Central University of Kashmir Law Review
Vol. 5 (2025)
eISSN: 2583-6935
pp. 220-235

Legal Analysis of the Prevention of Cyber Abuse Among Children and the Role of Digital Communication Tools

Ashish Kumar Singhal[*]
Eakramuddin[ǂ]
Seema Sharma[‡]

Abstract

The greatest resource of country is young generation. Our main goal of eliminating inequality and establishing social justice should be served by providing equitable developmental opportunities to all children during the growth period. However, crimes are increasing along with technology, and regrettably, our children are not safe. Although there are many advantages to technology, but side effects cannot be denied. Digital media has become a heaven for criminal activity. Due to the intrinsic anonymity and absence of in-person communication, a veil of secrecy is created, which decrease responsibility. Because of this, it is simpler for people to act in a negative way without worrying about the consequences right away. The prevalence of cyberbullying has increased along with other offences like grooming, sexting, identity theft, and harassment. The study describes and discusses the rights of children in cyber world. In addition to this, this paper also discusses the role of social networking sites along with existing laws in India to regulate these sites and provide safe access to internet.

Keywords: *Digitalization, Cybercrimes, Internet, Cyberbullying, Social Media, Human Rights*

1. Introduction

Human rights are inherent freedoms that are essential to people's dignity and general well-being. People have these rights regardless of their caste, creed, colour, sex, religion, age, or place of residence. The same human rights apply to children as they do to adults. When the internet was first discussed in 1990, nobody could have predicted that it would become a ubiquitous presence in people's lives. Information and Communication Technology is now ingrained in many aspects of

[*] Associate Professor, ICFAI University, Dehradun, Uttarakhand, India
[ǂ] Associate Professor, Jamia Millia Islamia University, New Delhi, India
[‡] Research Scholar, ICFAI Law School, ICFAI University, Dehradun, Uttarakhand, India. email: simigaur2@gmail.com

https://doi.org/10.66498/CUKLR.5.2025.220-235

people's everyday lives around the world, including education, information and communication, e-government, the health sector, and many more. Children have been involved in this phenomenon as an integral component. The way humans live has changed fundamentally. Nowadays, it is hard to imagine a world without information technology because most human endeavours rely on it. One of the main issues with information technology is its misuse by anti-social elements. Computers, computer systems, and computer networks enable the commission of traditional crimes by providing new sophisticated tools.

2. Types of Cyber Crimes

The word 'cybercrime' refers to any unlawful activity in which a computer or computer network is utilised as a tool, a target, or an accomplice. It covers any illegal behaviour that occurs within the purported boundaries of internet.[1]

(a) Cyberbullying: This is one of the grievous offences in which Digital communication tools, including social media, instant messaging, and online platforms, are purposely used to harass, threaten, or hurt individuals. Section 66E of India's Information Technology Act, 2000, outlines the consequences, for instance, violation of the right to privacy by taking, publishing, or sending a picture of anyone's private area of the body without that person's permission. This section is used when cyberbullies post private or explicit photos without permission.[2] Several countries have taken initiative to enact legislations to tackle such offence. For instance, US has many federal and state laws to combat cyberbullying. It includes anti-harassment legislation, child protection legislation and electronic communication legislation. In this regard *Megan Meier case* [3]is a leading case. In this case Megan Meier who was a teen committed suicide after being bullied on myspace by an adult posing as a teen boy. This case sparked debate on need for legislation to combat such behaviour, as well as the serious consequences of engaging in cyberbullying.

---

[1] U. Siber, *The International Emergence of Criminal Information Law* (Köln, 1992) 49–55.

[2] F. Gontard, *Buddhist Understanding of Childhood Spirituality: The Buddha's Children* (London, Jessica Kingsley Publishers, 2017) 55–56.

[3] United States v. Drew 259 F.R.D. 449 (C.D. Cal. 2009).

Another significant case[4] is of Canada in which one woman was accused of criminal harassment and imprisoned. The court emphasised the importance of legal intervention in the fight against cyberbullying.

In the significant case of *Ravi Kumar v. State of Tamil Nadu,*[5] a college student impersonating a female classmate created a fake Facebook profile and posted slanderous content. The defendant was found guilty for the violation of section 66D (penalty for impersonating someone using a computer resource) and section 67 of the Information Technology Act, 2000. One more important case heard by the supreme court was *Shreya Singhal's case*[6]in which section 66A of the Information Technology Act, was in question which deals with the offence of sending obscene electronic messages. The apex court declared Section 66A unconstitutional. This judgement acknowledged the significance of the right to free expression.

The issue of cyberbullying caused by improper use of social media platforms was brought before the Indian Supreme Court in the 2018 case titled *Swapnil Tripathi v. Supreme Court of India*.[7] The judge emphasised that it is the responsibility of social media platforms to prevent cyberbullying by responding quickly to complaints and acting against those who bully others online.[8] In another case, *Rajesh Kumar v. State of Uttar Pradesh (2019),*[9] the defendant was punished for the offence under sections 354D of Indian Penal Code as well as section 66E of IT Act for sending vulgar and offensive WhatsApp messages to a woman.

Cyberbullying perpetrator and victim can be of any age but mostly children who use social media or online websites are more vulnerable and considered easy target for such offences. However, adults can also be a victim of cyberbullying.[10] Such offences affect the mental as well as general health of victim and resulted in anxiety, despair, and

[4] *R v. Elliott* (2002) EWCA Crim 931.

[5] *Ravi Kumar v. State of Tamil Nadu* (2004) 10 SCC 776.

[6] *Shreya Singhal v. Union of India* (2015) AIR SCW 1989.

[7] *Swapnil Tripathi v. Supreme Court of India* (2018) 10 SCC 639.

[8] Kaelber, O. *Tapta-Marga: Asceticism and Initiation in Vedic India* (State University of New York Press, n.d.) 33.

[9] *Rajesh Kumar v. State of Uttar Pradesh* (2021) AIRONLINE 2021 ALL 2534.

[10] Sarl, N., Biiyiikiinal, & S. N. C. 'A Study of the History of Child Abuse' (1991) 6(6) *Paediatric Surgery International* 401.

even suicidal acts. Cyberbullying can also cause long term psychological harm. Hence, it is crucial that awareness should be raised and digital literacy should be ensured along with effective mechanism to prevent such heinous offences. This includes programs that instruct parents, educators, and society on how to handle cyber offences. To effectively combat cyberbullying and create safer online environments, multiple stakeholders, including schools, government agencies, and technology companies must work together.[11]

(b) Revenge Porn: This refers to the practise of publishing or disseminating private or explicit photos or films of someone else without that person's consent. The intention behind this offence is mostly to embarrass or otherwise coerce the targeted person that violate person's privacy as well as autonomy and cause detrimental effects on their mental as well as emotional health. Section 67 of the IT Act, 2000 contains the provisions pertaining to the sharing of explicit content without the agreement of the parties. It acknowledges the potential harm of these actions and attempts to protect persons from the unlawful sharing of private photos or videos.[12] In the *Air Force Bal Bharti School Case*[13], a 16-year-old student who had been bullied for having a pockmarked face decided to exact revenge by creating a pornographic website. He posted the modified and scanned images of his teachers and classmates to that porn website. The boy was charged under sections 292, 293, and 294 of the IPC, the Indecent Representation or Women Act, and section 67 of the IT Act, 2000.

(c) Doxing: It involves illegal disclosure and publication of private information in a public place without the consent of concerned person. For instance, home address, phone number, email address and social media profile disclosure. It can be done by online or offline modes intended to harass, threaten, or harm the victim.[14] It can happen when someone with illegal intention gathers private information about another person by several methods like social media platforms, online directories, or hacking and subsequently

[11] *Ibid*.

[12] Sen, R. K., & Dasgupta, A. *Problems of Child Labour in India* (Deep & Deep Publications Pvt Ltd, 2003) 270.

[13] The Air Force Bal Bharti, Delhi Cyber Pornography Case (2001).

[14] Tripathy, S. N., & Pradhan, S. P. *Girl Child in India* (Discovery Publishing House, 2003) 93.

make this information public. Section 66 C of the IT Act contains the provision relating to identity theft. Doxing is also a part of identity theft. Identity theft means unauthorised use of another person's identity information, like personal information, electronic signature, biometric data. Furthermore, section 72A of the IT Act provides punishment for the disclosure of personal information by the person who deals with the information while performing the legal contract with someone and use that information without the consent of that person.

Even though there may not be specific cases focusing solely on doxing, there are relevant rulings that recognise the harm caused by the unauthorised disclosure of personal information. The Madras High Court acknowledged the gravity of actions comparable to doxing in the 2014, in the case, *Malathi v. State*[15], ruling that the publication of private and personal information without the individual's consent violates the individual's right to privacy. In the opinion of the court, the victim may face harassment, intimidation because of the action of the offender. Although this case does not deal with the offence of doxing directly but established a precedent for recognising the harm that can result from the inappropriate disclosure of information. These case laws basically create precedent along with other legal provisions of the IT Act for the prosecution of doxing offences.[16]

(d) Website Defacement: This is typically accomplished by using a system cracker to replace a website's homepage. The cracker compromises a web server and modifies the hosted website to create a new one.

(e) Morphing Pictures: One approach to take advantage of people who post pictures on social networking sites is to morph someone's face onto another person's body and broadcast it to blackmail or otherwise threaten the person.

(f) Online Gaming: Children who are susceptible to clinical depression, low self-esteem, and loneliness may be drawn to risky online games that could further damage them and become addictive. Some even result in the victim taking his own life, such as the well-

[15] *Malathi v. State W.P*. Nos. 19728 of 2020 & 484 of 2021.

[16] Basu, A. *"Trafficking of Minor Girls for Commercial Sexual Exploitation in India: A Synthesis of Available Evidence"* (Population Council, August 2014).

known "*blue whale challenge.*" This presents a social and personal challenge to those in the vicinity.
(g) Dating Websites: On dating platforms untrustworthy individuals can use any intimate images or texts of their potential dating partners to blackmail them.

3. Role of Social Media
Now a days social networking sites have become heaven for the perpetrators to abuse each section of society specially children. Social networking services like Facebook, Twitter, and YouTube mandate that users should be of at least 13 years old in accordance with their privacy policies. Nevertheless, over half of teenagers who use these social networking sites do so by misrepresenting their age. The age verification threshold on social networking sites is meaningless because it is not the website owner's duty to verify that users are of legal age. As a result, all conventional age verification systems have been proven to be ineffective and defective. Kids are becoming more and more interested in social networking sites (SNSs), especially Facebook, because every time they check in, they discover something new.
According to Children's Online Privacy Protection Act (COPPA) (US) regulations, Instagram's age requirement is 13. However, this requirement is easily bypassed by the children by manipulating the data. Instagram faced significant criticism due to its role in facilitating cyberbullying.

4. UNCRC and Rights of Children
Following World War I, children's rights were recognised for the first time. For the first time in history, the **League of Nations** enacted the **Geneva Declaration** in 1924, which guaranteed parents a certain duty to their children and confirmed and acknowledged children's rights.[17] However, the **International Convention on the Rights of the Child,**[18]

[17] UNICEF "Geneva Declaration Drafted by Eglantyne Jebb, Founder of the Save the Children Fund" (n.d.) *available at:*https://www.unicef.org/child-rights-convention/history-child-rights (last accessed 5 January 2025).
[19] UNICEF "The Convention on the Rights of the Child is Adopted by the United Nations General Assembly" (n.d.) *available at:* https://www.unicef.org/child-rights-convention/history-child-rights (last accessed 5 January 2025).

was the first legally binding international agreement to acknowledge children's rights. The treaty acknowledges that children under the age of eighteen have fundamental rights. Regretfully, compared to adult rights, some children's rights—such as the right to privacy or the ability to speak—are severely restricted. Even in certain nations, children are not permitted to make their own decisions.

5. India's Cyber Security Infrastructure

To control the rising number of crimes, Indian law has put in place several regulations. The Information Technology Act enacted in 2000 is the most prominent illustration of it. A few relevant provisions from the 2000 Information Technology Act are as follows:

The IT Act's section 43 covers those who commit cybercrimes, such as causing computer damage to a victim without that victim's knowledge or consent. This section entails a fine of one lakh rupees and a maximum penalty of three years in prison. Section 66D provides the use of computer resources to impersonate someone else to cheat. A conviction entails a maximum fine of one lakh rupees and a maximum sentence of three years.

Voyeurism is defined in section 77 of the Bhartiya Nyaya Sahita 2023 as the capture or sharing of images of a woman engaging in private or intimate activities without her consent. Sections 292 of the Bhartiya Nyaya Sahita 2023 and Section 66E of the IT Act are sufficiently broad to include similar offences in the absence of the criteria specified by this section. For first-time offenders, carries a maximum term of three years in jail, with seven years for repeat offenders.

Under section 78, Bhartiya Nyaya Sahita 2023, both offline and online stalking are prohibited. cyberstalking is the practise of reaching out to or trailing a lady using technology, like email or the Internet, even though she does not seem interested. For a first offence, this offence has a maximum punishment of three years in jail and a fine. For a second offence, five years in prison and a fine

(a) The POCSO Act, 2012

This Act contains provisions pertaining to sexual offences, such as child pornography, sexual assault, abuse, and sexual harassment. Under the POCSO Act, 2012, Section 11 defines sexual harassment. Anyone who regularly approaches a child *via* any form of electronic communication makes or threatening to use the child's body or involve the youngster in sexual activity, whether such threats are true

or made up is engaging in sexual harassment. Section 13 of this Act prohibits the use of children for pornography. Sections 14 provides penalties for employing children in a pornographic purpose.

(b) The Digital Personal Data Protection Act, 2023 (DPDP Act)

This Act is enacted with the objective of safeguarding the digital privacy and personal information of persons. This is the first time when the term "child" is defined under the DPDP Act "as an individual who has not completed the age of eighteen years."

DPDP Act and Data compliance for children

- **Verifiable Parental approval:** According to Section 9 of the DPDP Act, before processing the children's personal data verifiable parental consent is required. Such consent should be free, unambiguous, and accompanied by a clear affirmative action.
- **Limitation of Purpose:** Such information should be used only for the purpose for which consent has been granted.
- **Ensure Well-Being:** The data fiduciary cannot use the personal data of child in such manner that could have negative impact on the well-being of child.
- **Absence of tracking or advertising:** Section 9(3) expressly prohibit the behavioural monitoring and tracking or targeting advertisements.
- **Right to Erasure:** Under this clause, kids or their parents can ask for their personal information to be deleted.
- **Marketing Restrictions:** Businesses may not be allowed to advertise to youngsters online, especially when it comes to focussing on vulnerable people for profit. Businesses are restricted from gathering information for children's targeted advertising.

(c) The Digital Personal Data Protection Rules, 2025[19]

The Digital Personal Data Protection Rules, 2025 as recently released for the public opinion, contains provision for verifiable consent and provides that data fiduciary is required to take specific verifiable consent from the parents before processing the personal data of

[19] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Gazette of India, Ministry of Law and Justice.

children and specific steps should also be taken to guarantee that the individual giving consent is the child's parent or legal guardian and such parent can be identified. The data fiduciary should use such methods of verification of consent which ensure that the consent is given by the parents only. This verification procedure is crucial to guarantee that consent is given by the adult person. It can be done by several methods like by using digital locker service to submit identification details when parent is a registered user of digital locker. Though the DPDP Act provides robust protections but there may be obstacles to its successful implementation because of the following reasons:

- **Global Reach of Digital Platforms:** Application of local data protection laws on global nature of data looks challenging. For example, one organisation which has many branches worldwide must follow different laws applicable on data which is confusing and difficult at the same time.
- **Technological Advancements:** Due to the non-stoppable advancement in technology, like (blockchain, artificial intelligence) it might be challenging to update the laws.
- **Parental Involvement and Awareness:** Due to the unawareness, parents cannot predict the risks that children may face while utilising technology. Hence, it can be said that DPDP Act will be helpful for those parents who are educated and aware of all the aspects of the technology.[20]

(d) India's first hotline to report Child Pornography: The first-ever hotline in the country to stop child sexual abuse online and to remove child pornographic content is set to launch. Users will be able to anonymously and securely submit images and videos of child sexual abuse *via* the hotline.[21] An industry watchdog and the world's most successful hotline for eradicating child pornography, the UK-based Internet Watch Foundation (IWF) has teamed up with the Aarambh Initiative, a network of organisations and people dedicated to child

[20] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Gazette of India, Ministry of Law and Justice.

[21] Ministry of Electronics and Information Technology, Government of India, *Directions to Internet Service Providers for Blocking Child Sexual Abuse Material* (July 2017).

protection in the country.[22] Using the hotline in India, which will be hosted on aarambhindia.org, anyone will be able to anonymously and securely send images and videos of child sexual assault. The hotline will eventually be offered in up to 22 regional languages, with Hindi and English being the initial languages. The hotline's three primary objectives are to identify and report the perpetrator to the appropriate law enforcement agency in his country, block and eventually remove offending content, and, if required, contact the underage victim, and offer rehabilitation.[23] In order to prevent the dissemination and transmission of such content into India, the Union Ministry of Electronics and Information Technology directed all ISPs to adopt and implement Watch Foundation Resources by July 2017 at the latest.[24]

6. Initiatives taken by the Government to control Cyber Crimes

Under the Nirbhaya Fund, the government opened platform named "Cyber Crime Prevention against Women and Children" (CCPWC).[25] To make reporting all cybercrimes easy, The National Cybercrime Reporting Portal (NCRP), located at www.cybercrime.gov.in, was created under CCPWC, with a focus to protect women and children. In all states and union territories, a toll-free Helpline number 1930 is available. The NCRP has seen over 16.18 crore complaints as of April 2024 and 1.94, million Child Pornography/Rape or Gang Rape (CP/RGR) complaints had been submitted.[26] A Memorandum of Understanding (MoU) was signed in April 2019 between the National Crime Records Bureau (NCRB) in India and the National Centre for Missing and Exploited Children (NCMEC) in the United States about the receiving of the Tip-line report on online child pornography from

[22] Internet Watch Foundation, *Annual Impact Report* (2023).

[23] United Nations Children's Fund (UNICEF), *Child Online Protection Guidelines* (2021).

[24] Aarambh India Initiative, *India's First Hotline to Combat Online Child Sexual Abuse, available at*: https://aarambhindia.org/ (last visited on September 20, 2025).

[25] Ministry of Home Affairs, Government of India, *Cyber Crime Prevention against Women and Children (CCPWC) Scheme*, Nirbhaya Fund.

[26] National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Govt. of India, 2024).

NCMEC.[27] Several technology-driven programs and plans are part of the Nirbhaya Fund. One of these programs is the Emergency Response Support System (ERSS)-112, which has been operationalised in 36 States and Union Territories. By April 30, 2024, it had handled more than 36.29 crore calls and had downloaded more than 14.36 lakh copies of the "112 India" app. Safe City Projects are all-encompassing, integrated initiatives created by the city's police and municipal corporations to address any gaps in the current infrastructure and meet the expectations of their female residents.[28] In Phase I of the project, technology will be installed in eight cities to support smart police and safety management, and State Forensic Science Laboratories (SFSLs) established in 30 States and UTs will be strengthened or established.

Cyber Crimes against Children (2017 to 2021)[29]

Year	Total cases of cyber crimes	Total cases of cyber-crimes against children	Percentage distribution of cybercrimes against children to that of total cases
2017	21796	88	0.40%
2018	27248	232	0.85%
2019	44546	305	0.68%
2020	50035	1102	0.20%
2021	52974	1376	2.59%

The Integration of Women Helpline (WHL)-181 with ERSS is operational in 35 States and UTs, as of May 31,2024 and have helped over 76.02 lakh women. 11 States and UTs, including Bihar, Puducherry, Himachal Pradesh, Chandigarh, Andaman & Nicobar Islands, and Odisha, West Bengal, Sikkim, Uttarakhand, Mizoram, Chhattisgarh have commissioned Monitoring Centres for the implementation of the Vehicle Tracking Platform (VTP). The Central

[27] National Cyber Crime Reporting Portal, Government of India, *Cyber Crime Statistics, available at* https://www.cybercrime.gov.in. (last visited on May 25, 2025).

[28] Ministry of Home Affairs, Government of India, *Safe City Projects under Nirbhaya Fund – Phase*

[29] National Crime Records Bureau, *Crime in India 2021* (Ministry of Home Affairs, Govt. of India, 2022).

Forensic Sciences Laboratory in Chandigarh inaugurated a DNA analysis facility on December 23, 2019. Furthermore, four separate units have been established, completely furnished with contemporary DNA methodologies and profiling.[30]

People Arrested and Cyber Crimes/Cases Filed under the IT Act (2014 to 2024)[31]

Year	Cases registered	Person arrested
2014	9,622	5,752
2015	11,592	8,121
2016	12,317	8,613
2017	21,796	9,622
2018	27,248	18,930
2019	44,546	21,796
2020	50,035	24,064
2021	52,974	25,789
2022	65,893	27,612
2023	75,656	34,597
2024* Till August	77,858	36,235

7. After Effects of Cyber Abuse on Child Victims

Multiple studies have shown that policies and plans designed to educate individuals, especially young people, about internet safety precautions can be improved to be more effective. Individuals under the age of 18 should exercise caution when interacting with unfamiliar individuals online and should refrain from sharing any personal information with third parties.[32] Further investigation into the means through which teenagers access social media platforms and engage in fraudulent behaviours will enhance public awareness of the activities and behaviours they engage in while using the internet. By embracing this viewpoint, it is possible to develop improved strategies and precautionary measures to protect adolescents while they use the internet. The recognition of cybercrime as a significant problem

[30] Press Information Bureau, Government of India, *Inauguration of DNA Analysis Facility at CFSL Chandigarh* (Dec. 23, 2019).

[31] National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Govt. of India, 2024).

[32] David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007).

has occurred during the past twenty years. Cybercriminals demonstrate a strong inclination towards targeting young adults in modern society. Several factors can heighten the probability of an individual becoming a target of cybercrime, such as gender, educational attainment, financial circumstances, and even coercion.[33]

The after-effects of cyber abuse cannot be ignored because it targets that section of society which because of the lack of the emotional maturity and blindly coping mechanisms to effectively navigate such traumatic experiences. Children are increasingly involved in online environments, where they may encounter various forms of cyber abuse, including cyberbullying, online harassment, and grooming.[34] To create robust mechanism and support system specially to protect children from cybercrimes understanding of the seriousness of the effects of cyber abuse on children is essential. Following are some side effects of technology on children:

(a) Psychological Impact: One of the most significant after-effects of cyber abuse on child victims is the psychological trauma. For example, when victims endure constant harassment and humiliation online, cyberbullying can result in emotions of worry, sadness, and low self-esteem.[35] Sleep issues may be developed in children because of cybercrimes, especially those who are exposed to disturbing content or face cyberbullying, which may be resulted in chronic fatigue and difficulties in daily functioning.[36] In some cases, children who experience cybercrimes may engage in riskier behaviours, such as attempting to "get revenge" on perpetrators, more frequent use of the internet in unprotected ways.[37]

(b) Physical health impact: The physical health effects of cybercrimes cannot be ignored as these effects are significant, especially when considering the overall progress of children because of the stress, anxiety, and other emotions associated with wellbeing

---

[33] Organisation for Economic Co-operation and Development, *Protecting Children from Digital Risks* (OECD Publishing, 2020).

[34] K. Jaishankar, *Cyber Criminology* (CRC Press 2019).

[35] World Health Organization, *Mental Health Impacts of Cyber Abuse among Children and Adolescents* (2022).

[36] Mark Yar, *Cybercrime and Society* (2d ed., Sage 2013).

[37] Sonia Livingstone & Amanda Third, *Children and Young People's Rights in the Digital Age* (New Media & Society 2017).

of a victim. While cybercrimes are primarily psychological in nature, the physical repercussions can also be caused due to the emotional distress. For instance, Sleep Disturbances, Headaches and Migraines, Digestive Issues, Fatigue and Low Energy, Physical Symptoms of Anxiety, Weakened Immune System, and Isolation.[38]

8. Suggestions to prevent Cyber Crimes

A multi-stakeholder strategy is needed to effectively address child cyber abuse. The following are thorough recommendations meant to curb and stop child internet abuse in India:

(a) Enhancing regulatory and legal structures: Revise current legislation to specifically handle new types of cyber abuse. Create proper trained and specialised cyber units to deal with crimes involving children. Reporting procedure should be made simpler and ensure privacy.

(b) Solution based on Technology: AI tools can be used to track and identify negative online activities. Social media companies should impose more stringent age verification mechanism. Encourage the use of safe browsing resources and parental control software. Forensics should be prepared not only to stop cyber incidents but also to collect evidence to bring criminal charges against those responsible. Since the introduction of multi-user systems, password security has been essential People should ensure that their Passwords to sensitive data always be kept secure.[39]

(c) Parental and Community Involvement: Encourage conversation about online safety between parents and kids. Local governments, NGOs, and schools should establish support system.

(d) Cooperation amongst interested parties: With the collaboration of tech firms that are kid-friendly the aim of safe virtual world can be achieved. To answer cross-border challenges, collaboration between international organisations, NGOs, and law enforcement authorities should be promoted.

(e) Counselling and Rehabilitation Services: Helplines and counselling facilities can be ensured for people who have been the victim of online harassment. Offer psychological support to aid in the

[38] World Health Organization, *Mental Health Impacts of Cyber Abuse among Children and Adolescents* (2022).

[39] Jonathan Clough, *Principles of Cybercrime* (Cambridge Univ. Press 2015).

trauma recovery of the sufferers. Counsellors should receive training on how to tackle unique problems associated to online abuse.[40]

(f) International collaboration: International collaboration is essential since cybercrimes have no boundaries. India needs to collaborate with international agencies like UNICEF and INTERPOL. MOU should be signed to make it easier to share information and prosecute transnational criminals. Engagement in global forums to implement best practices for protecting children in cyber world is essential. Cybercrime Convention a true international treaty to police cybercrime through international cooperation is desperately needed.[41]

(g) Education and Awareness: National awareness initiatives aimed at educators, parents, and kids need to be launched. In the curriculum, digital ethics and cybersecurity should be Incorporated. Training sessions on identifying and reporting online abuse required to be planned. In the fight against cybercrime, numerous countermeasures can be employed. These defences include education, one of the most effective ways to combat cybercrime and raise awareness and spread knowledge. People must understand the risks associated with social media and how to protect themselves from cyberattacks. This entails teaching people how to recognise phishing emails and protect their personal information. To deal with thwart cyberattacks many tools like Firewalls, antivirus programmes, and intrusion detection systems are examples of cyber security technology that can be used. These tools prevent fraudsters from gaining access to private information by identifying and stopping unlawful communication. Strong passwords should be used for safeguarding personal data. Security mechanisms, such as encryption, to prevent unauthorised access to user information should incorporated by online platforms.

[40] Stephen Furnell, *Cybercrime: Vandalizing the Information Society* (Pearson 2018).

[41] Eoghan Casey, *Digital Evidence and Computer Crime* (3d ed., Academic Press 2011).

9. Conclusion

Platforms like E-mail, Facebook, Google, Hotmail, and Instagram are being used by children round the clock in the world to learn "ABCs". Apple, Bluetooth, chat, followed by download, leave persistent digital fingerprints on social media according to Justice S.S. Kaul's observations in the Puttaswamy case. Extra care must be taken to protect children's privacy in both the real and virtual world.

Although internet provides a wealth of knowledge and socialisation but create serious risks as well. An inclusive strategy that includes education, technology, community involvement is needed to address this issue. Legal frameworks must be updated to combat new types of cyber abuse with the use of strong enforcement tools and specialised training for law enforcement.

Technology may be a problem as well as a solution. Social media, artificial intelligence, and other technological developments can be used to track, identify, and stop abusive behaviour. To tackle cross-border cybercrimes and build a secure online ecosystem, governments, IT businesses, non-governmental organisations, and international organisations must work together. Lastly, counselling services, support systems, and rehabilitation initiatives must be ensured to heal and flourish well-being of children. The battle against child cyber abuse cannot be handled alone by any organisation. It requires collective efforts from all parties involved to pursue the goal of protecting children's rights and welfare in the digital world. India should make endeavour to create the internet a safest place for its children by putting these tactics into practice and motivating a culture of alertness and empathy. By this way technology can fulfil the aim of providing safe and child friendly cyber space.