

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 4 | Issue 3

2022

© 2022 *International Journal of Legal Science and Innovation*

Follow this and additional works at: <https://www.ijlsi.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

This Article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in International Journal of Legal Science and Innovation after due review.

In case of **any suggestion or complaint**, please contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication at International Journal of Legal Science and Innovation, kindly email your Manuscript at editor.ijlsi@gmail.com.

Child's Right in Cyberspace: A Critical Analysis of Protection and Privacy under the Indian Legal System

SUMEDHA GUPTA¹

ABSTRACT

The internet and digital communication tools, such as mobile phone messaging services, have proven to be tremendously beneficial to human society. However, technology, particularly digital technology, has unintended consequences. Children are the most susceptible population that may be subjected to the harmful consequences of internet and digital technology advancements. The world's most important resource and best hope for the future are children. A child accounts for one out of every three internet users worldwide. In the global South, this share is likely to be substantially greater. The internet is not seen by young people as a distinct entity or environment. It's just another place where they may connect with friends, pursue interests, or meet new people. In recent years, online child safety has gotten a lot of attention around the world. International groups that have been focused on child abuse and exploitation as a violation of children's rights have noticed that it overlaps with children's internet use. Children's daily lives are increasingly replete with the use of digital devices and technologies. Aside from the numerous benefits connected with the online environment, such as education, entertainment, and communication, it has also been linked to a number of hazards, such as grooming and cyber bullying. As the most vulnerable members of society, it is critical to analyze the level of risk, mediation, and digital literacy among youngsters. This paper examines the opportunities and risks in cyberspace for children. It also discusses the policies and regulatory framework in India to protect the digital child rights. Lastly, the paper concludes with few suggestions and recommendations to promote the child's best interests in this digital era.

Keywords: *Child Rights, Online threat, privacy, protection, cyberspace*

I. INTRODUCTION

Even at an early age, children increasingly spend a significant amount of time online. According to estimates, 26% of the world's population is under the age of 15, and they are enthralled by the possibilities offered by digital technologies. Without a question, digital

¹ Author is a Research Scholar at Galgotias University, India.

technologies play an important part in the lives of most children throughout the world; technology access is fast rising among children, and its integration is having both beneficial and bad effects on their lives. According to estimates, one out of every three digital technology users in the globe is a child, and technological penetration has a profound impact on everything from child protection to politics, economics, health, and education.

Children have increased access to communication, entertainment, and information through digital devices, as well as opportunities for self-expression, learning, and engagement. Digital gadgets also provide a mechanism to communicate, learn, and publish to billions of people in ways that were unimaginable only twenty-five years ago.² With all of these unrivaled advantages come hazards. For example, digital gadgets have made it simpler to create and distribute violent photographs of children, as well as providing new ways for abusers to contact youngsters. Regardless, many intertwining in children's lives might either encourage or discourage their use of digital devices.

Children are among the most active web users, and they are unfortunately exposed to a variety of risks. They spend a lot of time on the internet. Because the internet is a perplexing place, it exposes children to the murky side of the world. Organizations working to better the lives of children need to know how to keep them safe online while still maximising their potential for learning, engagement, and creativity. To effectively regulate children and teenagers' use of digital media, policymakers and technologists must consider children's perspectives and experiences. However, there is still a lack of global data that would allow policy and practise to serve the greatest interests of children.³

With the declaration of UNCRC (United Nations Convention on the Rights of the Child), which has more than 100 signatures and parties, the recognition of juvenile rights, or the rights of children, in hundreds of countries made an important step forward. Regardless of race, colour, sex, language, religion, political or other opinion, national, ethnic or socioeconomic origin, property, disability, birth, or any other status whatsoever of the children or their parents, the Convention endowed them with certain basic child rights. In addition to basic human rights, children today have the right to be loved, protected, and cared for.⁴

² Shariff S and Johnny L, "Child Rights in Cyberspace: Protection, Participation, and Privacy" (*De Gruyter*, January 29, 2016) <<https://www.degruyter.com/document/doi/10.3138/9781442687615-012/html>> accessed June 16, 2022

³ Orijit Das, 'Cyber Laws in India' (2000) 28 Int'l Bus Law 327 pp. 327-329. HeinOnline, <https://heinonline-org.gnlu.remotlog.com/HOL/P?h=hein.journals/ibl28&i=329>.

⁴ Miyazaki, Anthony D., et al. "Self-Regulatory Safeguards and the Online Privacy of Preteen Children: Implications for the Advertising Industry." *Journal of Advertising*, vol. 38, no. 4, 2009, pp. 79–91. JSTOR,

II. THE ABUSE OF CHILDREN'S RIGHTS ON DIGITAL PLATFORM

On the Internet, children can and have been subjected to a variety of 'sin', the most apparent of which is undoubtedly child pornography. When children use the internet to communicate, they may also expose themselves to privacy violations. Furthermore, "the Internet may and has been used to persuade youngsters to join groups with dubious origins or goals, such as hate groups, and to commit fraud against them. Apart from the recruitment of children into child pornography, the availability of pornographic content that children can access can also be considered a violation of children's rights."⁵

III. CYBER THREATS FOR CHILDREN IN INDIA

Children can benefit from digital technologies in terms of development and education. However, as children get more access to and usage of ICT, they become more vulnerable to online abuse and exploitation. As new technologies are utilized to harass, abuse, and exploit children, cyber-crime against them is growing and diversifying.⁶ Children are frequently found to be cyber criminals. Digital technologies open up new possibilities for reinforcing and spreading current social and cultural norms, as well as mediating virtual social situations and connections.⁷ "Offline types of criminality and violence against children are taking on new forms in the online world, amplifying their consequences on children."⁸ Offline and online violence are frequently linked, with online abuse containing offline elements. Children can be harmed by non-contact abuse, which can make the transition to contact abuse easier. The ability to remain anonymous online and mimic others may encourage people to engage in offensive and criminal behavior, reducing the deterrent effect of legislation.⁹

The following are examples of current kinds of child online abuse and exploitation:

- Emotional harassment, defamation, and social exposure, intimidation, and social isolation are all examples of cyberbullying.

<http://www.jstor.org/stable/27749661>. Accessed 16 Jun. 2022.

⁵ Abdul Aziz N, "Child's Right to Free Flow Information via Internet: Liability and Responsibility of the Internet Service Provider - ScienceDirect" (*Child's Right to Free Flow Information via Internet: Liability and Responsibility of the Internet Service Provider - ScienceDirect*, April 19, 2012) <<https://www.sciencedirect.com/science/article/pii/S1877042812008154>> accessed June 16, 2022

⁶ davda zeel, "Laws Applicable in Cyberspace in India - Legal Desire" (*Legal Desire*, August 8, 2020) <<https://legaldesire.com/laws-applicable-in-cyberspace-in-india/>> accessed June 17, 2022

⁷ Székely, L., & Nagy, Á. (2011). Online youth work and eYouth - A guide to the world of the digital natives. *Children and Youth Services Review*, 33(11), 2186-2197. <https://doi.org/10.1016/j.chilyouth.2011.07.002>

⁸ United Nations, *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography*, New York 2000.

⁹ YOUN, SEOUNMI. "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents." *The Journal of Consumer Affairs*, vol. 43, no. 3, 2009, pp. 389-418. *JSTOR*, <http://www.jstor.org/stable/23859694>. Accessed 16 Jun. 2022

- Online sexual abuse: sexually graphic and violent content distribution, sexual harassment
- Child sexual abuse material (CSAM) (child pornography), “sextortion,” and “revenge pornography” are all examples of online sexual exploitation.
- Cyber extremism: recruiting and ideological indoctrination, as well as threats of extreme violence
- Identity theft, phishing, hacking, and financial fraud are all examples of online commercial fraud.
- Online enticement to criminal behaviors: access to alcohol, cheating, plagiarism, gambling, drug trafficking, sexting, and self-exposure.
- Grooming is the process of preparing a child, major adults, and the environment for sexual abuse and exploitation, as well as ideological influence.

IV. CONVENTION ON THE RIGHTS OF THE CHILDREN OF THE UNITED NATIONS

The UNCRC defines "child rights" as "The fundamental rights and opportunities that should be available to all children under the age of 18 in all countries without regard to their "race, nationality, colour, gender, language, religion, opinions, origin, wealth, birth status, disability, or any other characteristic."¹⁰

These rights improve possibilities for children and their social equality, as well as the family climate, essential medical services and government aid, training, recreation and social activities, and extreme security measures.¹¹ The UNCRC breaks down the most fundamental liberties that children should have in four broad categories that cover all of a child's affable, political, social, economic, and social rights.¹²

V. CHILDREN'S RIGHTS IN CYBERSPACE

As previously stated, the UNCRC is the primary legal framework that governs children's rights around the world today. The UNCRC does not specifically provide any rights for children online, which appears to be an issue at first glance. As a result, it appears that

¹⁰Calciano, Elizabeth M. "United Nations Convention on the Rights of the Child: Will it help children in the United States." *Hastings Int'l & Comp. L. Rev.* 15 (1991): 515. <<https://heinonline.org/HOL/LandingPage?handle=hein.journals/hasint15&div=25&id=&page=>>

¹¹Mbise, Amana Talala. "The diffusion of the United Nations Convention on the Rights of the Child (UNCRC) more than the African Charter on the Rights and Welfare of the Child (ACRWC) in Africa: The influence of coercion and emulation." *International Social Work* 60.5 (2017): 1233-1243 <<https://journals.sagepub.com/doi/abs/10.1177/0020872816639370>>

¹²Corner L, "Law And Policy In Indian Cyberspace" (*Law Corner*, September 4, 2020) <<https://lawcorner.in/law-and-policy-in-indian-cyberspace/>> accessed June 17, 2022

children in cyberspace do not have any form of enforceable or legal rights.¹³

Given how difficult it is to draw a line between the online and offline worlds, it's a logical assumption that the same laws, rules, and regulations apply to cyberspace, with issue-specific interpretations¹⁴. As previously stated, the virtual aspect of cyber space, as opposed to the real and tangible world, does not ipso facto imply that children's rights in cyberspace are suspended. In this regard, the UNCRC and other existing laws and treaties can be subjected to a digital-age-specific interpretation to identify the child's rights in cyberspace.¹⁵

Experts in the subject have worked hard to interpret the UN Convention on the Rights of the Child in a digital-age setting. Livingstone and O'Neill (2014) have begun the job of evaluating how the CRC pertains to the digital, convergent, and networked environment, concentrating on the three P's of Protection, Participation, and Provision.

VI. ONLINE PRIVACY PROTECTION FOR CHILDREN

Many advertisers and marketers have begun to focus their efforts on the constantly expanding numbers of youngsters online in order to acquire a foothold in the lucrative children's market.¹⁶

To preserve children's privacy in cyberspace, it appears that some type of regulation is required. Effective self-regulation appears to be exceedingly implausible, and will not develop at all without government assistance, according to studies and anecdotal data.¹⁷ The following principles should be used "to guide the creation of legislation for online advertising and marketing to children. Personal information (including clickstream data) about children should not be collected, and personal information about minors should not be sold."¹⁸ Children's advertising and promotions should be clearly labeled and separated from the content. Advertising sites should not be directly linked to children's content regions. There should be no direct interaction between youngsters and the characters who represent the product. There should be no direct-response marketing or online microtargeting of

¹³ Anil S, "SCC Online | Session Expire" (SCC Online | Session Expire, 0 0, 2003) <<https://www.sconline.com/Members/SearchResult.aspx>> accessed June 16, 2022

¹⁴ Sahoo, Prachilekha. "Cyber Space the Double-Edged Sword." *Supremo Amicus*, 4, 2018, pp. 324-334. HeinOnline, <https://heinonline-org.gnlu.remotlog.com/HOL/P?h=hein.journals/supami4&i=334>.

¹⁵ Choo, K. R. (2009). Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences. *Australian Institute of Criminology*, 132. <https://doi.org/10.1037/e582922012-001>

¹⁶ Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, 2012, pp. 817-85. *JSTOR*, <http://www.jstor.org/stable/23249823>. Accessed 16 Jun. 2022.

¹⁷ Sharma D and others, "Memorandum of Cooperation in the Field of Cybersecurity between India and Japan | SCC Blog" (*SCC Blog*, October 8, 2020) <<https://www.sconline.com/blog/post/2020/10/08/memorandum-of-cooperation-in-the-field-of-cybersecurity-between-india-and-japan/>> accessed June 17, 2022

¹⁸ K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 : 2017 SCC OnLine SC 996

youngsters.¹⁹

It may be time for governments to reconsider establishing legislation to ensure that children are given some level of protection when surfing the Internet, with the least amount of invasion of their privacy possible. Industry regulation, as the previous excerpt so well indicates, is unlikely to be totally effective in this regard. While some governments are beginning to focus on privacy issues and considering sector self-regulation as a viable solution, the special and distinctive concerns of children are frequently disregarded.²⁰ The limited efficacy of a self-regulation approach in protecting the interests of minors online is often overlooked in the drive to build a privacy regime that applies to activities undertaken online. This has impeded efforts to build a privacy framework that adequately protects children's online interests.

It's also worth noting that in the US Internet-related legislation aimed at protecting youngsters is frequently overturned on the grounds that it infringes on adult constitutional rights. Unfortunately, in some situations when judges have been willing to dismiss proposed Internet regulation enforcement tactics on this ground, they have failed to propose alternative, less-restrictive methods of regulating.²¹

VII. INDIA'S REGULATORY FRAMEWORK FOR THE PROTECTION OF CHILDREN'S RIGHTS

The law enforcement agencies take legal action against those who are involved in computerized sexual mistreatment or maltreatment of children in accordance with the law's provisions. The Information Technology (IT) Act of 2000 includes enough provisions for dealing with current cybercrime. Distributing, perusing, or sharing child sexual entertainment in an electronic structure is expressly prohibited by Section 67B of the Act²². In addition, the Indian Penal Code's Sections 354A²³ and 354D²⁴ make it illegal to harass or stalk women online.

The Protection of Children from Sexual Offences (POCSO) Act²⁵ is a crucial piece of legislation that handles sexual offences against children. Child pornography, cyber stalking,

¹⁹ Neal Kumar Katyal, "Criminal Law in Cyberspace", (2001) 149 *University of Pennsylvania Law Review* 1003.

²⁰ Best, P., Manktelow, R., & Taylor, B. (2014). Online communication, social media and adolescent wellbeing: A systematic narrative review. *Children and Youth Services Review*, 41, 27-36. <https://doi.org/10.1016/j.childyouth.2014.03.001>

²¹ *Reno v. American Civil Liberties Union*, 117 Supreme Court 2329 (1997)

²² Information Technology Act 2000, s 67B

²³ Indian Penal Code 1860, s 354A

²⁴ Indian Penal Code 1860, s 354D

²⁵ The Protection of Children from Sexual Offences Act 2012

cyber bullying, defamation, grooming, hacking, identity theft, online child trafficking, online extortion, sexual harassment, and privacy violations are all illegal under POCSO.

The International Centre for Missing and Exploited Children proposed six criteria to assess the efficacy of state laws for protecting children in its 2016 Global Review of Legislation on Child Pornography:

- i. Is there any national legislation specifically addressing child pornography?
- ii. Is there a definition for child pornography?
- iii. Are computer-assisted crimes punishable?
- iv. Is it illegal to simply possess child pornography?
- v. Are Internet service providers required to report suspected child pornography?
- vi. Are there any data retention requirements that force ISPs to keep digital user data in order to prosecute online criminal activity?

When measured against these criteria, Indian laws appear to be competent, but the issue for many Indian legal professionals and law enforcement officials is applying the law to prosecute violators. Due to variances in vocabulary and definitions, a lack of standard operating procedures and guidelines, and law enforcement agencies insufficient capacities, the existing legal laws do not provide enough protection to minors.²⁶

1. The Information Technology Act of 2000 and the Information Technology (Amendment) Act of 2008

They are the most important pieces of legislation that govern internet activities. The word “communication device” is used to refer to any device that can send text, video, audio, or image, such as cellphones, computers, iPads/tablets, gaming consoles, or other similar devices.²⁷ The 2008 modification increased the original law’s reach and clarified the scope of key provisions. Following are the examples of online offenses against children, according to the law:

- “Transmission and publication of obscene material in electronic form.
- Creating photos, text, collecting, searching, downloading, advertising, promoting, or distributing content that represents minors in an obscene or sexually explicit manner,

²⁶ Standard B, “What Is POCSO Act | POCSO Act News | POCSO Act Punishment | POCSO Act Summary” (*Business Standard*, 00, 2020) <<https://www.business-standard.com/about/what-is-pocso>> accessed June 17, 2022

²⁷ “Porn, Privacy, and Kids: Congressional Attempts to Make the Internet Child-Friendly.” *The New Atlantis*, no. 2, 2003, pp. 100–02. *JSTOR*, <http://www.jstor.org/stable/43152035>. Accessed 16 Jun. 2022.

or transmitting or publishing material depicting children in sexually explicit actions in electronic form;

- Inviting a kid or children into an online relationship for sexually explicit activities or in a manner that could offend a reasonable adult, or facilitating child abuse or recording own or others' abuse connected to a sexually explicit act with children in electronic form.²⁸
- Capturing, publishing, or sending photos of a person's private region with or without his or her consent as it breaches the individual's privacy
- Gaining unauthorized access to a computer, downloading or copying data (data theft), introducing a virus or causing damage with the intent to cause harm;²⁹
- Using someone else's password or electronic signature, cheating through personation and breaching confidentiality and privacy.³⁰

2. Constitution of India

The Indian government must make provisions for children in accordance with Article 15(3) of the Constitution.³¹ The state's policy is guided by Article 39 of Part IV of the Constitution, which mandates, among other things, that children are protected from abuse, are not coerced into activities below their developmental level for financial reasons, and are given the chance to grow up in an environment that is free of moral and material abandonment. In addition, the UN General Assembly's adoption of the Convention on the Rights of the Child (UNCRC) in 1989 mandates that all UN member states recognise the rights of children.

3. NPC (National Policy for Children), 2013

Despite the fact that online risks posed by ICT are an emerging threat to children's safety in India, the National Policy for Children (NPC) of 2013 makes no mention of them. The policy's broad parameters implicitly allow for measures to ensure that all children have equal access to opportunities through ICT, with appropriate safeguards.

Section 1.5: It reaffirms the government's commitment to a rights-based approach to resolving children's issues, both current and emerging.³²

²⁸ Deb, Abhijeet. "Cyber Crime and Judicial Response in India." *Indian Journal of Law and Justice*, 3 (2), Sep 2012, pp. 106-117. HeinOnline, <https://heinonline-org.gnl.u.remotlog.com/HOL/P?h=hein.journals/ijlj3&i=248>.

²⁹ Information Technology Act 2000 and Amendment 2008, and the Information Technology (Intermediaries guidelines) Rules 2011

³⁰ *Id.*

³¹ Constitution of India 1950

³² National Policy for Children 2013, s 1.5

Section 2.2: It also expresses the “State’s commitment to take affirmative measures – legislative, policy, or otherwise – to promote and safeguard the right of all children to live and grow in equity, dignity, security, and freedom, particularly those who are marginalized or disadvantaged; to ensure that all children have equal opportunities.”

Section 4.12: It emphasizes the importance of a proactive and responsive child protection system, as well as preventive and punitive actions against all forms of exploitation and abuse.³³

Section 4.13: It focuses on access to redress mechanisms. The protective requirements call for a holistic and comprehensive approach to addressing the issue of child’s online safety.

Section 4.14: “The State has the primary responsibility to ensure that children are made aware of their rights, and that they are provided with an enabling environment, opportunities, and support to develop skills, form aspirations, and express their views in accordance with their age, level of maturity, and evolving capacities, so that they can be actively involved in their own development and in the development of others.”³⁴The policy does not specifically address the threat posed by online risks to children all matters concerning and affecting them.

4. National Cyber Security Policy, 2013

The National Cyber Security Policy, 2013’s mission, aims, and provisions address aspects of cybercrime prevention, investigation, and prosecution. Advocacy is needed to ensure that the government’s new National Education Policy clearly targets the ways and means of decreasing possible hazards and harm to children through ICT, particularly cybercrime against children. It underlines the need for law enforcement authorities to improve their capacity and capabilities in order to investigate cybercrime and acquire essential data for punishment.³⁵

Section 11³⁶ focuses on enhancing law enforcement capacities and enabling effective cybercrime prevention, investigation, and prosecution through appropriate legislative intervention.

Section 12³⁷ stresses the formation of a cybersecurity and privacy culture that enables responsible user behavior and actions. In addition, Section D, which focuses on enhancing the

³³ National Policy for Children 2013, s 4.12

³⁴ National Policy for Children 2013, s 4.14

³⁵ Sharma D and others, “Data Privacy: Need for Stronger Laws | SCC Blog” (*SCC Blog*, September 1, 2020) <<https://www.sconline.com/blog/post/2020/09/01/data-privacy-need-for-stronger-laws/>> accessed June 17, 2022

³⁶ National Cyber Security Policy 2013, s 11

³⁷ National Cyber Security Policy 2013, s 12

regulatory environment, calls for frequent audits and evaluations of the security of information infrastructure's sufficiency and efficacy.³⁸

5. The Personal Data Protection Bill of 2019

The public authority postponed its first The Personal Data Protection Bill, 2019 in the Parliament in December 2019 after a lengthy delay. Individual information assurance is a charge that aims to protect an individual's personal information and the foundation of an information insurance expert for the same. The management of personal information and sensitive individual information of children is regulated in "Chapter IV of the Personal Data Protection Bill". The personal data protection measure was postponed in parliament in December 2019, and the Covid-19 pandemic struck the Indian region in January, thus the bill is currently in limbo. It will be presented to the "Parliament" once more, accompanied by official consent, in order to become an enactment.

A NEW DATA PRIVACY LAW IS ON THE WAY

In contrast to current privacy laws, the new proposed data protection framework of the Personal Data Protection Bill, 2021 ('the Bill') requires extensive privacy compliances for children's data. The Bill would harmonize Indian privacy rules with other Indian regulations by providing additional safeguards for minors.

The bill is based on the General Data Protection Regulation ('GDPR'), with a shift toward risk-impact regulation, in which certain activities will be regulated more closely based on their potential impact. Before processing a child's data, a data fiduciary must verify the child's age, according to the bill. It also requires that the parent/approval guardians be obtained prior to the collection of the child's data. Data processing activities that profile children, monitor their behavior, or target advertisements at children are also prohibited.

VIII. SUGGESTIONS AND RECOMMENDATIONS

- 1) Children's online privacy is protected by distinct legislation in developed countries such as the United States of America and the People's Republic of China. However, the proposed bill only mentions the protection of children's right to online privacy in a small section. Before the bills are enacted, the flaws mentioned above must be addressed.
- 2) It is necessary to indicate the right age verification procedures employed by data fiduciaries to validate the age of children.

³⁸ Jha A, "Cyber Law in India: Women & Children As Prone Targets - Getlegal India" (*Getlegal India*, December 9, 2021) <<https://getlegalindia.com/cyber-law-in-india/>> accessed June 17, 2022

- 3) The data fiduciary must be brought under the scope of the Act, which prohibits guardian fiduciaries from profiling, tracking, or monitoring the data of children.
- 4) The term “sensitive data” used in part IV of the Act needs to be defined broadly.
- 5) However, if the government had introduced a separate bill to protect children’s internet privacy that would have been a greater start.
- 6) The importance of providing victims of cybercrime with effective, efficient, and child-friendly remedies cannot be overstated. The establishment of support lines, awareness programmes, and hotlines can all be valuable in this regard. It is also vital to create an environment in which children feel believed and protected, in addition to providing appropriate support methods.
- 7) There is a scarcity of research in India on the short, medium, and long-term effects of the digital environment on children’s well-being and rights. Schools, as well as parents and guardians, need to be more informed. Cybercrime reporting should be encouraged.
- 8) The COVID pandemic brought to light the enormous challenge of universal digital inclusion, particularly in the context of children’s education. Digital exclusion was found to be both a cause and a consequence of a lack of or limited access to digital devices and connectivity, with long-term consequences. For dealing with situations where both access to education and digital inclusion are critical, policy guidelines are required.
- 9) Laws governing digital security and data protection must be reviewed on a regular basis.

IX. CONCLUSION

Children must be shielded against the negative effects of internet use since they are sensitive and impressionable. As a result, it is critical that we guide our children to adulthood through safe waters in an increasingly interconnected world that presents new challenges of the digital age. Cyberbullying, cyber sexual harassment, cyber grooming, privacy invasion, and enticement to illegal behavior are just a few of the dangers. Because an increasing number of children are using social media to document and share their lives through images and videos, specific policies and processes are needed to monitor children’s online activities, limit risks and vulnerabilities, and keep them safe.

Although “the information age has brought forth different types of citizens with distributed responsibilities and different perspectives, the accompanying challenges are concerning, particularly for children, necessitating the need to protect them. However, due to the digital nature of children, limiting online time as a means of preventing cyber victimization and

cyber bullying is practically impossible. As a result, it is critical to establish methods that will pique the interest of children.”

There are numerous dangers involved with the internet that are incomprehensible even to grownups. As a result, minors who lack that maturity are more vulnerable to cybercrime or other forms of undue liability. The concept of technological contracts and parental control systems were developed in response to the difficulties associated with children using the internet. The vast and important scope of internet kid protection necessitates child-safety legislation and methods. It is critical to ensure a thorough grasp of the problem, promote the child’s best interests, and provide appropriate recovery services for cybercrime victims.
