speech suffered a blow from the Union of India's (2015) decision to strike down Section 66A, but the Digital Personal Data Protection Act 2023, Now imposes heavy penalties reaching ₹250 crore for the improper handling of children's data and requires documented consent from parents.

Indian Penal Code (IPC)[13]:

- Section 354D (Cyberstalking):3 years' imprisonment.
- Section 509 (Insulting Modesty): This covers gender-based harassment.
- Section 507 (Anonymous Threats): Addresses intimidation via fake profiles.

POCSO Act, 2012[14]: Criminalizes online sexual harassment of minors, with mandatory reporting obligations for platforms.

Bharatiya Nyaya Sanhita, 2023[15]: Introduces Section 73 on image-based abuse, explicitly criminalizing nonconsensual sharing of intimate content. The government has also brought about multiple institutional mechanisms-

[11] Information Technology Act, No. 21 of 2000.
[12] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[13] Indian Penal Code, No. 45 of 1860, § 354D (India)
[14] Protection of Children from Sexual Offences Act, No. 32 of 2012, § 11 (India).
[15] Bharatiya Nyaya Sanhita, § 73 (2023) (India).

National Cyber Crime Reporting Portal (2019): Facilitates anonymous reporting, with 50,035 cybercrime cases registered in 2020 alone. However, only 15% result in convictions due to jurisdictional complexities and evidence preservation challenges.

Cyber Crime Cells[16]: Established in 28 states, these units focus on child exploitation cases. Bengaluru's cell reported a 45% increase in cyberbullying complaints in 2023, driven by gaming platforms and Instagram.

School Initiatives:[17] NCERT mandates cyber safety modules in curricula, while states like Kerala conduct workshops on reporting mechanisms. Yet, only 30% of educators are trained to handle such cases.

India's response to cyberbullying represents a complex interplay of legislative measures, institutional mechanisms, and educational initiatives. While the legal framework demonstrates comprehensiveness through multiple statutes—from the IT Act to POCSO and the recent Bharatiya Nyaya Sanhita—significant implementation challenges persist. The low conviction rate at 15% occurs as case numbers increase, which demonstrates the difference between established law and actual implementation practices. India is required to move beyond legislative expansion as the country advances its digital transformation by focusing on effective implementation through capacity building, technology modernization, and public awareness drives. A comprehensive methodology that targets internet user safety will allow India to establish secure digital spaces for its 830 million users while focusing especially on protecting its young people.

DIGITAL RIGHTS VIOLATION

The landscape of digital rights violations against children has become increasingly complex and concerning.

Digital space provides cybercriminals with opportunities to victimize children by stealing their identities and engaging in grooming and illegally sharing their images. Cyber groomers begin their operations by choosing victims from vulnerable clusters of accessible children who frequently operate on social media networks and communication applications. Recent

[16] National Crime Records Bureau, Crime in India 2020 (2021).
[17] Manpreet Kaur & Munish Saini, Indian Government Initiatives on Cyberbullying: A Case Study on Cyberbullying in Indian Higher Education Institutions, 28 Educ. Info. Technol. 581 (2023).

information from the National Crime Record Bureau shows a concerning 32% increase in online attacks on children in India, giving rise to 1,823 recorded cases in 2022. The personal data of children experiences abuse through digital pornography along with obscene material distribution and cyberstalking and bullying incidents. The problem becomes worse because India has a distinct digital environment containing 82% of kids who share devices, which considerably raises their risk of encountering objectionable content.

Prosecuting digital offenders becomes extremely difficult because the criminals tend to use international networks as their operating arena. The virtual nature of modern offenses produces substantial difficulties for determining jurisdiction because cyberspace has no fixed geographic limits. The pursuit of cybercriminals across international borders becomes fruitless and challenging because of various legal framework conflicts between countries. India has encountered various obstacles while using the Digital Personal Data Protection Rules to resolve these problems. The rules' reliance on digital lockers and government IDs for parental consent verification has proven vulnerable to misuse. Three main barriers prevent the effective implementation of protective measures because fewer than thirty percent of children, thirty-five percent of parents, and twenty-six percent of educators have any awareness of digital safety protocols.

The rural population faces a critical situation because digital literacy levels remain low, and it becomes difficult to monitor individual child device use due to shared equipment. The digital divide and insufficient awareness and enforcement systems combine to create an ideal environment for children to face growing risks of online abuse while they are unprotected. Digital literacy protections for children need consistent collaboration between parents and educational centres, together with technology companies, to match the current online landscape changes. Educational institutions must prioritize two essential legal commitments, which include digital literacy training and online safety assurance for their students. Schools need to establish complete digital literacy initiatives with technology used throughout every academic subject and effective protection measures. Locally and internationally implemented guidelines require schools to define technical regulations for devices while supporting content filters alongside protective measures for student informational assets. Scholarly institutions must follow policies like COPPA and equivalent regulations to implement educational application

and website usage by securing parental consent for student information obtained from children under 13.[18]

Research in the digital era demonstrates that parents' responsibility for monitoring their children creates substantial effects on their online protection against harm. Parents need to supervise their children online while setting proper age-based rules and talking frequently about internet activity. Studies confirm that children avoid potential threats both when parents do actual supervision and when they simply share the same room during online time. When children are younger than 13, parents require authorization from the perspective of data processing laws and must proactively handle the digital activities of their children. Minors receive protection from technology platforms through the integration of legal binding requirements and additional non-compulsory security features. Different regulatory requirements demand platform operators to develop design features that consider user age alongside comprehensive moderation systems and detailed privacy information meant for this demographic. The platforms are bound to supply parent-monitoring functionalities while developing age-verifying structures and adopting rigorous data security procedures. The platforms need to maintain complete transparency regarding their data procedures while establishing specific procedures to report improper activities and content. The Online Safety Act of the UK, along with similar global legislation, has enhanced the responsibility of platforms.

These platforms must maintain complete accountability for young user protection by doing proactive risk assessments and applying safety-by-design as design principles. Success in safeguarding children online depends on a faultless interconnection between educational institutions, parents, and technology platforms that establishes a complete system of protection for young users in digital spaces. An alliance between different parties protects children by allowing them to benefit from digital technology while maintaining their security from possible harms.

SHARENTING AS A GROWING TREND ON SOCIAL MEDIA PLATFORMS

Sharenting describes the blended practice of sharing content with the characteristics of parenting. Parents have adopted the practice of using social media to depict their children in pictures beginning from their ultrasound images and continuing until their first day of school.

[18] Supra 5

Before their first birthday, most children in the modern generation have already established an online digital presence. There are plenty of virtual communities presently, and we can find a plethora of videos, pictures, and posts depicting the lives of children, which are documented by their parents. Internet-based information maintains its ability to survive indefinitely after information value expires, which means child confessions can persist forever. People from Generation Z frequently create online records and blog updates about their children while also seeking social feedback through audience reactions. Through these interactions with unfamiliar people, the parents receive feedback, which serves as their validation to continue posting content online. Liking, sharing, or commenting creates positive outcomes that lead parents to post additional content. Fostering audience demand for kid-related content eventually causes parents to post underage information while seeking social confirmation, which results in the loss of their children's privacy.

National Health Institute's data shows that sharing practices by parents have increased since parents post childhood photos and videos in 74.4% of cases but hide children's faces or bodies in 24% of posts as a privacy measure.[19] The sharing of child-related content by parents through location tagging reaches 28.2% of users, creating identifiable risks to their children's privacy. The primary drivers for parental online sharing include daily documentation at 41% and showing off their child at 40%. Only three percent of parents use social media for professional sharenting activities, and just one percent generate financial income through their child-related posts. Parental content satisfaction mostly depends on social media interactions regarding children because 36% of parents strongly enjoy receiving likes along with other engagements on their child-related posts, while 17% experience moderate satisfaction and 21% only show minimal satisfaction. The emotional perception of sharenting differs between parents as 25% report no satisfaction while 36% and 17%, along with 21%, experience delighted and moderately satisfied and slightly satisfied reactions, respectively. Experts have validated the sense of connection parents gain through social media while they raise concerns about hazards that include identity theft, child exploitation, and cyberbullying.

Some parents are lulled into a false sense of security that the data they share about their children will not be seen beyond a select audience.[20] The research has shown that Facebook provides

[19] Maria Giulia Conti et al., *Sharenting: Characteristics and Awareness of Parents Publishing Sensitive Content of Their Children on Online Platforms*, Ital. J. Pediatr., July 30, 2024, at 50:135, https://pmc.ncbi.nlm.nih.gov/articles/PMC11290302/, doi: 10.1186/s13052-024-01704-y.
[20] Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 Emory L.J. 839 (2016).

another form of social behavior, closely related to voyeurism, and occurs due to the social control and the need for monitoring other users.[21]

LEGAL PERSPECTIVE

The legal systems of France, together with Illinois and India, follow different approaches to address privacy concerns through privacy rights regulations and financial compensation and data protection protocols.

France: The Right to Privacy and the "Right to Be Forgotten": As a protector of children's digital privacy, France maintains legal restrictions with great severity. Under the Children's Image Rights Law of 2024, minors gain legal authority to order their parents to remove online content like photos or videos from public. The "right to be forgotten" provision in Article 17 of GDPR matches the French legislative approach. The 2020 Child Influencer Law establishes regulations for child labor in online monetized content, which provides financial safeguards to children who create such content. The Commission Nationale de l'Informatique et des Libertés (CNIL), together with other French authorities, has the power to step in when parents deny requests from children to delete personal content, thus upholding the legal privileges of children regarding their data.

Illinois: Financial Protection for Child Influencers: Under Illinois law, the approach to sharenting focuses on financial issues when monetized content is involved. In 2024, Illinois established itself as the first U.S. state to pass legislation that offers monetary remuneration to children who appear online similar to child performers. Under Illinois law, parents are required to establish a trust fund when their child ends up featured in more than thirty percent of monetized content throughout thirty days. Under the new regulations, teenagers can obtain access to their stored income after their 18th birthday while possessing the right to file a complaint against their parents for uncollected funds. The new legislation adopts principles from the Coogan Law, which offers protection to Hollywood child performers. The Illinois law refrains from regulating non-monetary sharenting content yet acknowledges economic exploitation problems that arise when parents use their children as profitable assets online.

India: Data Protection but No Direct Sharenting Regulation: The Indian government established data protection standards instead of creating specific laws about sharing practices.

[21] Anna Brosch, *When the Child is Born into the Internet: Sharenting as a Growing Trend Among Parents on Facebook*, 43 TNER 1, 19 (2016), doi: 10.15804/tner.2016.43.1.19.

The Digital Personal Data Protection (DPDP) Act, 2023, demands guardian approval from parents for children under 18 and bans monitoring user behavior and toxic data handling of children. The DPDP Act lacks the same key provision as France regarding children's rights to request content deletion posted by parents. Indian laws shield children from corporate data misuse, yet they fail to address or provide a remedy for parental over-sharing activities when posting online and do not serve minors who want to erase their online presence. The Indian courts fail to recognize children's self-ownership of digital identity at the same level that France refers to their digital identity rights.

COMPARATIVE ANALYSIS AND FUTURE IMPLICATIONS

- French legislation grants children the right to delete their online posts with full respect for their privacy and independent choices.
- Under Illinois law, all earnings resulting from sharenting activities must be secured for child influencers who participate in this business.
- Indian privacy regulations emphasize protecting corporate data while refraining from establishing direct rules that regulate parental actions on the internet with their children.

The social media practice of Sharenting has developed as a phenomenon that gives children ways to connect with people yet puts their online privacy at risk. People use various purposes to share child-related content, including photo documentation and social media participation. Social media development demands worldwide legal systems to establish policies regarding child protection of privacy rights and permission grants while preventing exploitation. Future laws need to harmonize parental rights of internet self-expression with child online security measures so children can safely manage their digital identity data.

CYBERBULLYING: AN INDIAN PERSPECTIVE

India, a rapidly expanding nation in cyberspace, is witnessing an alarming surge in cybercrimes, including cyberbullying.[22] The high percentage of children facing online harassment in India establishes an unfortunate record as the country stands at 33%, whereby it maintains the leading position for internet harassment. The growing threat of cybercrimes proves that India requires urgent protective measures for both cybercrime prevention and

[22] M.V., Balamurugan G., Sevak S., et al., *Silent Screams: A Narrative Review of Cyberbullying Among Indian Adolescents*, 16(8) CUREUS e66292 (2024), https://doi.org/10.7759/cureus.66292.

internet safety. The National Crime Records Bureau reveals that cybercrimes in India have experienced significant growth.[23] A total of 50,035 cybercrime reports from 2020 consisted of 762 cyber blackmail cases together with 2,384 instances of cyber stalking, 84 defamation incidents, 247 fake profile cases, and 838 instances of fake news. The number of cybercrimes reported to authorities surged steadily throughout 2018 to 2019 and reached its highest extent in 2020 with 50,035 cases. The rising cybercrime figures call for urgent intervention measures to handle the crisis. One research study about cyberbullying identified public understanding regarding online harassment. Results illustrate how most individuals do not accept cyberbullying as natural to the digital environment. The majority of respondents (70%) disagreed with the belief that cyberbullying cannot be prevented, yet around 15% believed it is a typical part of online communication. The strong data shows disagreement with the idea of making cyberbullying acceptable while demonstrating the critical need to establish prevention methods.[24]

The causes behind cyberbullying targets remain unidentified to victims who become subject to harassment but do not know the root of their victimization. People most frequently cite physical appearance and religious beliefs as bullying reasons before reporting sexual orientation and racial background and disability discrimination. Research indicates that personal characteristics that exist from birth function as major factors that fuel online bullying targets. The research study demonstrated substantial distinctions between male and female experiences of cyberbullying and bystander activity, as well as cyber victimization during analysis. Female participants showcased the following different rates of cyberbullying experience: 51.30% had experienced it, while 11.30% were not sure, and 37.39% had no such experience. Research reveals that male participants experienced cyberbullying at a rate of 55.24%, whereas 14.24% were unsure and 30.48% did not face this type of bullying. Among those with disabilities, the incidence of cyberbullying exceeded standard rates since 83% of male victims and 75% of female victims revealed experiencing it. According to research findings, 64.40% of bully perpetrators were male, and 35.60% were female. A portion of 18.26% of female participants acknowledged bullying someone, while the male respondents totaled 36.19% for cyberbullying activities, which equated to nearly double the female percentage. The data showed no significant gender gap among cyber bystanders because 44.34% of female participants,

[23] National Crime Records Bureau, https://www.ncrb.gov.in (last visited Feb. 01, 2025)
[24] Manpreet Kaur & Munish Saini, *Indian Government Initiatives on Cyberbullying: A Case Study on Cyberbullying in Indian Higher Education Institutions*, 28 Educ. Info. Technol. 581, 615 (2023), https://doi.org/10.1007/s10639-022-11168-4.

together with 56.19% of male participants, acknowledged watching cyberbullying happen without taking any action.

A study by UNICEF showed that 99 percent of individuals between the ages of 12 and up who used the internet in both urban and rural areas were using mobile phones. Mobile technology extends widely throughout India, which allows cyberbullying to occur easily, according to this statistic. The rise of cybercrime alongside daily occurrences of cyberbullying and mobile internet accessibility across India requires complete safety policies and thorough online awareness programs. Major judicial decisions have developed new strategies to handle these problems, which strengthen internet rights and accountability measures. Courts function as essential entities that determine how internet expression limits connect with online privacy rights, together with cyber harassment protection boundaries. Major decisions in the legal field serve as fundamental principles for Indian cyber law jurisprudence.

Shreya Singhal v. Union of India:[25] This pivotal decision served as a landmark ruling in India's cyber law history by looking into the validity of Section 66A from the Information Technology Act in 2000. The government index to punish users who posted offensive content online through this provision. The Indian Supreme Court ruled against Section 66A by declaring it unconstitutional since it endangered the basic right to free speech and expression through Article 19(1)(a) of the Constitution. The court ruled in favor of free speech online by striking down Section 66A, thus creating an essential law against subjective and unbridled censorship practices.

Ritu Kohli Case: Cyberstalking, along with online harassment, received its first legal recognition in India during this particular case. Ritu Kohli became aware that someone had fabricated an online identity that stole her identity. Through her fraudulent profile, the impersonator triggered explicit discussions under her name and publicly published her cell phone number, which generated numerous offensive phone calls with no regard to convenient hours. She went to the Delhi Police after experiencing violation through an impersonating threat. The police investigation resulted in Section 509 Indian Penal Code (IPC) charges being filed against the accused offender for violating female decency. Online impersonation and harassment gained legal protection through this case, which created new standards for future cases.

[25] AIR 2015 SC 1523

RECOMMENDATIONS TO STRENGTHEN THE LEGAL FRAMEWORK

Several legal frameworks have been assessed in India, but the country lacks a dedicated cyberbullying law that handles this problem. The increasing problem of cyberbullying receives partial legal protection from provisions within the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC) and the Bharatiya Nyaya Sanhita (BNS), 2023, but no law exists to address this type of cyber abuse specifically. The law offers several ways to combat cyberbullying through its implementation of Defamation (Section 356 BNS), violation of privacy (Section 66E IT Act), criminal intimidation (Section 351 BNS), sexual harassment (Section 76 BNS), and stalking (Section 78 BNS). Any suicide act that emerges from cyberbullying can become punishable due to current laws regarding abetment to suicide cases. The following suggestions outline how to enhance the existing electronic harassment laws:

Defining Cyberbullying Clearly: The difficulty of fighting cyberbullying through legal mechanisms exists mainly because there remains no definitive definition of what constitutes it. The multiple existing laws that deal with online harassment fail to provide a complete definition of cyberbullying. A precise legal definition will help victims by establishing effective enforcement policies with standard response guidelines.

Introducing a Dedicated Cyberbullying Law: The current legal framework enables cyberbullying prosecution since they exist in different legislation, but enforcement becomes complicated due to their distribution among multiple laws. Specific cyberbullying legislation would unite existing cyberbullying provisions into a UUV act that enhances victim access to justice. Such legislation would provide distinct and comprehensive punishment for all cyberbullying varieties, including harassment and stalking activities online.

Clarifying Overlapping Legal Provisions: Several laws concerning cybercrime demonstrate overlapping features, which cause problems with specific le cyberbullying situation allows either a breach of privacy under the IT Act or defamation under the BNS to be applied because both provisions can address the situation. The process of cybercrime enforcement would benefit from a transparent legal framework with specific guidelines that specify how individual cybercrime laws should be applied.

Training Law Enforcement and Judiciary: The prosecution of cyberbullying remains challenging because police, along with court officials, typically hold limited computer-related expertise. The training of personnel in digital forensics and handling online harassment cases,

along with victim impact knowledge, enhances abilities to manage such digital crimes competence. Special cybercrime units with expert personnel would both accelerate case investigations and ground investigations in the needs of victims.

Strengthening Reporting and Support Systems: The majority of cyberbullying victims stay silent because they expect further persecution or feel ashamed or do not put faith in the systems that are meant to protect them. The likelihood of reporting incidents of cyberbullying increases when people have access to special helpline services and private reporting platforms combined with victim assistance programs, which include counseling and legal assistance. Schools and workplaces, together with social networking sites, must create well-documented policies that enable users to report cyberbullying through simple procedures. Digital evidence becomes a main requirement for achieving a successful outcome in cyberbullying cases. Advanced cyber forensic techniques, along with trained experts, allow digital evidence collection and preservation that results in court acceptability for successful prosecutions.

The Establishment of Awareness Initiatives: Merely having legal guidelines remains insufficient to stop cyberbullying situations. Every person needs to receive information about their rights, along with responsible digital conduct and the effects of cyberbullying, through public awareness efforts, education programs, and digital literacy programs. Students should learn digital citizenship through educational programs at schools that instruct them about showing empathy while using the internet properly and teaching them to report dangerous cyber activities.

Encouraging Collaboration Between Stakeholders: A collective action proves necessary for solving the intricate issue of cyberbullying. To protect digital users from harm, all stakeholders, including representatives in government positions and those from law enforcement, plus educational professionals, together with psychological health professionals and technology firms, need to collaborate to develop safer online environments. The legal framework keeps current with digital dangers through scheduled discussions between different stakeholders and regular policy reviews, as well as the establishment of public-private partnerships.

A safer, more responsible online culture emerges through implementing these recommendations together with addressing existing gaps, making the legal system developed to penalize cyberbullying also prevent its occurrence. We need to adopt prevention-based

strategies that will protect the digital realm from becoming a fearful domain of harassment instead of a friendly online world.

CONCLUSION

Simple regulatory measures are necessary to protect children from both positive and negative digital transformation consequences regarding their privacy, security, and rights. The online actions of parents through sharenting and the possibility of cyberbullying and digital predator behavior create ethical and legal problems for children throughout the world. The global governments of India, the UK, the EU, and the US have passed various legislative acts to handle the situation. The practice of posting child-related content online is known as sharenting. The widespread practice produces multiple problems that affect digital privacy rules and consent and digital identity protection. Under French law, children can request the removal of their posts from the internet however, the state of Illinois pays child influencers, while India possesses data protection rules, although parental internet activity remains unregulated by law. The worldwide problem of cyberbullying reaches its highest point in India because India has the highest number of child harassment incidents online. The laws to combat online abuse are present in the IT Act, and POCSO demonstrates limited enforcement capabilities because prosecution rates are very low.

The Digital Personal Data Protection Act of 2023 in India joined the Online Safety Act (2023) for the UK and EU GDPR decisions and US COPPA rules to create new obligations for platform data protection. The implementation of India's Digital Personal Data Protection Act of 2023 faces difficulties because it struggles with jurisdictional independence, and important populational groups have low digital literacy skills. The legal landscape targets the development of complete child protection by establishing prevention measures and ensuring responsibility along with international partnership. Most organizations currently require collaboration to establish safety in their digital environments. Organizations must strengthen their laws and teach online capabilities alongside enforcing platform accountability, yet parents require complete involvement. National governments should expand their forensic computer techniques as well as establish better ways for reporting cybercrimes. International digital laws require standardization from governments to secure children in both the digital and physical realms. The establishment of an equal digital system with safety protocols for children's rights requires everyone in society to work together.