International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 123-126 www.ijaem.net ISSN: 2395-5252

Protection of Children in Cyber Space

Dr. Kasturi Bora, Ms. Upasana Bora
Assistant Professor, NEF Law College, Guwahati, Assam
Student, NEF Law College, Guwahati, Assam

Date of Submission: 05-11-2020 Date of Acceptance: 18-11-2020

ABSTRACT: The Internet has changed the way we communicate, learn and live by opening up our world to endless possibilities. We can now see the world without leaving our home, learn without books and even meet people from all over the world without actually seeing them. However, with all the good that the Internet has to offer, we have to also be aware of the dangers that lurk within. As parents and guardians, it is our responsibility to ensure that children can safely access the Internet and its valuable resources without fear of falling prey to unscrupulous predators in cyberspace. This paper highlights the dangers and threats children face online and also suggests ways to keep kids safe online.

Keywords: Online games, internet, protection, cyber security.

I. INTRODUCTION

Cyberspace is a new social environment that is distinct and yet can encompass all the physical places in which people interact. The protection of children and young people in this environment is as essential as in any other location. But there are special challenges: Identifying potential harms, understanding the perspective of young people, and enacting practical measures to assure children of their right to protection. Violence against children and young people in cyberspace is a new phenomenon that will continue to affect more children and young people across diverse locations unless safety planning is built into the structure of the so-called new information society. Violence and harms against children and young people in cyberspace and in relation to new technologies include:

- The production, distribution and use of materials depicting child sexual abuse.
- Online solicitation or ‘grooming’ (securing a child’s trust in order to draw them into a situation where they may be harmed).
- Exposure to materials that can cause psychological harm, lead to physical harm, or facilitate other detriment to a child.
- Harassment and intimidation, including bullying.

Children and young people of all social classes risk confronting any or all of these forms of violence as they occur in relation to new technologies. The likelihood of harm can be expected to increase if forethought for the interests of children is not provided for in development planning, especially planning aimed at promoting new information and communication technologies (ICTs) and resolving inequities in access to them. At risk are children and young people who currently use new ICTs and those who will do so in the future. As well, children who do not have access to the latest communications devices also may be subjected to influences arising from their usage. These children are made the subjects of photos that are then sent into cyberspace, or they are advertised online as commodities, and/or they are affected by violence and harms arising from other people’s online interactions, including the use of pornography (depicting adults and/or children).

Some children are especially at risk due to a range of vulnerability-enhancing factors common to all environments. They are in socially and economically difficult situations, they have already experienced harm such as sexual abuse and exploitation, they are lonely, they feel alienated from their parents and others, they have low self-esteem, and/ or they lack confidence. Gender is also seen to be a risk factor, with seemingly more girls than boys appearing to be harmed through cyberspace interactions (although boys are increasingly featured in pornographic images circulating online).

EVOLVING TRENDS: EARLY WARNING

The scale of violence against children in virtual space is closely related to the rapid expansion of ICTs since the early 1990s when the emergence of web browsers triggered the Violence against Children in Cyberspace 11 Internet boom. The take-up of new ICTs has occurred unevenly according to the economic circumstances and location of communities. Now, the unfolding convergence between the Internet and mobile phones, however, will envelop diverse societies rapidly. Children and young people, who are commonly in the vanguard of those who quickly make use of new ICTs – the Internet and World Wide Web, mobile phones, digital cameras, web-cameras, and online and offline electronic games – can be expected also to embrace convergence. Some important emerging trends include:

Phones and 3G/ 4G/ 5G

The convergence between the Internet and mobile phones (made possible by 3G/ 4G/ 5G technology) is making and will continue to make a profound difference to the ways in which children and adults alike enter into cyberspace. Until recently, entry into cyberspace required access to fixed phone lines and computers.But now, a phone – and also the newer handheld games consoles – will provide access to cyberspace from any location. Parents and guardians will find it more difficult, therefore, to supervise children and young people while they are online. Photo and video capabilities will permit phone users to transmit imagery even further afield than their personal call lists, and directly into cyberspace. Some businesses are seeking to implement measures to protect children when using phones, for example by installing age verification systems so that they will not easily be able to access pornography online (though adults may access it legally).

Online games

Online multiplayer interactive games are a boom business. This business, involving both fantasy game-playing and gambling sites, will be promoted and expanded greatly in the near future. Handheld games consoles with Internet capabilities will further promote virtual interactions. Online games potentially provide a new platform where children and young people will be exposed to solicitations and potentially harmful interactions with other people online. Social impact assessments from a child protection perspective appear not to be available.

Peer-to-peer exchanges

In recent years, most concern about protecting children in online interactions has focused on chat rooms. In light of recognition that adults have lured children from chat rooms into face-to-face meetings where the child has been assaulted or otherwise violated, some Internet businesses have adapted or closed chat room services. In the meantime, children and young people with access to the latest technologies have been moving into peer-to-peer exchanges, due to the availability of free software that encourages the sharing of music files and other materials. Peer-to-peer transmissions occur directly from one server to another without any tracking devices. This facility is also popular among people exchanging images of child sexual abuse. In addition, children and young people are increasingly opting to use instant messenger (IM) services. Social impact assessments on peer-to-peer usage appear lacking.

Internet cafes

Many children who do not own a mobile phone or computer still go online or play games through Internet cafes. Some prefer to use a cafe even if they have access to a computer at home or school. Concerns are rising in various locations about children looking for and downloading age-inappropriate, harmful or illegal materials while in these public places, as well as their unsupervised engagement in online interactions with unknown people. In some communities, local groups are lobbying for Internet cafes to be required to operate according to safety guidelines and to implement protection measures, including the use of software to filter and block pornographic and other offensive material, and to set up user registries. The impact of 3G/ 4G/ 5G convergence on Internet cafes remains to be seen.

Cyber Dangers And Threats Children Face Online

- **Cyber-bullying:** These days, children are open to bullying even while surfing the Internet. They can be tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another person online, which can affect their self-confidence and personal development.
- **Pornography:** With over 4 million pornography websites online, pornography is now both prevalent and easily accessible by children. While filtering programs and parental controls are getting better, many children are still at risk of viewing such images. Even worse is when children themselves are used and depicted as objects of sexual pleasure.
- **Violence:** It is shocking and disturbing to know the sheer range and volume of online violence that our children are exposed to, such as images of war, domestic abuse, bigotry, misogyny and other vicious attacks on others.
- **Racial abuse & hate:** The most common expression of racial abuse is through racist name-calling and its impact on children can be profound. The Internet has given us instantaneous global access which can promote greater communication, understanding and respect. However in some cases, this global reach makes it easier to spread racial abuse and hate.
- **Online gaming & addiction:** There is growing evidence that many children are developing an unhealthy addiction to spending time online, from Internet gaming to any online activity The dangers of such an addiction are an increased risk of health and social problems.
- **Online fraud & deception:** Children are usually targeted by fraudsters, as young people often don’t have the experience and knowledge to distinguish legitimate requests from fraudulent ones. Fraudsters can then use the knowledge gained from children online to steal, blackmail, terrorize and even kidnap.

WAYS TO KEEP KIDS SAFE ONLINE

- **Increase awareness:** Help ensure younger children know the basics of staying safe online by using techniques like online games and videos that will define computer terms (e.g., cyberbullying, netiquette, virus protection) to establish basic understanding.
- **Protect your kid’s identity:** Remind your kids never to give out personal information, such as name, home address, or telephone number, to anyone they don’t know through email, Twitter, Facebook, or in online chat rooms or bulletin boards. Talk with your children about the online risks of interacting with strangers through the computer and sending notes and pictures into cyberspace. Online games may help kids understand how to protect their personal information and the ramifications of stolen identity.
- **Protect your computer:** Regularly updating security software can protect your family against scammers, hackers, and other online threats that can compromise your computer system and, consequently, your family’s financial security and other private information. Using software security that automatically updates keeps your technology current and decreases the likelihood of picking up bad programs or malware.
- **Create unique passwords:** For online safety, tell your kids to use different passwords for every online account they have to help prevent others from accessing their personal information. Make sure that you monitor each account and make sure your children know that strong passwords should include elements like symbols, numbers, uppercase and lowercase letters, and no names or words that others could easily guess.
- **Monitor online activity:** Monitoring your kids’ online activity can help keep them safe. Explore various parental controls and consider what options may work best for you and your family.
- **Prevent cyberbullying:** Cyberbullying—bullying using electronic technology—can happen anytime and anywhere. Teach your children to think through what they post on the Net about other people and the consequences those posts could have if they are unkind or mean. Also, keep communication with your child open and speak up if you suspect someone is bullying him or her.
- **Promote appropriate online interactions:** Use some online games to help show kids how to make responsible decisions about online communication and learn about key issues of digital citizenship. Online activities can include exploration of methods of communication in chat rooms and emails, for example.

II. CONCLUSION

The harms done to children and young people within and via virtual settings constitute acts of very real violence and have physical world consequences. This violence, ranging from involvement with online materials depicting sexual abuse of children to cyber bullying, emerges as a result of or is influenced by new forms of social interaction occurring within a wholly new environment, commonly known as cyberspace.

As governments, business entities and civil society plan and pursue the development of a global information society, cyberspace will be in reach of very many more people very soon. More children and young people will be at risk, therefore, unless action is taken to provide greater protection in all quarters. Preventing violence against children and young people in cyberspace requires acknowledging the violence being done now, acting against it, and Conclusion taking responsibility to develop more than ad hoc responses.

A range of actors has responsibility and a duty to act to safeguard children and young people: Governments, private sector entities, international agencies, civil society, parents and families, and young people themselves. Many people and organisations acknowledge this responsibility and are working on positive actions to address the issue. But the approach is fragmented and often territorial, and risks permitting an exponential increase in technology-facilitated violence against children in all parts of the world. Strong collaboration and cooperation across local, national and international levels is urgently required.

Effective actions need to be implemented across all the physical settings in which children operate – in families, schools, institutions and other settings – while taking note of a child's own agency in relation to cyberspace and other new ICTs. In addition, the character of the virtual environment, as outlined in this report, means that children and young people may be better informed on several issues, including topics with which adults may prefer they did not engage.

Of course, new ICTs are not inherently harmful. But they may be used in ways and for purposes not considered in their initial development. Foresight and decisive planning and strategising on the part of decision and policy-makers in all sectors will help to address this. These individuals and entities indeed have a responsibility to factor in the welfare of children, not as consumers but as holders of rights entitled to protection. The World Summit on the Information Society (WSIS), for example, has an important role to play in centralising the safety and rights of children and young people as its participants work to bridge the digital divide between societies.

The incorporation of a child-rights mindset into the structures of decision and policymaking would then provide greater assurance of seeing children and young people enjoy only the benefits of new ICTs and cyberspace.

REFERENCES

1. https://www.ecpat.org/wp-content/uploads/2016/04/Cyberspace_ENG_0.pdf
2. https://www.childprotectionindia.com/cyber-threats-children-face-online.php
3. https://www.itu.int/council/groups/wg-cop/first-meeting-march-2010/Malaysia-%20COP-WTISD_Eng.pdf