

Cybercrime and Cyberbullying Targeting Minors

Vinit Dhage^{1,*}

Abstract

Cybercrime and cyberbullying aimed towards minors are severe concerns that may have long-term effects for young people. Cybercrime refers to illegal crimes carried out through digital technology, such as hacking, phishing, or identity theft. Cyberbullying is the use of digital technology to harass, degrade, or intimidate another person. Children and teens are especially susceptible to these sorts of online abuse because they have less experience accessing the internet and may be unaware of the hazards connected with sharing personal information online. Cybercrime and cyberbullying may cause mental misery, social isolation, and, in rare circumstances, physical injury to adolescents.

Keywords: Cybercrime, hacking, cyberbullying, minors, emotional distress

INTRODUCTION

Cybercrime and cyberbullying are serious issues that can have a devastating impact on minors. With the widespread use of the internet and social media, it has become easier for perpetrators to target vulnerable children and adolescents. Schools and community organizations can also play a role in preventing cybercrime and cyberbullying by promoting digital literacy and cyber safety education. This can include teaching students about online privacy and security, responsible social media use, and the risks associated with sharing personal information online.

It is important to take cybercrime and cyberbullying targeting minors seriously and to take steps to prevent and address these issues. This can help to ensure that young people are able to use digital technology safely and responsibly and to protect them from the potential harms associated with online abuse.

Cybercrime is any criminal activity that involves the use of the internet or computer technology. This can include identity theft, hacking, phishing scams, and online harassment. Cyberbullying, on the other hand, involves the use of digital communication tools to bully, intimidate, or threaten another person. Minors are particularly vulnerable to cybercrime and cyberbullying, as they may lack the knowledge and skills to protect themselves online. It is essential for parents, educators, and other responsible adults to educate children about online safety and to monitor their online activity.

Preventing cybercrime and cyberbullying targeting minors requires a collaborative effort between individuals, government agencies, and technology companies. Governments can enact laws to deter cybercriminals and impose harsh penalties on those who target minors. Technology companies can develop tools and software that make it easier for parents and guardians to monitor their children's online activity and prevent access to harmful content.

*Author for Correspondence

Vinit Dhage
E-mail: Vinitdhage@nlunagpur.ac.in

Student, Faculty of law, Maharashtra National Law University,
Nagpur, Maharashtra, India

Received Date: March 04, 2023
Accepted Date: April 22, 2023
Published Date: May 02, 2023

Citation: Vinit Dhage. Cybercrime and Cyberbullying Targeting Minors. National Journal of Cyber Security Law. 2023; 6(2): 1–11p.

RESEARCH METHODOLOGY

The paper has been completed using the doctrinal method, with the research conducted with the

assistance of secondary sources made available to the researcher. The major source of information used for the research is the internet. The accessibility of technology has enabled the students to access relevant facts and has also provided them a wide scope of availability of research material. Data base made available by the university have been referred and have been a very useful help in finding about the topic.

AIM AND OBJECTIVES

- To analyse Cyberspace and Cyberbullying.
- To understand threat on minors.

Scope And Limitation

The limitation of the study is limited to Indian and US foreign point of view on cybercrime and cyberbullying targeting minors. the researcher chose to design the study and/or the method used to establish attention towards security of minors.

Doctrinal method of research is method in which past research and evidence are checked to come to a conclusion thus it does give a large quantity of material, but different theories exist for the same event which hinders the research at time. The scope is limited till the aim and objective set by the researcher. This makes the research limited but with a vast area to study about. This limitation is due to time limit also the resources available for the project.

Research Questions

- What is meant by Cybercrime and Cyberbullying?
- Legal perspective of Cyberbullying?

WHAT IS CRIME?

Crime is an act or behaviour that is considered illegal and punishable by law. It is an action that goes against the norms and values of society and has negative consequences for individuals or communities. Crimes can range from minor offenses such as traffic violations and petty theft, to serious offenses such as murder, rape, and terrorism. The specific definition of crime varies depending on the jurisdiction and legal system, but in general, it involves a violation of laws or regulations that are put in place to protect individuals and society as a whole.

WHAT IS CYBERCRIME?

Cybercrime refers to criminal activities that are committed using or targeting computer systems, networks, or digital devices. It involves the use of technology to carry out illegal activities or to facilitate unlawful acts. Cybercrime encompasses a wide range of activities, including hacking, identity theft, financial fraud, data breaches, cyber espionage, ransomware attacks, phishing, online harassment, and more. The proliferation of the internet and the increasing reliance on technology in our daily lives has made cybercrime a significant global threat that impacts individuals, businesses, governments, and society at large.

One of the most common types of cybercrime is hacking, which involves gaining unauthorized access to computer systems or networks. Hackers may exploit vulnerabilities in software, hardware, or networks to gain unauthorized access and steal sensitive information, disrupt operations, or cause damage. Hacking can be motivated by various factors, including financial gain, activism, espionage, or simply the thrill of illicit activities.

Another prevalent form of cybercrime is identity theft, wherein criminals steal personal information, such as social security numbers, credit card numbers, or login credentials, to impersonate individuals and commit fraud. This can result in financial losses, damage to credit scores, and reputational harm. Phishing, a type of social engineering attack, involves tricking individuals into revealing their personal

information through deceptive emails, messages, or websites. Cybercriminals may also use malware, such as viruses, worms, or trojan horses, to gain unauthorized access, steal information, or control compromised systems.

Financial fraud is another common form of cybercrime, involving schemes such as online scams, investment fraud, credit card fraud, or cryptocurrency fraud. Cybercriminals may use fake websites, emails, or advertisements to deceive victims and steal their money. Data breaches, wherein criminals gain access to sensitive information from databases or systems, are also prevalent. This can result in significant financial losses, reputational damage, and legal liabilities for affected individuals or organizations.

Cyber espionage, often carried out by nation-states or state-sponsored actors, involves stealing sensitive information from governments, businesses, or individuals for political, economic, or military purposes. Ransomware attacks have also become a widespread form of cybercrime, wherein criminals encrypt victims' data and demand a ransom for its release. This can cause severe disruptions to businesses, critical infrastructure, and individuals' lives.

Online harassment, stalking, bullying, and extortion are forms of cybercrime that target individuals and can have serious psychological and emotional impacts. Cybercriminals may use social media, online forums, or other digital platforms to harass, threaten, or blackmail victims. Additionally, cybercrime can also encompass illegal activities such as online trafficking, spreading hate speech or extremist content, and spreading malware or viruses for malicious purposes.

The financial impact of cybercrime is staggering. According to estimates, the global cost of cybercrime is projected to reach trillions of dollars by 2025. The costs include financial losses from stolen money, intellectual property theft, business disruption, legal fees, and reputational damage. Cybercrime can also have far-reaching societal consequences, such as erosion of trust in digital technologies, loss of privacy, and impacts on economic growth and innovation.

Efforts to combat cybercrime involve various stakeholders, including governments, law enforcement agencies, private sector organizations, and individuals. Governments around the world have enacted laws and regulations to address cybercrime and enhance cybersecurity. Law enforcement agencies collaborate across borders to investigate and apprehend cybercriminals. Private sector organizations invest in cybersecurity measures, such as firewalls, encryption, multi-factor authentication, and employee training to protect against cyber threats. Individuals are also encouraged to practice good cyber hygiene, such as using strong passwords, keeping software up to date, being cautious with online communications, and being aware of potential cyber threats.

Analog and digital crime share many continuities. Both types of crime involve illegal activities that are committed with the intent of causing harm or obtaining some kind of benefit, and both types of crime are subject to prosecution and punishment under the law.

Some specific continuities between analogue and digital crime include:

Theft

One of the most basic forms of crime is theft, which involves taking property that belongs to someone else without their consent. In the analogue world, theft can involve stealing physical objects, such as money, jewelry, or cars. In the digital world, theft can involve stealing information, such as personal data, financial information, or intellectual property.

Fraud

Fraud involves deceiving someone in order to gain something of value. In the analogue world, fraud can take many forms, such as mail or phone scams, counterfeit money or goods, or identity theft. In the

digital world, fraud can involve phishing, social engineering, or other tactics that exploit vulnerabilities in computer systems or networks.

Cyberbullying

Cyberbullying is a form of bullying that takes place online or through digital communication channels. It can include harassing or threatening messages, posting embarrassing or private information, or spreading rumours or lies about someone. Although cyberbullying is a relatively new phenomenon, it shares many similarities with traditional forms of bullying, such as harassment and intimidation.

Hacking

Hacking is the unauthorized access, manipulation, or exploitation of computer systems, networks, or digital devices, often with the intent of gaining unauthorized access to data, disrupting operations, or committing other illegal activities. Hackers are individuals who possess technical expertise in computer systems and use their knowledge to breach the security measures of computer systems or networks for various purposes, ranging from financial gain and personal gratification to political activism and espionage.

Cyberstalking

Cyberstalking involves using the internet or other digital communication channels to stalk or harass someone. It can include sending threatening messages, monitoring someone's online activity, or using technology to track someone's location. In the analogue world, stalking can involve following someone in person, making threatening phone calls or letters, or vandalizing someone's property.

Cybercrime Against Minors

Cybercrime against minors, also known as "online child exploitation", refers to any illegal activity involving the use of technology that targets children under the age of 18 [1]. It is a type of crime that is committed using a computer or the internet. Cybercriminals often target minors because they are more vulnerable and less aware of online threats. This can include online sexual exploitation, cyberbullying, sexting, grooming, child pornography, and other forms of abuse and exploitation.

Some common types of cybercrime against minors include:

- *Online sexual exploitation*: This includes the use of technology to sexually exploit or abuse minors, such as through online grooming or soliciting sexual content from them.
- *Cyberbullying*: This refers to the use of technology to harass, intimidate, or humiliate minors, often through social media platforms or messaging apps.
- *Sexting*: This involves the sharing of sexual content (such as photos or videos) among minors or between a minor and an adult.
- *Grooming*: This refers to the use of online communication to build trust and emotional connections with minors, often with the intention of sexually exploiting them.
- *Child pornography*: This involves the creation, distribution, or possession of images or videos depicting child sexual abuse.
- *Cyberstalking*: This is when someone repeatedly contacts, follows, or harasses a minor online.
- *Identity theft*: This is when someone steals a minor's personal information (such as their name, address, or social security number) with the intention of committing fraud.
- *Online scams*: This is when someone tricks a minor into giving them money or personal information by pretending to be someone they're not.

Cyberbullying Against Minors

Children and teenagers are often targets of cyberbullying because they are more vulnerable to the effects of online abuse and less likely to know how to defend themselves. The impact of cybercrime on children's mental and emotional health may be profound and long-lasting. The best way for parents,

teachers, and cops to keep kids safe online is to teach them how to be safe while using the internet, keep tabs on what they do online, and report anything suspect to the proper authorities.

PREVENTION AND RESPONSE

Prevention and response are key to addressing cybercrime and cyberbullying targeting minors. Parents and guardians may help keep children safe online by limiting their access to inappropriate content, keeping tabs on what their kids are doing on the internet, and teaching them basic safety precautions. In addition, schools and community organizations can provide resources and support for children and families affected by cybercrime and cyberbullying.

Reporting of Cybercrime

It is essential to report instances of cybercrime and cyberbullying targeting minors to the appropriate authorities. This can include law enforcement, internet service providers, and social media platforms. Reporting helps to hold perpetrators accountable and can prevent future incidents from occurring.

Cyberbullying targeting minors is a growing problem in today's digital world, and raising awareness about it is crucial. Cyberbullying refers to the use of digital technology, such as social media, texting, and messaging apps, to harass, intimidate, or bully someone. It can take many forms, including name-calling, spreading rumours or lies, sharing embarrassing photos or videos, and threats of physical harm. Here are some response measures:

Report Incidents

If a minor experiences cybercrime, it should be reported to law enforcement or relevant authorities. Parents and guardians can also report incidents to their child's school or the platform where the incident occurred.

Seek Support

Victims of cybercrime may experience emotional distress, and it's important to seek support from mental health professionals or support groups.

Preserve Evidence

Collect and preserve any evidence of cybercrime, such as screenshots, messages, or images, as this can be useful for law enforcement investigations.

Take Legal Action

If the cybercrime is severe or continues, legal action can be taken against the perpetrator.

Block and Report

Minors should be taught how to block and report any suspicious or inappropriate behaviour online to help prevent further incidents.

Step to be Taken for Spreading Awareness

Cybercrime against minors, such as cyberbullying, online child sexual exploitation, and grooming, is a serious problem that can have lifelong consequences for the victims. Here are some prevention and response measures that can help protect minors from cybercrime:

Talk Openly About Cyberbullying

Parents and caregivers should have open and honest conversations with children about the risks and consequences of cyberbullying. They should encourage children to speak up if they experience or witness cyberbullying.

Set Rules and Boundaries

Parents and guardians should monitor their children's online activities, including social media accounts and messaging apps, to identify any signs of cyberbullying or online grooming. This includes limiting screen time, monitoring online activity, and prohibiting the use of technology during certain times, such as at bedtime.

Monitor Online Activity

Parents and caregivers should monitor children's online activity regularly. They can use parental controls and monitoring software to keep an eye on their children's online behaviour.

Teach Children How to Respond

Children should be taught how to respond to cyberbullying, including blocking the bully, reporting the incident to a trusted adult, and keeping evidence of the cyberbullying.

Use Parental Control Software

Install parental control software on devices used by minors to block inappropriate content and limit access to certain websites or apps.

Seek Help When Necessary

If cyberbullying is severe or ongoing, parents and caregivers should seek help from a mental health professional or law enforcement.

By raising awareness about cyberbullying targeting minors and taking steps to prevent and address it, we can create a safer and more supportive online environment for all children.

INTRODUCTION OF INFORMATION TECHNOLOGY ACT 2000

The Information Technology (IT) Act, 2000 [2] is a body of Indian legislation addressing issues of online business, government transparency, and criminal activity. The Act provides for the prevention and response of cybercrime through several provisions.

Scope of Act***Offences and Penalties***

The IT Act identifies various cybercrimes such as hacking, identity theft, cyberstalking, cyberbullying, etc., and prescribes punishments for such offences. The penalties range from imprisonment to monetary fines.

Cybercrime Investigation

The Act empowers law enforcement agencies to investigate and gather evidence in cases related to cybercrime. It also provides for the establishment of Cyber Crime Investigation Cells at the state level to handle such cases.

Cybercrime Reporting

The Act mandates service providers to report cybercrime incidents to the appropriate law enforcement agency. Failure to do so may result in a penalty.

Cybersecurity Practices

The Act also requires organizations to implement reasonable security practices and procedures to protect sensitive information. This includes the implementation of information security policies, risk assessment, security audits, and incident response plans.

Cyber Appellate Tribunal

The IT Act establishes a Cyber Appellate Tribunal to hear appeals against the orders of the Adjudicating Officer.

Overall, the IT Act provides a legal framework for the prevention and response to cybercrime in India. However, it is essential to note that preventing cybercrime also requires the collaboration of individuals, organizations, and the government to create awareness and implement best cybersecurity practices.

LEGAL PERSPECTIVE

Acts

Megan Meier Cyberbullying Prevention Act [3]

An adult masquerading as a young guy on “Myspace” cyberbullied 13-year-old Megan Meier until she committed herself in 2006. The law is named after Meier. The Megan Meier Cyberbullying Prevention Act would make it illegal to utilise any kind of electronic communication for the purpose of bullying, harassing, or intimidating another person.

Though it has been proposed in Congress since 2009, the measure has yet to become law. It would be illegal under the new rule to utilise electronic communication to “coerce, intimidate, harass, or cause substantial emotional distress to a person”. Violators could be fined and sentenced to up to two years in prison.

Supporters of the bill argue that cyberbullying is a serious problem that can have devastating consequences for its victims, and that federal legislation is needed to address the issue. Critics of the bill argue that it could infringe on free speech rights and that cyberbullying should be addressed at the state level rather than by federal law.

As of 2021, the Megan Meier Cyberbullying Prevention Act has not been passed into law, but several states have enacted their own laws to address cyberbullying. The act criminalizes the use of electronic communication to cause emotional distress to minors.

Tyler Clementi Cyberbullying Prevention Act [4]

The law was named after Tyler Clementi, a college student who died by suicide in 2010 after being cyberbullied by his roommate. The Tyler Clementi Cyberbullying Prevention Act is a federal law in the United States that was enacted in 2015.

The act amends the Higher Education Act of 1965 to require colleges and universities that receive federal funding to have policies in place to address and prevent cyberbullying. The policies must include procedures for reporting and responding to incidents of cyberbullying, as well as measures to protect the confidentiality of victims [5].

According to the legislation, cyberbullying is defined as “sufficiently severe, persistent, or pervasive” behaviour that creates a hostile learning environment and substantially disrupts a student's emotional well-being and academic performance.

The Tyler Clementi Cyberbullying Prevention Act also requires the Department of Education to issue an annual report on the incidence of cyberbullying on college and university campuses, as well as information on best practices for preventing and addressing cyberbullying.

Overall, the law aims to promote safe and respectful environments for students in higher education and to raise awareness about the serious harm that cyberbullying can cause. The act criminalizes the use of electronic communication to cause emotional distress to anyone, regardless of age.

India has Implemented the Information Technology Act, 2000 (IT Act), Which Addresses Cybercrimes Including Cyberbullying

Section 66A [6] of the IT Act, which criminalized the sending of “offensive messages” via a computer or other communication devices, was struck down by the Supreme Court of India in 2015 as it was considered vague and violated freedom of speech.

However, other provisions of the IT Act, such as *section 67 and 67A*, which criminalize publishing or transmitting obscene content and material containing sexually explicit acts, are still in place and can be used to address cyberbullying. Additionally, the Indian Penal Code (IPC) also provides for criminal liability for online harassment and stalking under Section 354D and 509.

These cases highlight the need for increased awareness about online safety, especially among minors. Parents, educators, and law enforcement agencies need to work together to ensure that children are safe from cybercrime.

In recent years, the Indian government has also taken steps to combat cyberbullying, including launching a web portal called "*cybercrime.gov.in*" to report cybercrimes, including cyberbullying. The government has also introduced guidelines for social media platforms to regulate and prevent cyberbullying on their platforms.

Case Laws

Here are some notable case laws related to cyberbullying against minors.

A.B.V. Bragg Communications Inc [7]

On the one hand, the case relied on finding a balance between open court principles and the freedom of the press. On the other hand, the argument focussed on protecting children's right to privacy and preventing sexualized forms of cyberbullying. In addition, B. argued that if her identity were not protected, "young victims of sexualized cyberbullying like her would refuse to proceed with their protective claims", and as a result, they would be "denied access to justice". In her dissenting opinion, Justice Abella said that "it is not merely a question of her privacy, but of her privacy from the relentlessly intrusive humiliation of Sexualized Online Bullying".

Amanda Todd Case

The Amanda Todd case is a tragic story of a young Canadian girl named Amanda Todd who committed suicide in 2012, she was just 15 at the time of incident. Cause of death was being bullied and harassed in online as well as offline.

Before her suicide, Amanda had posted a video on YouTube where she held up handwritten notes that described her experience of being cyberbullied, harassed, and physically assaulted by her peers. The video went viral and received widespread attention, drawing attention to the devastating consequences of cyberbullying and online harassment.

Amanda's story has become an alarm for online safety and anti-bullying campaigns. Her case has also led to changes in Canadian law, with the introduction of Bill C-13 [8], also known as the Protecting Canadians from Online Crime Act, which criminalizes the non-consensual distribution of intimate images, known as "revenge porn."

The Amanda Todd case serves as a reminder of the importance of educating young people about online safety and the need to take online harassment and bullying seriously. It also highlights the need for greater legal protections for victims of cyberbullying and online harassment.

The case brought attention to the issue of cyberbullying and led to the development of new laws and policies to address the problem.

Phoebe Prince Case

The Phoebe Prince case is a tragic incident that occurred in 2010 in South Hadley, Massachusetts. Phoebe Prince, a 15-year-old Irish immigrant, had arrived at South Hadley High School, where she rapidly became the victim of bullying and abuse from a gang of pupils.

The bullying reportedly began in September of 2009 and continued for several months, both in school and online. Phoebe was subjected to verbal abuse, threats, and physical intimidation, including having objects thrown at her. On social media, she also got harassing messages.

On January 14, 2010, Phoebe Prince took her own life, which was attributed to the ongoing harassment and bullying she experienced. Her death brought national attention to the issue of bullying and cyberbullying, and many states subsequently enacted laws to address the problem.

The case resulted in criminal charges against several of the perpetrators and helped to raise awareness about the serious consequences of cyberbullying. Students who had been involved in the bullying were charged with various crimes, including statutory rape, criminal harassment, and civil rights violations. Some were convicted and sentenced to probation and community service, while others had their charges dismissed or reduced in plea deals.

The Phoebe Prince case remains a tragic example of the devastating impact that bullying and cyberbullying can have on young people, and it has led to increased efforts to prevent and address these behaviours in schools and communities.

Unfortunately, there have been several cases of cybercrime against minors in India. Here are a few recent cases:

- In 2021, a 14-year-old girl from Delhi was allegedly blackmailed by a man who had obtained her private pictures. The man demanded money and threatened to make the pictures public if she did not comply.
- In 2020, a 16-year-old girl from Uttar Pradesh was allegedly kidnapped and sexually assaulted by a man she had met on social media. The man had posed as a 19-year-old and had convinced the girl to meet him in person.
- In 2019, a 15-year-old girl from Maharashtra was allegedly raped by a man she had met on a social media platform. The man had promised to marry her and had convinced her to meet him in person.
- In 2018, a 13-year-old girl from Kolkata was allegedly lured into a hotel room by a man she had met on Facebook. The man had promised to buy her gifts and had convinced her to meet him in person.

Overall, cyberbullying against minors is a serious problem that has received increased attention from lawmakers and law enforcement officials in recent years. There have been many efforts to develop new laws and policies to address the issue and protect young people from harm.

CONCLUSION

In conclusion, it is important to recognize the seriousness of cybercrime and cyberbullying targeting minors and take steps to prevent them. In conclusion, cybercrime is a complex and evolving threat that poses significant challenges to individuals, businesses, governments, and society at large. With the increasing reliance on technology and the interconnectedness of our digital world, cybercrime has become a pervasive global issue that requires concerted efforts to combat.

One of the key challenges of cybercrime is its constantly evolving nature. Cybercriminals continuously develop new techniques, tactics, and tools to exploit vulnerabilities in technology and human behaviour. They may target individuals, businesses, or governments with varying motives, ranging from financial gain and political agendas to personal vendettas and sheer thrill-seeking. Cybercrime has also become highly organized, with criminal networks and syndicates operating across borders and leveraging sophisticated methods to carry out their illegal activities.

The financial impact of cybercrime is staggering, with the costs reaching trillions of dollars globally. Businesses and individuals may face financial losses from stolen money, intellectual property theft,

ransomware payments, legal fees, and remediation efforts. The costs of cybersecurity measures, such as investing in robust defences, conducting investigations, and implementing cybersecurity protocols, also add to the financial burden. In addition, the reputational damage resulting from data breaches, financial fraud, or other cybercrime incidents can have long-term consequences for businesses and individuals alike.

Beyond financial losses, cybercrime also has broader societal impacts. It can erode trust in digital technologies, which are integral to modern life and the global economy. Data breaches can compromise personal privacy and lead to identity theft, resulting in long-term consequences for victims. Additionally, the proliferation of cybercrime has led to an increased need for skilled cybersecurity professionals, creating challenges in recruiting and retaining talent in this field.

Addressing cybercrime requires a multi-faceted approach involving various stakeholders. Governments play a critical role in enacting laws, regulations, and policies that aim to prevent, detect, and prosecute cybercrime. International cooperation and collaboration among law enforcement agencies are essential for investigating and apprehending cybercriminals who operate across borders. Private sector organizations, ranging from small businesses to large corporations, need to invest in robust cybersecurity measures to protect their systems, networks, and data. This includes implementing firewalls, encryption, multi-factor authentication, security awareness training, and incident response plans. Individuals also play a vital role in protecting themselves and their online presence by practicing good cyber hygiene, such as using strong and unique passwords, being cautious with online communications, and being aware of potential cyber threats.

It is a multifaceted and ever-evolving threat that poses significant challenges to individuals, businesses, governments, and society. It has financial, societal, and reputational impacts that require a multi-faceted approach involving governments, law enforcement agencies, private sector organizations, individuals, and technology innovations. Efforts to combat cybercrime need to be proactive, collaborative, and innovative to stay ahead of the evolving threat landscape and safeguard our digital world.

Overall, cybercrime and cyberbullying against children are important concerns that demand the attention and action of parents, carers, schools, and communities. We can help safeguard children and teens online by taking efforts to avoid, react to, and report these instances. We can build a safer online environment for our children and help them navigate the digital world with confidence and security by working together.

In addition to educating youngsters about safe online conduct, parents and educators may utilise monitoring and filtering software to assist prevent cybercrime and cyberbullying. These technologies may assist in blocking unsuitable information, limiting screen time, and providing notifications when questionable behaviour is found.

Finally, everyone must act together to avoid cybercrime and cyberbullying against youngsters. We can help safeguard the next generation from the damaging impacts of online crime and bullying by being aware and taking proactive efforts to encourage safe online conduct.

REFERENCES

1. United Nations Convention on the Rights of the Child. CRC/C/156: Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. Geneva, Switzerland: The Office of the High Commissioner for Human Rights, United Nations (OHCHR); 2019. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/268/13/PDF/G1926813.pdf?OpenElement>
2. The Information Technology (IT) Act 2000, Section 2, India.
3. H.R.1966, Megan Meier Cyberbullying Prevention Act. 111th Congress (2009-2010). <https://www.congress.gov/bill/111th-congress/house-bill/1966/titles>

4. Tyler Clementi Higher Education Anti-Harassment Act. Human Rights Campaign, 2021. <https://www.hrc.org/resources/tyler-clementi-higher-education-anti-harassment-act>
5. State of New Jersey v. Dharun Ravi. Superior Court in Middlesex County, New Jersey, USA. 2012. <https://law.justia.com/cases/new-jersey/appellate-division-published/2016/a4667-11.html>
6. The Information Technology Act, 2000, Section 66 (A), India.
7. A.B. v. Bragg Communications Inc., 2012 SCC 46 (CanLII), [2012] 2 SCR 567. <https://www.canlii.org/en/ca/scc/doc/2012/2012scc46/2012scc46.html>
8. Statutes of Canada 2014. Protecting Canadians from Online Crime Act. C-13 (Second Session, Forty-first Parliament), Parliament of Canada; 2014. <https://www.parl.ca/LegisInfo/en/bill/41-2/C-13>