



**INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW**

*An International Open Access Double Blind Peer Reviewed, Referred Journal*

---

Volume 4 | Issue 2

Art. 33

---

**2025**

**Children In Cyberspace**

Dhwani Goyal

---

**Recommended Citation**

Dhwani Goyal, *Children In Cyberspace*, 4 IJHRLR 494-508 (2025).  
Available at [www.humanrightlawreview.in/archives/](http://www.humanrightlawreview.in/archives/).

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto Media and Publications administrator. For more information, please contact [info@humanrightlawreview.in](mailto:info@humanrightlawreview.in).

---

# Children In Cyberspace

**Dhwani Goyal**

*Law Student, 5<sup>th</sup> Year,  
B.Com.LL.B., Banasthali Vidyapith, Rajasthan*

---

**Manuscript Received**  
06 Apr. 2025

**Manuscript Accepted**  
08 Apr. 2025

**Manuscript Published**  
10 Apr. 2025

---

## ABSTRACT

*The expansion in digital era has significantly impacted the child's mental health in various ways. Cyber space was introduced to facilitate the interaction, education and to grab opportunities at global level. The sudden surge in usage has lead to cyber crimes such as cyber bullying, sextortion, harassment and grooming. With the rapid growth in tech world, the platforms have gained recognition. With the passage of time the reel world has been exposed in to crimes and has destroyed the mental health of the vulnerable section of society.*

*Cyber bullying in today's time is the heinous offence of cyber space and has become an alarming issue, giving rise to depression, anxiety, and self harm in serious cases. In many situations it has given rise to suicides among children's. sextortion and cyber grooming has focused more on minors as they are easy to manipulate. Additionally, the harmful websites, dark webs are the hiding spots for cyber criminals.*

*This paper has tried to examine the risk children's face in cyber world. A comprehensive approach involving authorities, cyber security cell and society is effective to build a ethical environment for children in cyber space. The legal framework is must in order to curb these crimes. Moreover, the decision makers are required to introduced more strict provisions for the security of children's.*

*The study highlights the need for effective legal frameworks, awareness campaigns and equal efforts to safeguard the children in cyber threats and foster safe online sites. By adopting a secure approach, society can curb the crime and provide a health cyber environment to children's. The ethical environment which was the*

*dream before introducing internet can somehow be achieved if the decision makers focus more towards amending old provisions and altering the existing ones.*

### **KEYWORDS**

*Cybercrimes, Crimes, Children's, Cyberworld.*

### **INTRODUCTION**

In the twentieth century 'internet' has become an integral part of our daily lives. The development of technology has hyped-up to the extent that each and every site is just one click away. The advancement of technology through internet has undoubtedly provided many benefits to our society. The internet was introduced in people's life to make it hustle free and enjoy the various advantages from internet. In today's time internet is being used in every sector of the society including educational field, industrial field, and many others. Internet has changed the lives for good but 'everything comes with pros and cons'. Increasing the use of internet has also increased the use of cyber crimes. The technology has also provided varied tools to grow the child in cyberspace not educationally but also tech wise. Children's today are evolving their minds rapidly when it comes to tech knowledge. Cyber crime is the new legal issue. Cyber crime as per Information technology act, 2000 is 'an illegal behavior conducted through or on computers, the internet, or other technologies'. The crimes are committed through computers in today's world and misconduct which the criminals are causing to general public is unlawful and must be penalized for the same. The daily usage of internet has turned into the 'basic need' of people's life, the day-to-day activity is impossible without internet; this basic need has turned the criminals to use it against us.

India has the fastest growing netizens on internet and by every passing day more young and sharp minds are getting online. The speed of joining internet has raised the privacy concern as there is a lot of risk & threats associated in tech world. Children's using technology through internet can easily access to any information and many a times such information costs them passing their personal information to criminals. People fall in the trap of cyber-frauds and they are still children who are blind to such risks. Cyber criminals take it as an advantage and commit crimes against children in cyber world as they found them easy to manipulate. The child exploitation in cyber world has varied crimes such as "child trafficking", "cyber-grooming", & "cyber bullying".

## CYBER SPACE

Cyber Space is a word which is created using different components of computers such as internet enable devices as in routers, servers or many other components. The word '*cyberworld*' was first used 'Neuromancer' the science fiction of William Gibson in 1982. It is the novel which depict cyberspace as" the creation of a computer network in a world filled with artificially intelligent beings<sup>1</sup>."

Cyber space is an intangible domain that exists in digital world. The domain can't be touched but can be sensed and one has to accept the transactions happened in cyber world. Cyber space is interconnected to tangible world in different ways i.e. telephone, television or internet.

The impact of cyber space is very challenging. The cyber space is affecting children's in many different ways and the effects are very adverse. The internet offers n number of benefits and many different opportunities but it comes with many disadvantages. The cyber space land children's into trouble which they are not prepared for and due to such blind trust on internet and site they face to face many challenges.

## THE FAVORABLE OUTCOMES

- 1. Easily accessibility of Internet-** Nowadays, Internet is easily accessible in every corner of the world or the world is completely relied on Internet. Internet has given vast opportunities across all sectors and for every age people. Each information and material is now easily accessible and this has created a very easy learning process to children's and the one who are looking for it.<sup>2</sup>
- 2. Linkage-** Internet helps in connecting with people globally. This helps children's in fostering their connectivity, friendships, and cultural exchange.
- 3. Entertainment-** Cyber space provides countless platforms, including games, live streaming, reel content etc. These activities keep children's engaged in cyber world and helps in alleviating the pressure of physical world.
- 4. Learning Skills Development-** Cyber space has enable children to explore new activities through internet and has foster their interest in learning the reel content. This is the

---

<sup>1</sup> Cyberspace | Digital Communications & Security | Britannica, <https://www.britannica.com/topic/cyberspace> (last visited Apr 07, 2025).

<sup>2</sup> Dr Vishwanath Paranjape, Cyber Crimes and Law Book by Dr Vishwanath Paranjape - 2<sup>nd</sup> Edition.

new hobby in today's time and the Gen-Z generation is more into it and given them a new opportunity to explore the internet.

### NEGATIVE IMPACTS

- 1. Cyber Bullying-** Cyber space has given plethora of opportunities for communication but after all the pros it has many cons out of which one is cyber bullying. The cyber world has facilitated harassments and cyber bullying, making children their target as they are easy to manipulate. This may lead to mental agony, stress and even depression among children's. These negative impacts highlight the needs for awareness.
- 2. Privacy Concerns-** Children's are vulnerable and are not that aware about internet and the cons of internet. Many a times they do unknowingly click on sites and share their personal data which lead them to trouble. They may fall in the trap of malicious sites and compromise with their privacy.
- 3. Addiction-** The urge to develop tech knowledge or to explore internet has ended up with high screen time. The increased screen time has led to addiction, sleep deprivation and sluggish behavior.
- 4. Cyber world Predators-** They are the individuals who exploit children's or deceive them through internet. These predators target children's in exploit them sexually, trafficking, or sexual abuse.

### CYBER CRIMES

The term '*Cybercrime*' is an umbrella term where many unlawful activities are clubbed together. Cyber crime generally defined as an offense which took place through internet. The malicious website on internet is operated by predators and it possesses with different crimes. Cyber crime has no jurisdiction, as the internet allows criminals to operate remotely and commit an offense.<sup>3</sup>

The weapons through which these crimes are committed are internet and technology operated through computers. The predators are skilled in operating computers and have a thorough knowledge of tech and internet. Many crimes that are emerged through internet may include cyber-stalking, cyber-terrorism; child-pornography, email-spoofing, cyber-defamation, polymorphic virus, email bombing, and the list don't ends here. The prevention of cyber crime requires a robust measure such as

---

<sup>3</sup> Ishan Atrey, *Cybercrime and Its Legal Implications: Analysing the Challenges and Legal Frameworks Surrounding Cybercrime, Including Issues Related to Jurisdiction, Privacy, and Digital Evidence*, (2023).

cyber-security, effective legislation and innovative advancement in digital forensics.<sup>4</sup>

### **DEFINITION OF CYBER CRIME**

The Interpretation of cyber crime is not enacted in any statute, even the IT Act, 2000 does not contain any definition of cyber crime. In a layman language, cybercrime can be defined as any unlawful activity which is committed through internet falls under the ambit of cybercrime. The forgoing define of cybercrime states that there is a very thin line of division between conventional crime and cyber crime<sup>5</sup>. The '*sin qua non*' for cyber crime says that there should be an involvement at any stage, of the virtual cyber medium i.e. internet or computer.

A simple definition of cyber crime can be "unlawful acts wherein the computer is either a tool or target or both<sup>6</sup>. Thus, the crimes that are directed through computers and internet are considered as cyber crime.

Cyber crime as defined internationally by the U.N. Congress on prevention of cyber crime and treatment of offenders<sup>7</sup> is made up of two categories-

1. In a narrower sense, the cyber crime is any act which is illegal and is directed by illegal means and is directed by computer networks that attacks the security of computer system and database.
2. In the broader sense, cyber crimes include all the crimes that are committed through an internet. The illegal possession of information and distributing such information are stated under this part.

In the Indian context, cyber crime is an offense that is committed against an individual or person. The crime may affect the property and mental state of the person and such acts are punishable under IT Act, 2000 and Bhartiya Nyaya Sanhita, 2023. The crimes that are committed against individuals may include cyber defamation, theft, fraud and others. Such offences are performed

---

<sup>4</sup> Goyal Mohit, *Ethics and Cyber Crime in India*, 2 IJEMR 1-3 (2012).

<sup>5</sup> Ibid.

<sup>6</sup> Cybercrimes where computers is a target include sophisticated illegal activities such as unauthorized access to networks or computer system, email bombing, trojan attacks, data diddling, denial of service attack, internet time theft, logic bombs, virus or worm attacks.

<sup>7</sup> Tenth U.N. Congress on prevention of crime & treatment of offenders was held in Vienna on April 10-17-2000.

through different networking sites.

### **ESSENTIALS OF CRIME & CYBER CRIME**

“Every crime violates the law but every violation of law does not commit a crime.”<sup>8</sup> The crime is an unlawful act which is punishable under lawful authority. The crime is an offense that can destroy person’s well-being in many ways. Any act which is done to harm others must be voluntary and for which he should held liable.

To establish the criminal liability, prosecution beyond reasonable doubt has to prove-

- a) The soundness of mind of the accused while performing the offense.
- b) Any event which is done is unlawful in nature.

Thus, crime consist of two major principles i.e. ‘*Actus rea*’ & ‘*Mens rea*’. These two principles helps in defining the conventional crimes but crimes are crimes and how will these principles fall under the head of internet crime is a tricky question.

#### ***Actus rea-***

The term ‘*Actus rea*’ connotes ‘deed’ a tangible result of human conduct. The *Actus rea* includes every components of crime in its definition except the mental element. The well known definition of *Actus rea* is “such result of human conduct as the law seeks to prevent.”<sup>9</sup>

#### ***Actus Rea in Cyber Space-***

The act done through internet is comparatively quick to identify, but is not easy to substantiate. In order to prove the performance, the accused should be –

1. Making an effort to operate a device.
2. Trying to access the stored data.
3. Attempting to login even if there are failed attempts.
4. Using the internet for wrongful gain.

#### ***Mens rea-***

---

<sup>8</sup> Mariya Paliwala, *Constituent Elements of a Crime with the Special Emphasis on IPC*, iPleaders (Dec. 7, 2019), <https://blog.iplayers.in/constituent-elements-of-a-crime/> (last visited Apr 07, 2025).

<sup>9</sup> J.C. Smith & B. Hogan *Criminal law*, 6<sup>th</sup> Edition, 1998, Butterworth and company publishers Ltd., London, pp. 31 – 36.

The term '*Mens rea*' refers to 'guilty mind' or 'Intention.' The mental attitudes that are defined under this term are intention, recklessness, and negligence.<sup>10</sup> The term 'intention' signifies the mentality of the person while the conduct. The prior foresight is must to form an intention. There can never be an intention unless there is prior foresight, since a person who intends a particular act must have a prior anticipation of the act.

Before 12<sup>th</sup> Century, the accused can be held liable for harm simply because of the physical conduct. With the passage of time the interpretation gradually changed until the modern law came to regard a "guilty mind" of some or some other, such mental element as always being necessary.

### ***Mens rea in Cyber space***

To establish the element of *Mens rea* on the part of accused must be visible that, at the time of accessing computer the accused must be aware that the obtained access is unauthorized. It is the most vital element in establishing criminal liability. In cyber world to determine the *mens rea* there are vital ingredients such as digital traits, user action, and automated processes. The intent in cyber crime is challenging but it's the key element. The cybercriminals brings pseudonymity names to hide their identity. Behind the mask of pseudonymous identities, cybercriminals use VPNs, fake accounts and encryption to hide their true identity.

## **CRIMES AGAINST CHILDREN IN CYBER-WORLD**

The information technology has provided a vast scope to humans to enjoy the internet and exchange the information on internet. These numerous advancements has benefitted us but they have also given rise to type of crime i.e. cyber crime. The crimes that are unlawful are considered as cybercrimes. The criminals while committing crimes exploit the vulnerable class of society who are blind to the risk of internet. The cybercriminals are so advanced these days that they have left no scope of detection. The technology has been referred as 'double edge weapon', presenting us the advantages as well as disadvantages. The crimes are ranged from simple wrongful gain of information to freeing of virus into computer. A wie range of illicit activities may include hacking computers, disturbance in computers through malicious software, online fraud, phishing, identity theft etc.

The cyber offenders are makes the use of internet to harass the

---

<sup>10</sup> Kenny's Outlines of Criminal law, 18<sup>th</sup> Ed, 1962 Cambridge University press, Cambridge, Pp. 31-36.



individual or use their personal data against them. In most of the cases the victims of cybercriminals are children's and this may include-

1. Child pornography
2. Cyber grooming
3. Cyber bullying
4. Cyber stalking
5. Sexual Harassment
6. Camera Hacking

### **KINDS OF CYBER CRIMES**

**1. Child Pornography-** Child pornography is referred as “any optical depiction of sexually explicit conduct engaging a child.<sup>11</sup> The frequent use of technology has made the children's cyber victim. Child pornography is one of the distinct crimes where the young individuals are involved in sexual activities. It is the visual representation, either the minor is involved with an adult or the minors are involved in sexual intercourse. It is nothing more than exploitation of child, which has a straight negative impact on child's mind<sup>12</sup>. *J. Murlidhar*, “emphasized the lack of specific legislation governing the issue of child pornography and stated “India should develop a modernized legislation to fill up the gap between child pornography and appropriate punishment therein. And to this he has also added that this issue requires the utmost priority and concern”. After the amendment in 2008, the child-pornography was recognized and given the emphasis in legal world.

This offence may include-

- a) Making Child pornography available through computer connections;
  - b) Sharing child pornography videos online;
  - c) Storage of child pornography in computer system.
- 2. Cyber Grooming-** Child grooming in layman language refers to ‘scam in friendships’. This type of offense is committing by befriending an innocent on internet and fools them into illicit activity. There are various sources through which groomer's fool's innocents such as, chat rooms, games, pseudonym accounts, mails, or social media. The groomers obtain personal information through these sites and use against them in future. The blind trust on these

---

<sup>11</sup> Section 2(da), POSCO, 2012.

<sup>12</sup> Ibid.

sites lead them in trouble and the groomers act as per child's interest<sup>13</sup>

- 3. Cyber Bullying-** The bullying through mobile phones, or computers are laid down under cyber bullying. The constant use of internet to harass or threaten someone can be considered under this head. The major activity which is done under this offense is leaking any sensitive information about the person, can be humiliating. The reason behind cyber bullying can be jealousy, hatred or insecurity. The influence of internet may lead the adolescents into a wave of negativity. Cyber bullying can affect anyone irrespective of their knowledge<sup>14</sup>
- 4. Cyber Stalking-** As per Oxford's Dictionary, stalking is referred as "Pursuing Stealthily". Stalking refers to 'being constantly engaged towards a person.' It is kind of a pattern; a target focused behavior both legally and illegally<sup>15</sup> promoted by the person's who are narcissistic and delusional.

The cyber stalking may refer to 'web obsession'<sup>16</sup>. Since it does not involve any kind of physical interaction between the accused and victim, there is a basic perception that it is not a serious offence. Many behaviors such as threats, defamation, sexually harassing, or other activities intended to persuade or threaten their victim, may engaged.<sup>17</sup>

- 5. Sexual Harassment-** The harassment is a kind of abuse where a child is exposed in illicit content, the delivered texts and videos contains the sexual tone, exhibited body parts online, or used for pornographic purpose. There is no specific provision in India about sexual harassment, can be interpreted through the words "electronic' or 'digital'.
- 6. Camera hacking-** In the new age of technology, the scariest notion is hacker gaining the unauthorized access to individual's camera.<sup>18</sup> This offence can be committed where there is no security camera. It usually happens when the malware is downloaded without permission.

---

<sup>13</sup> Dr. Samir Bhadury, "Child pornography in India: issues & Challenges" 6 Journal of Positive School Psychology 6525 (2022).

<sup>14</sup> Rufia Mitsu Eman Dawood, "Cyber bullying: An Overview" 4 Indonesia Journal of Global Health Research 195 (2022).

<sup>15</sup> Ibid.

<sup>16</sup> Ibid.

<sup>17</sup> Michael L. Pittaro, "Cyber Stalking: An Analysis of Online Harassment and Intimidation: 1 International journal of Cyber Criminology 180 (2007).

<sup>18</sup> In.norton.com/blog/malware/webcam-hacking.

## WHAT ARE THE LEGISLATIONS ON CYBER CRIME?

As per Indian Context, the main instruments for penalizing the offenders for committing cyber crimes are the protection of Children from Sexual Offences (POCSO) Act, 2012, Information Technology Act, 2000, Bhartiya Nyaya Sanhita, 2023, The Digital Personal Data Protection, 2023 and National Cyber security Policy, 2013.

### **A) IT Act, 2000**

The IT Act, 2000 is the most major act that provides security towards internet activity. The statute contains many provision which deals with crime in cyber world, imposing penalties on an unauthorized act done through computer such as, phishing, cyber attacks, installing malware/virus etc. the statute contains a specific provision for the protection of children in cyber world i.e. Sec. 67B, “the punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in digital form, as

1. Whosoever, publishes or transfer any material containing sexual act, depicting children in unlawful activity.
2. Creates text or digital pictures or videos, collect, download or browse and distribute it through any electronic form.
3. Induce children in online relationship for the purpose of sexual activity or other obscene activities.
4. Promote child abuse
5. In any digital form, own abuse or that of others pertaining to sexually explicit with children, shall be punished with imprisonment or fine.

### OTHER PROVISIONS-

Sec. 66E<sup>19</sup>, states any “publication or transmission of an image of a private area of a person without the consent of such person is made punishable, if such image are captured under circumstances violating privacy.” The accused shall be punished with detention for a term of three years and, or with fine of upto 2 lakh.

Sec 66C<sup>20</sup>, it outlines the penalty for the one who explicitly misused the personal data, such as passwords, documents and other relevant information.

---

<sup>19</sup> Punishment for violation of privacy.

<sup>20</sup> Punishment for identity theft.

Sec 66D<sup>21</sup>, “any person who impersonates another by cheating for the purpose of establishing personal and sensitive information, shall be punished with imprisonment for a term which may extend to 3 years and shall be liable to fine which may extend to 5 lakh”.

### **B) POSCO ACT, 2012**

The act is enacted to protect the children below 18 years of age in 2012; children’s who are minor are needed to be protected from every sexual offence including, sexual harassment, assault, abuse, & child pornography. Section 11<sup>22</sup>, few instances involved electronic media are-

1. Whosoever, representing any sexual video or pornography video to the child with the intention of sexual intercourse would be deemed to have sexually harassed the child.
2. Individual who is constantly connected with a child and forcing him to commit any sexual activity.
3. Threatening a child through computer to use any body part against the child, can be fabricated.

The punishment or the same has been provided in Section 12, of the said act, “Any individual who commits the crime of sexual harassment faces a fine in addition to up to 3 years in jail”

Section 14<sup>23</sup>, it outlines the penalties for using a child for pornographic purpose.

Section 15<sup>24</sup>, “Any person, who stores, for commercial purposes any pornographic material in any form involving a child shall be punished with imprisonment or either description which may extend to 3 years or with fine or with both.”

### **C) DPDP ACT, 2023**

This new act has come into the light to bring advance protection in order to protect the child from being sexually harassed. The clause in this act states that, consent of parents must be given of the children’s who are below 18 years of age. The fiduciary data must get permission from the parents before processing the data. As per DPDP Act, to monitor the children’s

---

<sup>21</sup> Punishment for cheating by personating by using computer resource.

<sup>22</sup> Sexual Harassment, POSCO Act, 2012.

<sup>23</sup> Punishment for using child for pornographic purpose

<sup>24</sup> Punishment for storage of pornographic material involving child

data is against law and might cause danger to children's. It also suggests the data fiduciaries for mandatory registration of minors.

#### ***D) National Cyber Security Policy, 2013***

The main objective behind this is to aware general public about cyber security. It safeguards the data of the citizens and shields the privacy. The policy was enacted with plethora of goals, one was to protect the minors and investigate the cyber criminals.

#### ***E) Bhartiya Nyaya Sanhita, 2023***

Cyber crimes comprise of different offences, including acts of defamation and criminal intimidation. The punishments for which are provided under criminal law, "Promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc. and doing acts prejudicial to maintenance of harmony"<sup>25</sup>

"Tackles cheating by impersonation, stipulating imprisonment for up to 3 years, a fine, or both for offenders"<sup>26</sup>

Stalking is another offence, online stalking is a serious concern which can damage the mental health of a person. In most of the cases, women's are the victim of such offence. The punishment for the same is, "three years with fine for the first conviction and up to five years for subsequent convictions."<sup>27</sup>

### **GAPS IN INDIAN LEGISLATION**

Although crime against children is unlawful, India continues to witnessing a substantial amount of crimes in cyber world. With advance in technology and rapid evolution of technology, the percentage of such offences is increasing at alarming rate. In India, cyber bullying is a serious crime. However, absence of any specific provisions addressing cyber bullying and sexting, has lead to a serious issue of concern. Cyber bullying is carried out for exploitation.

The dual legal legislation of IT Act and POSCO Act needs to be altered, as –

---

<sup>25</sup> Sec. 196 of BNS, 2023.

<sup>26</sup> Sec. 319(2) of BNS, 2023.

<sup>27</sup> Sec. 78 of BNS, 2023.

1. Cross border agencies to receive actionable intelligence- The idea behind this plan will allow the local authority to share or connect intelligence across borders.
2. An amendment to POSCO Act, where there should be no legality to promote consensual activity with minors, any written document, audio recording or portrayal.
3. An amendment in IT Act, 2000 was amended to provide protective measures against the minors who are indulged in illicit activity or has obtain any unlawful information on child sexual abuse.

The Indian government has come up with several rights for the protection of children's in both real world and reel world. Unfortunately, we lacked the children's privacy right. To safeguard these rights few judgments are interpreted for the privacy of adolescents in this digital era.

In *Jayesh S. Thakkar v. State of Maharashtra*<sup>28</sup>, Chief justice of India on receiving letter from petitioner, stating the rise of pornographic websites on Internet, considered it as a writ petition. Thereafter, the CJ directed the formation of committee to formulate ideas for curbing such content, and ensuring that the protection of minors from such illicit websites.<sup>29</sup>

The SC of India and Kerala HC observed that, viewing pornography in the walls or privately is not an offence under 292 of penal code, downloading the same for children is illegal as per IT Act provisions.<sup>30</sup>

## CONCLUSION

The internet has given immense benefits to our society but it also has some unpredicted risk. In the digital era where the dependency is on internet, the crimes are hyping at alarming rates. A Cyber criminal exploits the vulnerable sections of society and harm them. The harm these innocent adolescents face are heinous in nature and can be varied depending upon situation, such as, cyber grooming, exploitation, harassment, sextortion etc.

With the legislation of India i.e. POSCO Act, 2012, IT Act, 2000, helps the victims in filling the voids. The lack of few provisions can risk the child's privacy and they can be suspected as

---

<sup>28</sup> Writ Petitioner No. 1611 of 2001.

<sup>29</sup> Ritu Chhabra and Dr. Sushil Kumar Singh, "Rights of Children in Cyber World: Indian Perspective" 43 *Sambodhi* 21 (2020).

<sup>30</sup> Gursimran Kaur Bakshi, "watching porn privately is not an offence".

mistreated.

Dealing this issue needs major concern from the decision makers, law enforcement agencies, tutors and civil organizations. By bridging the gap between the legislations and enforcements, the safe environment for children in cyber world can be seen.