https://doi.org/ 10.33472/AFJBS.6.10.2024.5312-5324

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Navigating the Digital Landscape: Understanding the Impact of Unlimited Internet Access on Children

Author- Abhishek Awasthi

Research Scholar, Faculty of Law, Integral University, Lucknow

Co-Author- Prof. (Dr.) Naseem Ahmed

Dean, Faculty of Law, Integral University, Lucknow

MCN- IU/R&D/2024-MCN0002753

Article History

Volume 6,Issue 10, 2024

Received:29 Apr 2024

Accepted : 27 May 2024

doi: 10.33472/AFJBS.6.10.2024.5312-5324

Abstract

In addition to being a vast repository of information, the internet is a ubiquitous force that permeates every aspect of our lives. Although it provides unmatched ease of use and limitless connectivity, it also exposes us to significant risks. These days, living in a digital age, we navigate complex virtual networks and frequently find it difficult to determine where our information comes from and goes. This can be dangerous for both our own and our children's safety. Children in the twenty-first century are greatly impacted by the digital world in their everyday lives. The National Institutes of Health (NIH), a branch of the U.S. National Library of Medicine, reports that teenagers between the ages of 8 and 28 spend 44.5 hours a week on average in front of digital screens. Twenty-three percent of children admit to having a video game addiction, according to another survey. The younger generation is growing more and more tech-savvy and dependent on the internet, thus it is inevitable that they will come across the negative parts of this enormous virtual world.

Keywords: Information source, Connectivity, Vulnerability, Digital era, Virtual networks, Threats, Children, Adolescents, Digital screens, Addiction.

Introduction

Engaging in activities that have an illicit impact on society as a whole is considered a crime, a characteristic shared by all torts. The club intends to initiate legal proceedings against the wrongdoer, as it seems the action was directed against the club. When unlawful acts involve information and communication technology, they fall under the umbrella of cybercrime. Our society is transitioning into a technology-driven era, witnessing constant inventions. Communication has become quicker and more affordable, financial transactions are more accessible, and business is flourishing with the aid of new software streamlining processes. With the rise of technologies like artificial intelligence, these structures are reaching new heights.

The more we rely on the digital world, the more vulnerable we become to the downsides of technology, a phenomenon known as cybercrime. While there's no single legal definition of "cybercrime" in India, the Information Technology Act (2000) and its 2008 amendment outline various cybercrimes and the laws governing them.

In the current age, there's no distinction between children and adults regarding technology access. Children are active participants in this tech-driven world, impacting their lives as significantly as adults. The pervasive peer pressure, particularly visible on social media, influences them. If these exposures are within acceptable bounds, children can adapt to the rapidly changing society. Unfortunately, technology is sometimes misused for wrongful purposes. Cyber fraud and various other cybercrimes are committed by minors seeking improper gain. These crimes include cyber frauds, cyberbullying, cyber stalking, identity theft, drug trafficking, digital piracy, cyber suicides, cyber theft, illegal hacking, and more. Despite the increasing severity of the situation, what's even more concerning is that many children engaging in such activities often perceive them as harmless, unaware of the severe legal consequences. In many cases, they lack an understanding of the repercussions, falling into the trap of committing cybercrimes without realizing the potential harm to others' rights. This lack of awareness and a focus on short-term pleasure and entertainment contribute to the rising trend of cybercriminal activities among children in India. A common example is digital piracy, where children download content from untrusted sources, unknowingly infringing on copyrights. Acts such as sending harassing emails, downloading and mocking others' photos from social media also fall under the realm of cybercrimes.

Children or juveniles can access the internet more quickly and easily than adults. Computer crimes committed by juveniles are just as serious as those committed by adults. Fraud and cybercrimes are increasingly prevalent in our society, and unfortunately, our youth are getting involved in these criminal activities. If a juvenile is found guilty of using a computer for hacking or identity theft, potential consequences include probation, fines, and incarceration. The most common cybercrimes among juveniles include defamation, cyberbullying, harassment, drug trafficking, and accessing stored communication. Juveniles engage in internet offenses due to factors like curiosity during their upbringing, boredom, ignorance of the law, and the perception that everyone is doing it. Peer groups, family, and other community influences also play a significant role in shaping their

behavior. Social media stands out as a major loophole in the realm of cybercrime, with a considerable number of juveniles actively participating in these activities.

Methodology

The research focuses on the intersection of juvenile justice and cybercrime, acknowledging the ongoing development of juvenile laws. The doctrinal method will be employed to analyze the current scenario in the country. Cybercrimes have shown a consistent increase in numbers annually, paralleled by a rise in cyber delinquency. Examining data from the National Crime Record Bureau reveals a growing trend in cyber delinquency. The multifaceted reasons behind this surge remain unresolved. The escalating exposure of individuals, especially children, to the internet is contributing to their increasing vulnerability. Notably, new forms of cybercrimes committed by juveniles in India have emerged recently. The research aims to delve into these issues and provide insights into the evolving landscape of juvenile justice in the context of cybercrimes.

What is Delinquency?

Delinquency refers to criminal behavior, particularly when committed by a juvenile. The age at which an individual is considered a juvenile can vary from nation to nation. Generally, juveniles transition to adulthood between the ages of 15 to 18, although this age range may be adjusted for serious crimes. Importantly, delinquency is not contingent on the legal or moral age of the juvenile; it typically pertains only to actions that, if carried out by an adult, would be classified as criminal. This distinction sets delinquency apart from a status offense.

The term ‘juvenile delinquency’ encompasses a wide range of behaviors in children and young adolescents that go beyond simply violating criminal codes. It includes actions deemed unacceptable by society for their age group. Delinquent behavior can manifest in two primary ways: individual and group delinquency.[1]

- **Individual Delinquency:** This occurs when a young person commits a crime on their own. This delinquency is often attributed to factors specific to the individual, such as personality traits, mental health challenges, or a lack of positive role models.
- **Group Delinquency:** This refers to situations where young people engage in delinquent behavior together. In these cases, the cause is often linked not to the individual's personality, but rather to the social environment they come from. The culture of their home life or neighborhood might influence their behavior, potentially due to factors like poverty, lack of parental supervision, or exposure to violence.

[1] Kalaivani R. Kumar Muthu, Juvenile delinquency in cybercrime, available at International Journal of Academic Research and Development 2020

Understanding these different types of juvenile delinquency is crucial for developing effective prevention and intervention strategies. By addressing both individual and environmental factors that contribute to delinquency, we can create safer and healthier communities for our youth.[2]

Cyber Offences

(A) Cyber Crime against Children

Youngsters usually get used to computers faster and easier than adults do. Children growing up in the digital age have easy access to computers that are effortlessly linked to the worldwide network via the Internet. Many children like investigating and experimenting with the potential of modern technologies because of their natural curiosity. Unfortunately, their experimentation and exploration may take children to "places" online that are illegal, turning them into criminals even though they aren't aware that they are breaking the law.[3] In movies and animations, morphing is a special effect that smoothly transforms one image or shape into another. Somebody coerces youngsters into an internet relationship for sexually explicit acts with one or more children by conducting cybercrime.[4]

(A) Cyber Pornography

The act of displaying, publishing, distributing, creating, importing obscene or pornographic material via online platforms is a violation of ethical and legal standards. Technology is designed to assist and advance humanity, but unfortunately, some individuals, particularly kids, misuse it for prohibited activities. Cyber pornography is one such illicit act where technology is misappropriated for engaging in explicit and inappropriate content, raising concerns about the responsible use of digital tools. Cyber pornography is not specifically described as a cybercrime under IT Act, 2000 but section 67[5] of the act provides punishment and fine for publishing, transmitting or causing to be published or transmitted any data which is obscene in nature. At times, children may engage in actions that run counter to the societal well-being. The foremost responsibility of the state lies in addressing these children, referred to as juveniles in conflict with the law rather than labeling them as juvenile delinquents, as per the Juvenile Justice (Care and Protection of Children) Act, 2015. This approach underscores a focus on the rehabilitation and protection of young individuals involved in legal conflicts rather than stigmatizing them.

(B) Cyber suicides

---

[2] Bhardwaj Kiran, Cyber Crimes And Its Impact On Children And The Alternative Solutions, avaible a https://www.indialegallive.com/top-news-of-the-day/news/cyber-crimes-and-its-impact-on-children-and-the alternative-solutions

[3] Deb Shinder, Juvenile cyber-delinquency: Laws that are turning kids into criminals, available https://www.techrepublic.com/blog/it-security/juvenile-cyber-delinquency-laws-that-are-tuming-lads-to criminals

[4] Syed Adnan Ataq, Mahd Shahid Husam, Almustapha Bello. Halima Sada, CHAPTER 12 A Critical Analysis of Cyber Threats and Ther Global Impact (2023), Computational Intelligent Secunty in Wireless Communications http://192.168.9.248:5080/jspui/handle/123456789/811

[5] For detail see, Section 67 of Information and Technology Act,2000

The term “cyber suicide” pertains to cases where suicide is facilitated or influenced through the use of technology. Individuals may record their suicidal acts or even live stream them on the internet. A concerning example is the emergence of a game called the Blue Whale game on social networking sites, where the final task involved participants taking their own lives. This highlights the disturbing intersection between technology, online platforms, and tragic real-world consequences. Numerous suicides occurred as a result of this game. The 21-year-old Russian who made this game said that his intention was for kids to kill themselves and for society to be purified.[6] Juveniles who break the law in India are rehabilitated rather than punished for their wrongdoings. The statute aims to rehabilitate the delinquent in order to prevent a minor who committed a wrongdoing without being able to comprehend the nature of the deed from becoming a lifelong criminal. The Information and Technology Act of 2000 and the JJ ACT of 2015 will both apply in conjunction with one another to cybercrime perpetrated by minors. However, these statutes have a vague definition for adolescent cyber delinquency.[7]

(C) Web Hijacking

The term "web hijacking" describes the unwelcome and violent takeover of someone else's website. In these situations, the legitimate owner of the website relinquishes control over it and its contents, giving the hijacker the freedom to alter and maybe abuse the platform. Unwanted software that changes a web browser's settings without the user's consent is known as web hijacking. As a result, the browser will likely display unwanted advertising and the hijacker page may replace the user's current home or search page.[8]

- **Website Hijacking:** This refers to taking unauthorized control of someone's website. Hackers can do this for various reasons, like stealing sensitive information, defacing the site, or launching other attacks.
- **Browser Hijacking:** This involves unwanted software modifying your web browser settings without your permission. It typically forces you to see unwanted ads, redirects you to specific websites, or replaces your homepage and search engine.

(D) Cyber Stalking

A pattern of continuous harassment aimed at the victim is known as stalking. This could involve things like stalking the victim, calling her inappropriately, damaging her belongings, leaving notes or items, and keeping an eye on how she uses the internet, email, or other electronic communication tools. More serious violent crimes, such as those in which the victim is physically harmed, frequently precede stalking. Cyberstalking is a specific type of cybercrime where a cybercriminal repeatedly uses online services to threaten their victim. Stalking is illegal in India under Section 354D of the Indian Penal Code 1860.

---

[6] https://www.ijeat.org/wp-content/uploads/papers/v8i5C/E12040585C19.pdf

[7] See, Supra foot no.5

[8] available at https://us.norton.com/internetsecurity-malware-what-are-browser-hijackers.html

- **Similarities:** Both stalking and cyberstalking involve a pattern of unwanted and harassing behavior that makes the victim feel unsafe or distressed. They can also be precursors to violence.
- **Differences:** Stalking traditionally happens in the physical world, while cyberstalking occurs online. Cyberstalkers use electronic means like social media, email, or text messages to harass their victims.
- **Cyberstalking methods:** You mentioned threats, but cyberstalking can encompass a wider range of behaviors. Some examples include:

(a) Monitoring the victim's online activity.
(b) Spreading rumors or lies about the victim.
(c) Doxing the victim (revealing their private information online).
(d) Impersonating the victim online.

(E) Virus Attacks

Fred Cohen first used the term "computer virus" in an official capacity in 1983. Humans are the ones who always develop computer viruses. Once within a computer system, a virus attaches itself to another programme such that when the host programme runs, the infection's functions are triggered concurrently. Although most computer viruses do not have harmful intent, most of them do participate in malicious acts like data loss. Viruses propagate when programmes or documents they attach themselves to are shared across computers via e-mail attachments, a network, a disc, or file sharing techniques.[9]

- **Evolution of the term:** While Fred Cohen coined the term in 1983, the concept of self-replicating programs existed earlier.
- **Motivation beyond individuals:** While individuals certainly create viruses, there can be organized groups or even state-sponsored actors behind them.
- **Virus vs. Malware:** It's important to note that "computer virus" is a specific type of malware. Malware is a broader term encompassing any malicious software, including viruses, worms, Trojans, etc.
- **Payload variety:** Data destruction is a common malicious activity, but viruses can have various payloads. Some steal data, corrupt files, install additional malware, or disrupt computer operations in other ways.

(F) Software Piracy

The illicit copying of software that does not belong to the offender in a way that infringes copyright is known as software piracy. Software piracy also includes patent infringement, theft of computer source code, trademark infringement, and copyright infringement, among other things.[10]

- **Copyright Infringement:** This is the core aspect of software piracy. Software is protected by copyright law, and copying it without permission violates that law.

[9] available at https://economictimes.indiatimes.com/definition/computer-virus
[10] available at https://www.yourdictionary.com/software-piracy

- **Scope beyond Copying:** While copying is a common method, piracy can include other activities that violate the software license agreement. This could involve distributing, modifying, or selling unauthorized copies.
- **Beyond Copyright:** Your definition rightly mentions other intellectual property violations associated with piracy. Trademarks might be infringed if pirated software uses logos or names illegally. Stealing source code is another concern, and some software might even be patented, making unauthorized use a patent violation.

(G) Phishing

Phishing is a dishonest technique that involves sending bogus emails purporting to be from respectable organisations. The goal of these emails is to deceive recipients into disclosing credit card details and passwords, which can result in identity theft or financial crime. The primary cause of phishing in India is public ignorance of phishing policies and assaults.[11]

Phishing is a deceptive attempt to steal personal information like passwords and credit card numbers. Attackers send emails or messages pretending to be from trusted sources like banks or social media. By creating a sense of urgency or trust, they trick victims into revealing sensitive data on fake websites or through malicious links. Lack of awareness is a key factor, but India's digital boom and increasing reliance on online services make it a prime target. Staying informed and cautious about online interactions can help us stay safe from phishing scams.[12]

(H) Online Gambling

Online gambling is a pervasive issue that transcends geographical boundaries, affecting countries worldwide. The accessibility and proliferation of the internet have led to the emergence of millions of websites dedicated to online gambling. These platforms offer a variety of opportunities for individuals to engage in activities such as sports betting, casino games, poker, and other forms of wagering. The ubiquity of online gambling present's challenges for regulatory authorities globally, as they grapple with issues related to consumer protection, responsible gaming practices, and the potential for illegal activities. The ease of access to online gambling platforms has raised concerns about the impact on individuals, including issues related to addiction, financial harm, and the potential for fraud and criminal activities within the online gambling environment. Efforts to address these challenges often involve a combination of regulatory measures, technological solutions, and public awareness campaigns aimed at promoting responsible gambling behavior.

(I) Cyber Terrorism

Cyber terrorism involves the use of the internet to execute violent acts with the intention of causing loss of life or bodily harm. The primary goal of cyber terrorism is to achieve specific political

[11] Khan, Suhel Ahmed ed. Kumar, Rajeev ed Kalwartya, Omprakash ed. Khan, Raees Ahmad ed. Faisal, Mohammad ed., Computational Intelligent Security in Wireless Communications(2023) http://192.168.9.248:8080/jspui/handle/123456789/811

[12] Phishing Scams in India and Legal Provisions, available at https://cyberpandit.org/?article_post=phishing-scams-inindia-and-legal-provisions

objectives through threats, intimidation, or coercion. This form of terrorism leverages technology and cyberspace to carry out attacks on critical infrastructures, systems, or networks, often aiming to create fear, disrupt societies, and advance ideological or political agendas. Cyber terrorists employ various tactics, such as hacking, spreading malware, or launching distributed denial-of-service (DDoS) attacks, to achieve their goals and instigate widespread panic or disruption. The evolving landscape of cyber threats has prompted governments, organizations, and cyber security experts to develop strategies to counter and prevent cyber terrorism. Common cyber-attacks in India are on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks Cyber terrorism is an attractive option for modern terrorists for several reasons.

(J) Cyber Bullying

Cyberbullying refers to the act of bullying someone on online platforms, including social media platforms like Facebook, WhatsApp, Instagram, Twitter, and others. The essence of cyberbullying is typically associated with sharing negative or harmful content about an individual, which can significantly damage their reputation. This form of online harassment is particularly dangerous because it has the potential to subject anyone to public harassment through various cyber devices.[13] The harmful effects of cyberbullying extend beyond the digital realm, impacting an individual's emotional well-being, mental health, and overall sense of safety. Efforts to combat cyberbullying often involve promoting awareness, implementing preventive measures, and encouraging responsible and respectful behavior on online platforms.[14]

- **Impact:** Cyberbullying aims to inflict harm mentally, socially, psychologically, or even physically.
- **Methods:** Abusers can employ various tactics like sending hateful messages, sharing embarrassing content, online impersonation, exclusion, humiliation, and spreading rumors.
- **Legal Gap:** The IT Act, 2000 lacks provisions specifically addressing cyberbullying by school children. There are also no regulations regarding appropriate cellphone usage age.
- **Trend and Solution:** Students often view phones as fashion accessories, using them for cyberbullying. The Juvenile Justice Act could be a framework to address these issues since both victims and perpetrators are likely minors.

  This highlights the need for a multi-pronged approach:
- **Legislation:** Updating the IT Act to address cyberbullying.
- **Education:** Raising awareness about cyberbullying and responsible online behavior among students and parents.
- **Parental Guidance:** Setting guidelines for cellphone usage and online activity.

(K) Debit card and credit card frauds

[13] Adrita, 'Cyber Bullying: A Disregarded Issue In India', http://www.legalserviceindia.com/legal/article-2358-cyber-bullying-a-disregarded-issue-in-india.html

[14] See, Supra note 3

Credit card or debit card fraud entails the unauthorized use of someone else's credit or debit card information with the intention of making purchases or withdrawing funds without the cardholder's consent. This fraudulent activity often involves obtaining the card details through various means, such as skimming, phishing, or data breaches. Perpetrators may use the stolen information to make unauthorized transactions, leading to financial losses for the cardholder. Preventive measures, such as regularly monitoring card statements, adopting secure online practices, and promptly reporting any suspicious activities to the card issuer, are crucial in mitigating the risks associated with credit card or debit card fraud.[15]

(L) Impersonation and identity theft

Impersonation and identity theft involve the fraudulent or dishonest use of another person's electronic signature, password, or any other unique identification feature. This deceptive act aims to misrepresent oneself as someone else, often for financial gain or to commit various forms of fraud. In the context of electronic transactions and online activities, perpetrators may exploit stolen or falsified credentials to gain unauthorized access to accounts, sensitive information, or conduct activities on behalf of the victim. Preventive measures such as secure password practices, multi-factor authentication, and vigilant monitoring of personal information are crucial in safeguarding against impersonation and identity theft. Legal frameworks and cyber security measures are also in place to address and deter such fraudulent activities.[16]

(M) Online Drug Trafficking

Online drug trafficking refers to the criminal activity of selling, transporting, or illegally importing prohibited controlled substances—such as heroin, cocaine, marijuana, or other illegal drugs—using electronic means. Perpetrators of this crime utilize online platforms, the internet, and electronic communication channels to facilitate the distribution and exchange of illicit drugs. This form of drug trafficking presents law enforcement and regulatory challenges due to the anonymity and global reach offered by online spaces. Authorities employ various measures, including cybercrime investigations, to combat and prosecute individuals engaged in online drug trafficking, emphasizing the need to address the evolving landscape of criminal activities in the digital realm.[17]

(N) Hacking

This action involves unauthorized penetration into someone's computer system with the intent to steal or destroy data, and it has witnessed a significant increase in frequency over the past few years. The widespread availability of information online has contributed to the ease with which even non-technical individuals can engage in hacking activities. As a result, the prevalence of unauthorized access to computer systems has grown exponentially, highlighting the need for robust cyber security measures to protect against such intrusions and safeguard sensitive information.[18]

---

[15] Available at https://cybercrime.gov.in/Webform/CrimeCatDes.aspx

[16] ibid

[17] ibid

[18] Cyber security: challenges and solution, https://www.convergenceindia.org/blog/cyber-security-challengessolutions.aspx

REASONS RESPONSIBLE FOR CYBER DELINQUENCY

Cybercriminals often seek opportunistic ways to generate significant profits, targeting affluent individuals or wealthy organizations, such as banks and financial firms, where substantial amounts of money flow daily. They employ hacking techniques to access sensitive information and compromise computer systems. Given the vulnerability of computers, laws are essential to establish protective measures against cybercriminal activities. Some possible reasons contributing to cyber delinquency include:

- **Opportunity and Technology:** The widespread availability of technology and the internet creates a platform for cybercrime. Weaknesses in system security or user carelessness can make it easier for delinquents to exploit vulnerabilities.
- **Financial Gain:** Many cyber delinquents are motivated by financial gain. This could involve stealing personal information for identity theft, hacking into bank accounts, or deploying ransomware attacks.
- **Social Recognition or Revenge:** Some delinquents might seek social recognition or notoriety within online communities. Cyberbullying or hacking might be fueled by a desire for revenge against someone.
- **Lack of Awareness or Empathy:** Sometimes, young people might not fully grasp the consequences of their actions online. They might lack empathy for the victims or be unaware of the seriousness of cybercrime.
- **Psychological Factors:** In some cases, cyber delinquency could be linked to underlying psychological issues like a need for control, a sense of alienation, or even boredom.
- **Peer Pressure or Group Mentality:** Online environments can create a sense of anonymity or embodiment. Delinquency might be fuelled by peer pressure or a desire to belong to a certain online group.

It's important to address these reasons through a combination of:

- **Improved cyber security education:** Educating users about online safety, responsible behavior, and identifying phishing attempts.
- **Stronger legal frameworks:** Having clear laws that deter cybercrime and hold delinquents accountable.
- **Promoting empathy and social responsibility:** Encouraging responsible digital citizenship and fostering empathy for the potential victims of cybercrime.

LEGISLATIVE FRAMEWORK

Since cybercrime is growing daily, we require strict laws to help reduce these infractions. Following the 2013 revision to the Indian Penal Code 1860, many new provisions were added to combat cybercrimes in India. These sections include Section 292A, which deals with printing material intended for blackmail, Section 354A, which deals with sexual harassment, and Section 354D, which deals with stalking. Cyberbullying remedies are also provided by the Information

Technology Act. The IT Act's Section 66A[19] penalises anyone who sends offensive messages using a communication device. Invasion of privacy is also subject to harsher penalties under Section 66E, and publishing pornographic images is punishable under Section 67. Receiving any stolen computer resource or communication equipment dishonestly is punishable under Section 66B of the IT Act.

Receiving any stolen computer resource or communication equipment dishonestly is punishable under Section 66B of the IT Act. The Information Technology Act's Section 66C lays out the penalties for identity theft. It states that anyone caught using someone else's electronic signature, password, or other unique identifying feature fraudulently or dishonestly faces up to three years in prison and a fine of up to Rs. one million. The Reserve Bank of India Act and the Indian Evidence Act were altered as a result of the IT Act. As cyber law developed, nearly all online activity was subject to examination.[20]

However, one thing about cyber law is that there are certain areas on which cybercrime laws in India do not apply such as[21]:

- **Need for Stringent Laws:** Existing laws are a good start, but cybercrime is constantly evolving. Regularly updating and strengthening these laws is crucial.
- **Existing Legal Landscape:** The amendments you mentioned (IPC Sections 499, 292A, 354A, 354D) and the IT Act with sections like 66A (offensive messages), 66E (privacy invasion), 67 (obscenity), 66B (receiving stolen data), 66C (identity theft) are important steps.
- **Broader Impact:** The IT Act's influence extends beyond itself, prompting amendments to the RBI Act and Indian Evidence Act, reflecting the interconnectedness of cybercrime with other legal domains.
- **Scrutiny of Online Activity:** As cyber law evolves, online activities are rightfully under greater scrutiny. This helps maintain a safer online environment.

Here are some potential areas for further development:

- **International Cooperation:** Cybercrime often transcends borders. Collaboration between countries for investigation, extradition, and information sharing is crucial.
- **Focus on Emerging Threats:** Laws need to adapt to address new cyber threats like ransomware attacks, data breaches, and deepfakes.
- **Balancing Security and Privacy:** Finding the right balance between online security and individual privacy is a continuous challenge that legal frameworks need to address.

SUGGESTIONS

- **Benefits of Unlimited Access:** Discuss how unlimited internet access can be a valuable tool for learning, research, and creativity for children. Explore educational resources, online courses, and interactive platforms that can enhance their knowledge and skills.

[19] Azmi, Ashraf, Domestic Violence-Where Lies the Solution (2022) http://192.168.9.248:8080/jspui/handle/123456789/846

[20] Bandakkanavar Ravi, https://krazytech.com/technical-papers/cyber-crime

[21] https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/

- **Challenges of Unlimited Access:** Highlight the potential downsides of unlimited access, such as excessive screen time, exposure to inappropriate content, cyberbullying, and online addiction. Discuss the importance of parental controls, open communication, and digital literacy education for children.
- **Finding a Balance:** Explore strategies for finding a healthy balance between encouraging responsible online behavior and allowing children to explore the vast potential of the internet. This could involve setting time limits, establishing screen-free zones, co-browsing with children, and teaching them critical thinking skills to evaluate online information.
- **The Role of Parents and Educators:** Discuss the crucial role parents and educators play in guiding children through the digital landscape. Explore ways to promote responsible digital citizenship, online safety practices, and healthy screen time habits.
- **The Evolving Digital World:** Acknowledge that the digital landscape is constantly changing. Discuss the importance of keeping up-to-date on emerging trends, threats, and safety measures to ensure children's online well-being.

CONCLUSION

Cybercrimes have proliferated with the peak of technological advancements. These crimes are distinct from conventional offenses and are often categorized into blue-collar and white-collar crimes. The term "blue-collar" is used because cybercrimes share similarities with traditional crimes, albeit under different names. On the other hand, they are deemed "white-collar" due to being committed by individuals with expertise in science and technology.

The impact of cybercrime poses significant threats to society, culture, and national security. Protecting against these crimes is paramount, involving measures at both individual and societal levels. Strategies include employing robust passwords, utilizing antivirus software, avoiding unknown or dubious websites, configuring private settings on social media platforms, and implementing encryption methods. These protective measures contribute to safeguarding against cyber threats, ensuring the social, cultural, and security well-being of a country.

Individuals are urged to exercise caution online, thinking twice before clicking on links or files of unknown origin. Responding to emails that request verification of information or confirmation of user ID and password should be avoided. By promoting awareness and adherence to best cyber security practices, individuals can play an essential role in mitigating the risks associated with cybercrimes.

Due to rapid globalization, affordable smartphones, easy access to the internet, and the lack of effective laws to prevent the abuse of school children by their peers, the issue of cybercrime among kids and young adults is on the rise. In Western cultures, schools are subjected to strict oversight by laws and authorities. However, in India, there is a deficiency in the legal framework to address the core issues of cybercrimes affecting children.

Children are particularly vulnerable to the negative impacts of electronic media, and in India, it is often the schools rather than parents that wield significant influence in shaping a child's behavior. Therefore, there is a pressing need for stricter laws to prevent school bullying and ensure the online

safety of schoolchildren in the digital world. The juvenile justice system, which prioritizes rehabilitation over punishment, is more suitable for handling cases involving young individuals. In certain circumstances, minors may be tried as adults, especially in cases of serious offenses like murder or for repeat offenders.

Understanding cybercrime among youth requires a criminological perspective. Youths with strong social bonds and a sense of belonging to a peer group are less likely to engage in cyber-related offenses. Social isolation and involvement in offenses are often linked to peer groups. To address and reduce these types of offenses among the youth, both the central and state governments have the authority to enact appropriate legislation. This legislative approach should focus on rehabilitation and preventing cybercrimes among the youth.