



INTERNATIONAL LAW  
JOURNAL

---

**WHITE BLACK  
LEGAL LAW  
JOURNAL  
ISSN: 2581-  
8503**

*Peer - Reviewed & Refereed Journal*

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

[WWW.WHITEBLACKLEGAL.CO.IN](http://WWW.WHITEBLACKLEGAL.CO.IN)



WHITE BLACK  
LEGAL.

## **DISCLAIMER**

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal

– The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK  
LEGAL

# **EDITORIAL** **TEAM**

## **Raju Narayana Swamy (IAS ) Indian Administrative Service** **officer**



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) ( with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru

and a professional diploma in Public Procurement from the World Bank.

## **Dr. R. K. Upadhyay**

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



## **Senior Editor**

### **Dr. Neha Mishra**



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

### **Ms. Sumiti Ahuja**

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



### **Dr. Navtika Singh Nautiyal**

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



### **Dr. Rinu Saraswat**

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

### **Dr. Nitesh Saraswat**

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

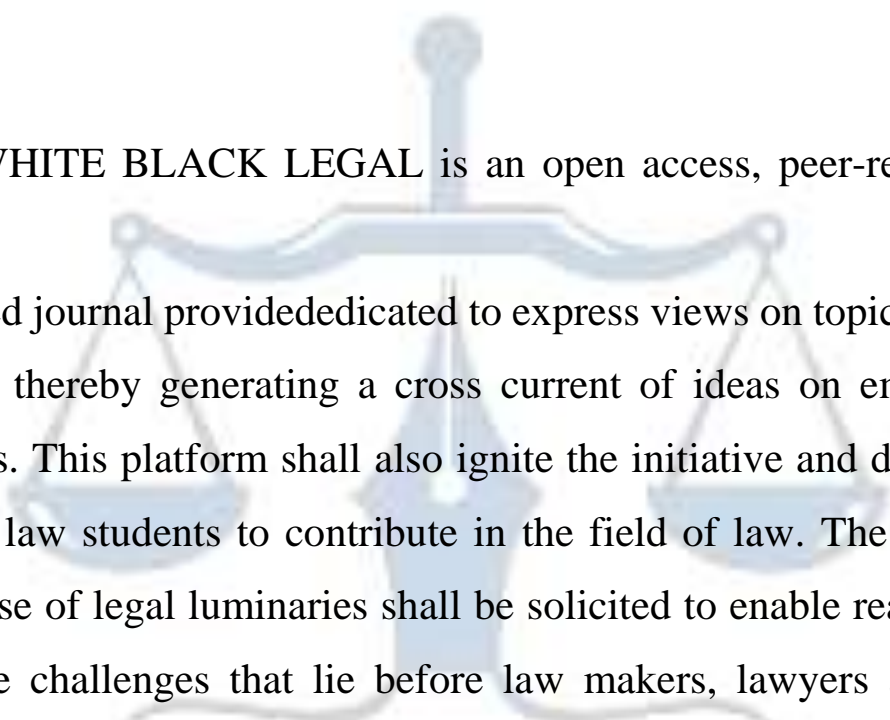


### **Subhrajit Chanda**

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

## ***ABOUT US***



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

# **CONTENT MONITORING IN CYBER SPACE** **FOR PROTECTION OF CHILD**

AUTHORED BY - SIDDHARTH BASKAR

## **ABSTRACT**

Given the rapid development of technology and the widespread use of the internet for socializing and exchanging information, child safety rules have become an urgent issue. Many countries, both wealthy and poor, are concerned about this. Nevertheless, it seems that the issue of kid protection has garnered more attention since the COVID-19 pandemic began. Studies have shown that the internet has become the "new medium" via which the cyber world routinely perpetrates many forms of child abuse, including physical, sexual, and emotional abuse, despite the numerous good consequences of the internet. Because of this, kids have less chances to get an education. This article explores the potential of cyber security to govern the safeguarding of children's online activities. It delves into the effects of online communication on kids and discusses the function of cyber laws meant to protect them. To combat the issue of children abusing the internet, this article considers both the viewpoints of parents and teachers as well as suggested laws from the European Commission. This paper draws on a pilot survey that sought to understand how parents and teachers felt about students' online activities both at home and in the classroom. Several recommendations for preventing the proliferation of online abuse are included at the end of the article.

**Keywords:** Internet, globalization, technology, child protection, legislation and Cyber Security

## **1. INTRODUCTION**

The rapid evolution of information and communication technologies has made them an integral part of our daily lives. The Internet is one of the most fascinating advancements in the field of information and communications technology because it allows people to interact and share information more quickly and effectively than ever before. Many more opportunities for education, art, and interpersonal contact have arisen thanks to the widespread use of Web 2.0 platforms on the Internet, and the number of social networks has exploded in recent years. This



is the main reason why more people, especially younger ones, have started using the internet.<sup>1</sup> All things considered, "children" and "adolescents" mean the segment of society that needs a lot more. There have been several concerns voiced about the information security of children and teenagers due to their heavy Internet use. Due to the prevalence of websites on the worldwide network that contain harmful information, children may be exposed to material that encourages aggression, violence, and sexual abuse. They face social and psychological risks in addition to technical ones, and they are targets of online hostility, deceit, and unethical activity. Because of this, cybercriminals are able to take advantage of victims. Because the Internet isolates children from their families and forces them to conform to the norms "dictated" by the online community, children are "trained" to act in ways that go against their traditional upbringing. Kids see the world in a more global light than adults do. Changes in this process make young kids feel like they don't have a permanent location to call "home." In addition to bolstering a "happy environment" or "habits," the data collected from the worldwide web influences how a user perceives things.<sup>2</sup> It also encourages the user to immerse themselves in other cultures and ways of living. Something like a "brain wash" is being imposed on children. There have been several global efforts to address the issue of children's internet safety, and this page offers opinion on such efforts. The regulations that regulate National Safer Internet Centres, the risks that children encounter while using the Internet, and possible remedies to these issues are all the subject of investigations.

Teens and young adults nowadays often spend long periods of time in front of their screens, whether for work or play. The internet is a wonderful tool, but it also poses significant risks. Young people struggle to balance the pros and cons of internet and digital system usage, even while an increasing amount of their lives are being recorded digitally, which might have long-term effects on their privacy and security. Until it's happened, individuals don't always see the danger or risk.<sup>3</sup> Cyberbullying might affect them negatively as a result. With the right mix of technology solutions and security expertise and practises, users may lessen or eliminate losses caused by cyber security risks. One of the many factors that go into good security processes is people's knowledge and ability to evaluate risks and mitigate threats.

---

<sup>1</sup> I A Sokolov and K K Kolin, 'Development of the Information Society in India and Actual Problems of Information Security' (2009) 4-5 *Information Society* 98.

<sup>2</sup> S S Allahverdieva, *Problems of Children's Security on the Internet* (Express-Information, Baku, Information Technology 2016).

<sup>3</sup> UNICEF, *Children at Increased Risk of Harm Online During Global COVID-19 Pandemic* (2020)

In the aftermath of the COVID-19 pandemic, children's dependence on the internet has grown. With the lockdown, schools closed, and online learning, most kids have started spending a lot more time online. The epidemic is directly responsible for the 50% increase in internet usage in India.<sup>4</sup> There may be good and bad effects of the Internet on kids' growth and development, as there are with many things. The Internet has grown into a vital resource in this era of immediate information. Children are exposed to content on the Internet that might be harmful or inappropriate, along with knowledge and entertainment. Some of the many online crimes that might stem from such exposure include cyberbullying, cybersexual harassment, cyber grooming, breach of privacy, and encouragement to illegal behavior.<sup>5</sup> Stricter regulations are required to protect children from internet dangers due to the increasing number of youngsters sharing recordings of their everyday activities and other information on social media.

Cybersecurity education programs for young people have received substantial funding and attention from both academic institutions and businesses in recent years. Despite the fact that childhood is divided into several stages. For this study, we have used the definition of "child" put out by the World Health Organization, the United Nations Children's Fund, and the Child Rights International Network (CRIN): any anyone below the age of eighteen is considered a kid. Research has focused on many areas to detect possible cyber security hazards for children, such as online privacy (Kumar et al., 2018; Prior & Renaud, 2020) and online safety (Prior & Renaud, 2020).<sup>6</sup> Additionally, there are a plethora of online tools designed to educate kids about cyber safety.

## 2. LITERATURE REVIEW

To protect children from cyber dangers, it is essential for families to establish routines for monitoring and supervising Internet use. (Wan Anita, 2016; Livingstone, 2007; Muhammad Adnan, Siti Zobidah, Jusang & Akmar Hayati, 2017; Valcke, Bonte, de Wever & Rots, 2010) It is crucial and urgent for parents to keep an eye on their children's online activities. Normah, Faridah, Wan Amizah, Fauziah, Chang, and Maizatul Haizan (2011) and Marshall and Jackman

---

<sup>4</sup> John Mcalaney, *Psychological and Behavioral Examination in Cyber Security* (n.p. n.d.) 153

<sup>5</sup> Aditi Shrivastava, *Cybercrime Against Women and Children: Escalation of Cybercrime During Pandemic and Laws to Curb* (2021).

<sup>6</sup> K Young, 'Internet Addiction: The Emergence of a New Clinical Disorder' (1998) 1 *Cyberpsychology and Behavior* 237

(2015) both agree that children need parental guidance when assessing the information and dangers found in online.<sup>7</sup>

Despite efforts by local ISPs like Digi, Maxis, and Celcom to provide parental control functions, only 17.2% of parents actually utilized them. This is due to the fact that 59.1% of parents said that they were unaware of the available functions. Rather of following the home rules while using the Internet, 69.2% of people did this. The procedure of monitoring and managing, however, might be affected if the parents lack technological abilities (Livingstone & Haddon, 2012; Wan Anita & Azizah, 2013).<sup>8</sup>

There has to be an improvement in parents' ability to monitor their children's use of social media, messaging applications, and platforms like WhatsApp, WeChat, and Telegram. The process of monitoring should begin at home, so parents should be on high alert and take the initiative. Utusan India (2017) notes that children are vulnerable to cyber dangers include addiction, pornography, cyberbullying, internet fraud, personal data leakage, and fraud if parents do not keep an eye on their online activity while they are at home. As an example, internet addiction is a major problem as it influences how people see themselves as they grow up.<sup>9</sup>

Approximately 78% of the country's internet users, particularly minors, suffer from a severe online addiction, according to the World Internet Statistics Review (Nadia, 2017). Being "overly concerned about social media and be driven by a strong motivation to log on or use the application, and to devote so much time and effort that impairs other social activities, studies/job, interpersonal relationships, and/or psychological health and well-being" is how Andreassen and Pallesen (2014) defined internet addiction. There are further indicators of social media addiction than time spent on the app, such as problems in relationships or uncontrolled, obsessive activity. Normah, Wan Amizah, Fauziah, Maizatul Haizan, and Mohd Helmi (2013) found that the addictive aspect of the Internet makes it particularly appealing to youngsters.<sup>10</sup>

---

<sup>7</sup> Brussels, 'A Digital Decade for Children and Youth: New European Strategy BIK+', European Commission.

<sup>8</sup> *Indian Penal Code* (Act No 45 of 1860).

<sup>9</sup> Smitha Krishna Prasad, 'Personal Data Protection Bill, 2019: Protecting Children's Data Online' (2020)

<sup>10</sup> C S Andreassen and S Pallesen, 'Social Network Site Addiction – An Overview' (2014) 20 *Current Pharmaceutical Design* 4053

## **1. Definition of Concepts**

This study has included concise definitions of the concepts. Here are the ideas defined:

## **2. Children**

Those under the age of eighteen are considered children under the Child Act of 2001 and the Convention on the Rights of the Child (KPWKM, 2015). The youngsters in this research are further divided into three age groups: Children whose ages range from six and under make up pre-school, children whose ages seven to twelve constitute primary school, and teens are those whose ages thirteen to seventeen.<sup>11</sup>

## **3. Cybermarketing**

"Demonstrating the appropriate parenting styles in digital culture while demonstrating proficiency in digital literacy and digital citizenship" is what cybermarketing is referred to as (Mohammad Nizam, 2015).

## **4. Cyber Safety**

The larger context of computer security includes the subfield known as cyber safety. Networking is a subfield of computer science that deals with computers and the networks they form. Computer crimes, particularly those involving hacking and identity theft, are the target of this effort. The cyber safety lesson, for instance, emphasized the need of being cautious with unknown internet users.

## **5. Cyber Threats**

Attempts to obtain unauthorized access to a computer network via a data communications conduit are known as cyber threats. These acts may be malicious and damaging.

## **6. Types of Cyber Threats**

This study covers five distinct forms of cyber threats: cyberstalking, cybergrooming, cyberbullying, cyberpaedophilia, and identity theft. These dangers often manifest in India.

## **7. Cyberbullying**

According to Hackectt (2017), cyberbullying is a major problem among kids worldwide. It occurs when other children threaten, harass, humiliate, or target other children online.

---

<sup>11</sup> Asiah Bidin, Shariffah Nuridah Aishah Syed Nong Mohamad, and Akmal Mohamad, 'Intipan Siber: Jenayah Baru dalam Masyarakat Kontemporari' (1994) <https://journal.unisza.edu.my/jimk/index.php/jimk/article/view/134> accessed 15 August 2024

## 8. Cyberstalking

The use of electronic communications, such as email, instant messaging (IM), website or forum messages, or other similar tools to harass, threaten, or otherwise harm a person is known as cyberstalking. To conduct cyberstalking, a person must first assume the identity of an anonymous user [24]. The purpose of cyberstalking is to cause psychological or bodily damage to the victims (Asiah, Shariffah Nuridah Aishah & Akmal, 1994).<sup>12</sup>

## 9. Cyber grooming

Cyber grooming is the practice of cybercriminals preying on unsuspecting victims, often youngsters, by creating an online persona and posing as a friend until the victim realizes someone is taking advantage of them (KPWKM, 2015). One study found that 10% of children had been asked to post personal photos or videos online; the number of rape cases that began with online relationships increased by 300% from 2010 to 2015; 80% of victims reported that their attackers were acquaintances on the Internet in the past two years; and the majority of victims were younger than 18 years old. (de Vaus., 2001). Cybergrooming is the first level of danger when it comes to child pornography.<sup>13</sup>

## 10. Paedophilia

A continuing sexual interest in children is characterized by the American Psychiatric Association as paedophilia (Seto, Cantor & Blanchard, 2006). From 2012 to 2016, 12,987 reports of child sexual assault were received by the Royal India Police (RMP), with 2,189 of the cases being successfully filed. Just 140, however, were found guilty.<sup>14</sup>

## 11. Identity Theft

A person commits identity theft when he or she utilizes another person's private information that has been leaked or stolen. Data such as names, DOBs, phone numbers, addresses, and the like are examples of personal information. In order to perpetrate fraud or other illegal activities, the cyber-thief retrieves this data (without permission) (KPWKM, 2015). The convenience of the Internet has made it easier for cybercriminals to steal sensitive data. The number of reported incidents of identity theft in India has

---

<sup>12</sup> S Byrne, S J Katz, T Lee, D Linz, and M McIlrath, 'Peers, Predators, and Porn: Predicting Parental Underestimation of Children's Risky Online' (2014) 19 *Journal of Computer-Mediated Communication* 215.

<sup>13</sup> D A de Vaus, *Research Design in Social Research* (SAGE 2001).

<sup>14</sup> DIGI, 'GuidetoFamilyFriendlyInternet\_BM.pdf' (2018) <https://www.digi.com> accessed 15 August 2024.

been steadily rising over the last three years, with 220 in 2015, 255 in 2016, and 262 in 2017.<sup>15</sup>

### 3. CYBER SECURITY AND LAWS IN INDIA

In terms of cybercrime rates over the last year, Norton's Cyber Safety Insight Report ranks the US and India in the top three. The number of reported cyber incidents in India in 2019 exceeded 3.13 million. The number of cybercrimes has increased since the pandemic reports began to surface, mostly because of the prevalence of internet activities.

According to Indian law, there are primarily four forms of cybercrime that target children: cyberbullying, child trafficking, pornography, and identity theft.

1. The government now enforces the Information Technology Act of 2000 and the Indian Penal Code of 1860<sup>13</sup> in order to prevent cybercrime. An update to the legislation regulating IT was made in 2008. In response to emerging threats brought about by the explosion of digital information and the development of cybercrime, many sections of the Information Technology (Amendment) Act, 2008 were updated.<sup>16</sup>
2. Section 43 details the consequences for wilfully permitting a computer virus to infect a system or network. Compensation for data breaches is covered under Section 43A.
3. Section 66C states that the maximum penalty for identity theft is three years in jail and/or a fine of one million rupees. One might be fined up to two million rupees (Rs. 2,000,000) and sent to jail for up to three years for violating someone's privacy.
4. Penalties for the distribution of child pornography via electronic means (Section 67B).  
These regulations are applicable to all individuals without exception, not only kids.

#### **Punishment under the Indian Penal Code, 1860**

The Indian criminal code, namely sections 354A and 354D, makes it unlawful to engage in cyberstalking or cyberbullying of a female victim. Neither statute adequately addresses cybercrime targeting children.<sup>17</sup>

---

<sup>15</sup> A Ghazvini and Z Shukur, 'Awareness Training Transfer and Information Security Content Development for Healthcare Industry' (2016) 7 *International Journal of Advanced Computer Science and Applications* 361.

<sup>16</sup> L Hackett, 'The Annual Bullying Survey 2016' (2017) <https://www.ditchthelabel.org/research-papers/the-annual-bullying-survey-2016/> accessed 15 August 2024

<sup>17</sup> Ili Hadri Khalil, 'India Negara Ke-9 Paling Aktif Media Sosial, Ke-5 Paling Ramai Guna E-Dagang - Laporan' (Astro Awani Online, 30 January 2018).

#### 4. LAWS FOR PROTECTING CHILD RIGHTS IN INDIA

Following the rules of the applicable legislation, law enforcement authorities will take legal action against anybody linked to the sexual abuse or maltreatment of a child via the use of a computer. The many types of cybercrime that are commonplace nowadays may be adequately controlled under the requirements of the Information Technology (IT) Act, 2000. Penalties for anyone found guilty of distributing, browsing, or communicating electronic adolescent sexual entertainment are laid forth in Section 67B of the Act. Furthermore, cyber harassment and online stalking of women may be sanctioned according to Sections 354A and 354D of the Indian Penal Code.

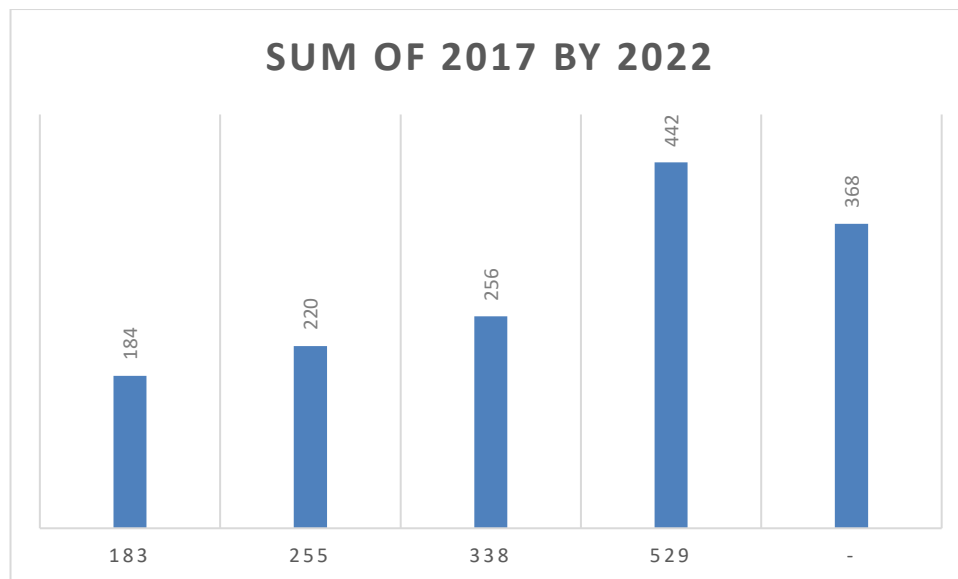
The Protection of Children from Sexual Offences (POCSO) Act, enacted in 2012, is a significant statute that addresses sexual offenses committed against minors. In 2012, this statute came into effect. Cybercrime directed at minors is now illegal according to POCSO. Some examples of these crimes include: sexual harassment, breach of privacy, cyberstalking, cyberbullying, defamation, grooming, hacking, identity theft, online child trafficking, cyberextortion, and online child pornography.<sup>18</sup>

##### a) *Cyber Threats Using Social Media*

Statistics of cyber threats have shown an increase from 2017 to 2022, as shown in Table I.

Threat	Year					
	2017	2018	2019	2020	2021	2022
Cyberbullying	260	389	291	256	338	-
Cyberstalking	300	512	550	442	529	<b>560</b>
Cybergrooming	54	44	60	184	-	-
Child pornography	-	-	60	184	183	<b>117</b>
Identity theft	-	-	223	220	255	<b>262</b>
Paedophilia	-	-	-	<b>184</b>	-	-

<sup>18</sup> KPWKM, *Pelan Tindakan Perlindungan Kanak-Kanak Dalam Dunia Siber* (Kementerian Pembangunan Wanita, Keluarga dan Masyarakat 2015).



The majority of young people (83%) use the Internet, and almost all of them (93%) access it from their own devices, according to a study (2017). An overwhelming majority of youngsters possess personal electronics; in fact, 85 percent of children surveyed admitted to owning a smartphone (Yunos, Ab Hamid & Ahmad Mustaffa, 2017). The vast majority of Internet users, particularly younger ones, utilize it to talk to one another, exchange material (photos and videos included), view videos, and search for information. According to the results of the study by Yunos et al. (2017), over half of the students in elementary school (ages 6 to 12) use social media. Aside from social networks, they also have accounts for movies and pictures on social media. Between the ages of thirteen and eighteen, almost all pupils (92.47 percent) have some kind of social media account. Many other kinds of social media accounts, including those for pictures and videos, have been registered. According to Yunos et al. (2017), the majority of students who have social media profiles enroll in order to engage with others.<sup>19</sup>

Young people suffer when they spend too much time online. Health, addiction, and emotional problems are among the impacts that have been previously studied (Yunos et al., 2017). According to Zakaria, Ahmad Munawar, and Noranizah (2012), children in India face dangers to their morals and sense of self-identity due to their exposure to harmful information. In India, over 78% of the population is addicted to the internet, with the majority of addicts being young people (Nadia, 2017).

---

<sup>19</sup> LPPKN, *How Internet and Communication Technologies Affect Both Family and Society* (2013).



Children are more vulnerable to these dangers because of the widespread usage of the internet. It is crucial for parents to keep an eye on their children's online activities and protect them from any dangers.

Table 1 shows that the majority of cyber threat instances have gone up. One factor that has led to the upsurge in cyberstalking incidents is the widespread use of social media. People, particularly youngsters, are easy prey for cyberstalkers on social media since no one can legally stop them from disclosing personal information to complete strangers, according to Asiah et al. (1994). Plus, social networking is more engaging than other apps, which is why kids love it. The rapid evolution of technology, the rise of interactive media, and the proliferation of personal electronic devices have all led previous studies to conclude that children's social media usage is out of their hands.<sup>20</sup>

## 5. METHODOLOGY

A quantitative strategy was used in this research to gather data using surveys and online questionnaires. A total of 872 parents whose children were under the age of 17 filled out the survey. The following questions are intended to be addressed by this study:

- How well do parents understand the risks that their children face online?
- How prepared are parents to let their children use their own gadgets for schoolwork? The purpose of this survey is to gauge parental preparedness for the BYOD program's new initiative.<sup>21</sup>

### *a. Research Design*

The quantitative methods used in this descriptive research are based on Creswell's design framework. Parents from all over Putrajaya were surveyed to gather information. Preliminary research, pilot studies to test validity and reliability, and the main study are the three stages of the research process. The study's methodology is shown in Table II.

No	Phase	Objective/Activities	Output
<b>1</b>	Preliminary study	To identify issues and Problems	<b>Problem statement</b>

<sup>20</sup> Mahyuddin Daud and Juriah Abd Jalil, 'Protecting Children Against Exposure to Content Risks Online in India: Lessons from Australia' (2017) 33 *Jurnal Komunikasi: Indian Journal of Communication*

<sup>21</sup> I A Marshall and G a Jackman, 'Parental Involvement, Student Active Engagement and the "Secondary Slump" Phenomenon — Evidence from a Three-Year Study in a Barbadian Secondary School' (2015) 8 *International Education Studies* 84.

		Determine the purpose of the study	<b>Research objective</b>
		Determine the scope of the Study	<b>Scope of the research</b>
		Review the results of relevant research from previous researchers, involving model theory, factors influencing cyber safety	<b>A comprehensive literary study on children's Internet use at home</b>
		Design research instruments	<b>Study instrument is developed</b>
<b>2</b>	Pilot research	Verify and finalize the research instrument	<b>Reliable research instrument</b>
<b>3</b>	Actual study / discovery	Implement an online survey	<b>Data collection from survey</b>
		<b>Analyze collected data using EXCEL</b>	<b>Respondent profiling and descriptive statistics results</b>

The first step is to conduct a thorough literature review that is in accordance with the research questions and the development of research instruments. This review will help to identify the issues, research objectives, scope, and purpose of the study, as well as to determine the research questions themselves. Articles from indexed journals such as the UKM Journal System, IEEEExplore, Google Scholar, and the UKM Digital Library are sought after for information pertaining to the theory, model, and implementation framework. To round out the image of what has been researched, expert groups from other ministries and departments were also asked to emphasize the state of department initiatives' implementation and any challenges with implementation.<sup>22</sup>

During the second part of the pilot project, which focused on validity and reliability, the instrument was evaluated before it was sent to the real respondents. This review included reliability testing and expert suggestions. The pilot study was helpful in developing trustworthy research tools. In order to make the study results more reliable, this method was used.<sup>23</sup>

<sup>22</sup> *Kawalan Teknologi ke atas Capaian Internet dan Pelaksanaan Program Klik dengan Bijak* (2017).

<sup>23</sup> Ministry of Education, Singapore, 'Cyber Wellness: What is Cyber Wellness?' (2018) <https://www.moe.gov.sg/education/programmes/social> accessed 15 August 2024.

The third stage comprises conducting a poll of parents and analyzing the results. We used SPSS, Survey Monkey, Microsoft Excel, and other programs to evaluate survey data on children's safe internet usage at home and the variables that influence this behavior.

The survey consisted of 71 questions and followed a conventional format. Logical, scientific, and tailored, it was structured according to predetermined parts and rooms. The questions were directed and arranged in a closed manner, so the responses were either right on the money or very similar to what the responder had requested. Because it is questionnaire-based, this approach is simpler to develop and evaluate.

The level of parental awareness and parental readiness can be measured and determined based on the indicators as shown in Table III.

<i>N</i>	<i>Mean Score</i>	<i>Level</i>
1	4.00 – 5.00	<i>High</i>
2	3.00 – 3.99	<i>Medium/Average</i>
3	2.00 – 2.99	<i>Low</i>
4	1.00 – 1.99	<i>Very Low</i>
5	0.00 – 0.90	<i>Not Available</i>

## 6. RESULTS AND DISCUSSION

The results are broken down into three sections in this report. This section begins with a discussion of parental awareness and how it relates to home cyber safety. In the second section, we discuss how prepared parents are to use their own devices in the classroom. In the third and last section, we talk about how cybersafety at home and cyberparenting are related.<sup>24</sup>

*First Part: How Cybersafe at Home Is Correlated with Parents' Awareness Levels According to Table IV, a significant majority of parents (80.9% to be exact) were aware of the online dangers that their children faced. Many parents have found success in limiting their children's access to inappropriate content online by using parental control software, having in-depth conversations with other parents, or even attending seminars hosted by Cybersecurity India. It*

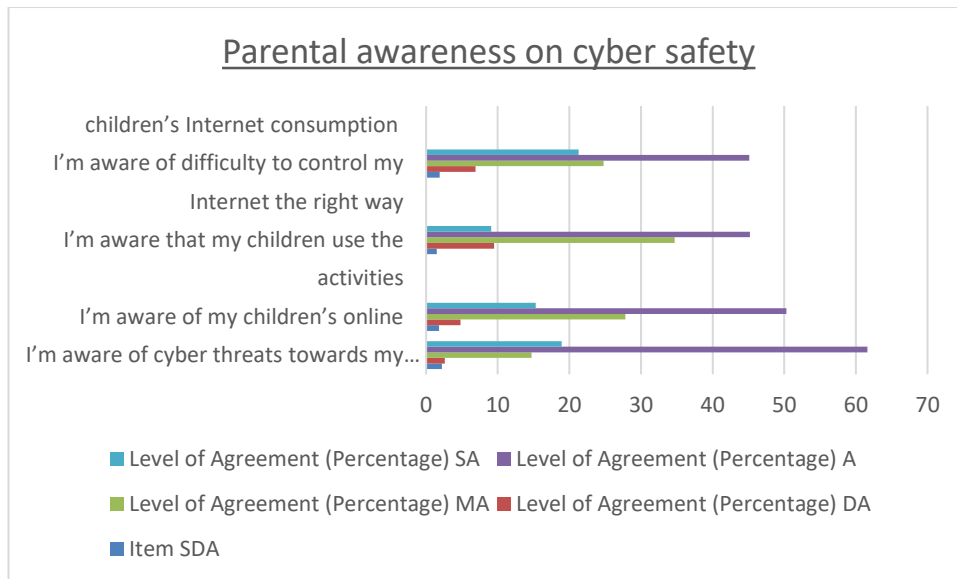
<sup>24</sup> Mohammad Nizam Kassim, *The 5 Strategies to Effective Cyberparenting* (CyberSecurity India 2015).

has been confirmed by Ghazvini and Shukur (2016) that an awareness training program may help reduce the risks. Contrarily, 31.4% of respondents had attended a cyber awareness lecture, while 68.6% have confessed that most of them still haven't. Approximately 68.6% of those who attended the presentation were pleased with it, whereas 31.38 % were dissatisfied and thought there wasn't enough information.<sup>25</sup>

Additionally, we inquired as to the respondents' familiarity with the Computer Criminal Act of 1997, the Digital Signature Act of 1997, the Multimedia and Communication Act of 1998, and the Copyright Act of 1997, all of which pertain to cyber law. The digital signature act was known by 13.3%, the copyright act by 23.50%, and the multimedia and communication act by 52.06% of the participants. In light of all the new technology, it is concerning that 39.10% of those who took the survey were unaware of any of the Acts. The likelihood of receiving fair treatment decreases dramatically if parents are unaware of the laws aimed at curbing, controlling, and convicting illicit behaviors. The results are consistent with those of the Royal India Police, who documented 12,987 instances of paedophilia but only managed to get convictions in 140 of those cases.

Item	Level of Agreement (Percentage)				
	SDA	DA	MA	A	SA
I'm aware of cyber threats towards mychildren	2.2	2.6	14.7	61.6	18.9
I'm aware of my children's online Activities	1.8	4.8	27.8	50.3	15.3
I'm aware that my children use the Internet the right way	1.5	9.5	34.7	45.2	9.1
I'm aware of difficulty to control me children's Internet consumption	1.9	6.9	24.8	45.1	21.3

<sup>25</sup> Muhammad Adnan Pitchan, Siti Zobidah Omar, Jusang Bolong, and Akmar Hayati Ahmad Ghazali, 'Analysis of Cyber Security from the Perspective of Social Environment: A Study of Internet Users in Klang Valley' (2017) 12 *Journal of Social Sciences and Humanities* 16.



Legend: SDA – Strongly Disagree; DA – Disagree; MA – Moderately Agree; A – Agree; SA – Strongly Agree.

Table V shows the degree to which parents are aware. The respondents' knowledge of the risk's cybercriminals pose to children and their children's online activity was moderate. Despite their frustration at the lack of control over their children's Internet usage, many parents insisted that their children were using the Internet responsibly. The parents' admission that they were unable to limit their children's Internet use raises concerns about the potential for Internet addiction, which should be handled before youngsters are exposed to other forms of cybercrime. It has been shown that severe cases of internet addiction may result in suicidal thoughts and sadness.<sup>26</sup>

Item	Mean Score	Std Deviation	Level of Awareness
I'm aware of cyber threats towards my children	3.92	0.80	Medium
I'm aware of my children's online activities	3.71	0.84	Medium
I'm aware of difficulty to control my children's Internet consumption	3.77	0.93	Medium
I'm aware that my children use the Internet the right way	3.51	0.84	Medium

<sup>26</sup> Nadia Hamid, 'Remaja, Kanak-Kanak Ketagihan Internet Serius' (BH Online, 22 October 2017).

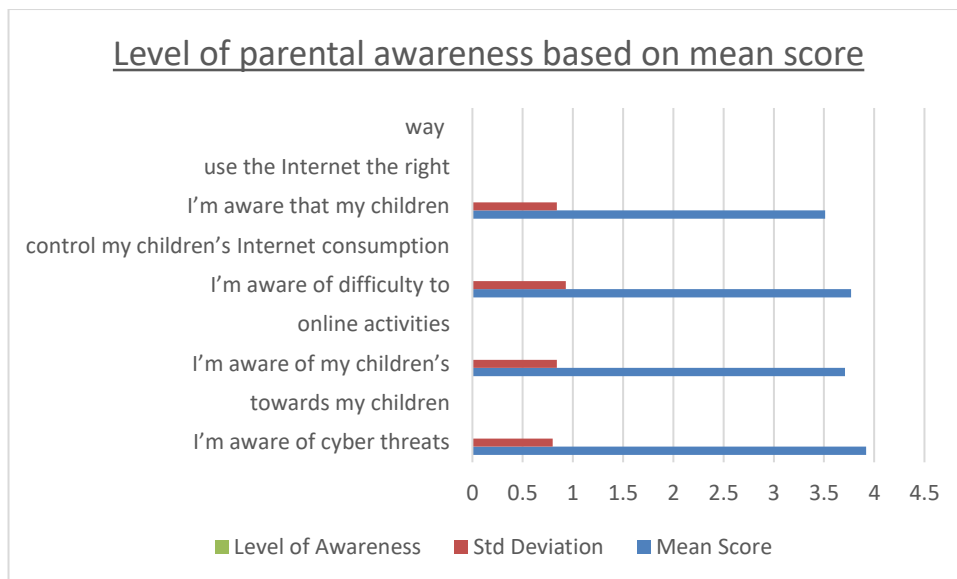


Table VI delves into the correlation between cyber safety awareness among parents and their children's online activity.

Parents' cyber knowledge correlates significantly with their children's cyber safety practices at home, according to the results. The chances of children being exposed to cyber dangers may be reduced if parents had more information about these concerns.

Because of this, it is critical that parents educate their children about online dangers at home.

## 7. LIMITATION AND SUGGESTION

The survey's limitations include its exclusive focus on parents whose children attend public schools. Only a subset of parents were surveyed for this research; those whose children attended public, charter, private, or special education schools were not included. Incorporating these types of schools into future research would help broaden the reach of cyber parenting in India and help shape the country's official curriculum.

## 8. CONCLUSION

Finding out how cyber-aware parents are and if there is a link between that knowledge and cyber-safety in the house is the primary goal of this work. This research is situated in India, a growing nation that is keen to adopt new technology in its pursuit of industrialization.

However, parental awareness is still on the lower side, so it won't be enough to keep kids safe online. The endeavors to educate parents on the need of cyber security are seen as vital. This is due to the fact that parents are unable to adequately safeguard their children if they are not well-informed and conscious. In order to improve cyber safety, programs that raise parental awareness should be extensively and publicly adopted. It is important to promote technology as an effective learning tool in order to increase parental preparedness to utilize BYOD/personal devices for formal learning. This endeavor must coexist with cyber safety promotion to guarantee that children's safety is not jeopardized, especially while they are online.

Compared to the actual world, there are less protections for children while they are online. The first step for parents should be to become more proficient in using computers and doing research online. To help parents restrict their children's access to harmful material online, antivirus software and "family control systems" may be installed on personal computers. Efforts to educate people about cyber security and encourage them to be more careful while using the internet are more important than ever. Some of the current issues in this area that need fixing include getting the word out about cybercrime, setting up support services, and making sure kids don't get exposed to harmful content. The best defense against cyber threats is a multi-agency strategy that includes parents, teachers, and the state. That being said, we need to do the following: - get the word out through the media about the mental health risks that kids face when using the Internet; - learn from other countries' experiences; - team up with Insafe, an organization dedicated to protecting children online; - launch a website focused on online safety for kids; - train experts in the field to help protect kids; - build social media platforms targeted towards kids. To safeguard children from internet dangers or assist in finding a solution to this problem, parents, schools, and other competent authorities may do a variety of things.