A CRITICAL STUDY ON CHILD PROTECTION AND INTERNET REGULATION THROUGH CYBER SECURITY

Sadaf Waseem, PhD. Scholar, Sharda School of Law, Sharda University, Greater Noida, U.P. and Dr. Rohin Koul, Assistant Professor, Sharda School of Law, Sharda University, Greater Noida, U.P.

ABSTRACT

Child safety laws have emerged as a major problem in light of the exponential growth of technology and the pervasiveness of online socialization and information exchange. This is an issue that bothers many nations all over the globe, both rich and poor. However, the problem of child safety seems to have received increased focus during the COVID-19 epidemic. Despite the internet's many positive effects, studies have shown that it has also become the "new medium" via which frequently recognized various kinds of child abuse, such as physical, sexual, and emotional abuse, in cyber world are perpetrated. The educational opportunities for children have suffered as a result. In this article, we look at how the cyber security can be used to regulate internet protection of children. It focuses on the impact of internet-mediated communication on children and addresses the role of cyber laws aimed at protecting them. This article uses legislation proposed by the European Commission and the perspectives of educators and parents to address the problem of child internet misuse. The report uses a pilot study to inquire into the perspectives of educators and parents on the topic of children's Internet usage at school and at home. The article finishes with several suggestions for curbing the spread of online abuse.

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

I. INTRODUCTION

The Information and Communication Technologies (ICT) have become an indispensable component of our everyday life as a result of their rapid development. One of the most exciting developments in information and communications technology is the Internet, which provides users with a platform from which they, more efficiently and effectively communicate with one another and exchange information. The utilization of a platform of the Web 2.0 on the Internet has resulted in a significant increase in the number of options for learning, creative expression, and interpersonal communication, as well as the proliferation of social networks. Because of this, a greater number of users, the majority of whom are children and adolescents, have joined the internet. The terms "children" and "adolescents" collectively refer to the category of the society that requires a significantly higher level of care. Because of the extensive use of the Internet by children and adolescents, there have been several issues raised regarding the information security of these age groups.[1] It is possible for children to be exposed to content that promotes sexual abuse, aggressiveness, and violence as a result of the availability of websites that are full of dangerous information on the global network. They are subjected to deception on the internet, as well as aggression and unethical behaviour, and they are threatened by technological as well as socio psychological dangers. As a result, people end up being taken advantage of cyber-criminals. Children are "trained" to behave in a way that is not in line with how they were brought up by their families because the Internet drives them away from their loved ones and causes them to behave in a manner that is "dictated" by the virtual world. Children have a natural international perspective on the world around them. This process alters young people's perspectives of the world and gives them the impression of not having a place to call "home." The information that is obtained from the global network has a direct impact on a user's perception, and it also supports a heartwarming, "happy environment," or "habits." Additionally, it stimulates the user's will to participate in other societies and lifestyles. Children are being subjected to what may be described as a "brain wash".[2] The article provides commentary on the various ways that have been taken to solve worldwide challenges linked to the protection of children in the online environment. Investigations are conducted into the workings of National Safer Internet Centers and the rules governing them, as well as the

[1] Sokolov I.A., Kolin K.K. Development of the information society in India and actual problems of information security // Information Society. –2009, No 4-5, pp.98-106

[2] Allahverdieva S.S. Problems of Children's Security on the Internet, Express-Information, Baku, Information Technology, 2016, 91 p.

dangers that children face when interacting with the Internet and the potential solutions to such problems.

Today's youth regularly log lengthy sessions at their computers, be it for schoolwork or leisure. The internet has both fantastic benefits and serious dangers. Despite the fact that more and more of their lives are being digitally recorded, which may have long-term repercussions on their privacy and safety, young people have a hard time weighing the benefits and drawbacks of internet and digital system use. Sometimes people don't see the risk or danger until it's already too late. Consequently, they are vulnerable to cyberbullying. Users can avoid or reduce losses from cyber security threats through a combination of technical remedies and security knowledge and practises. A number of elements contribute to effective security procedures, but one of them is the familiarity with and skill with risk assessment and threat mitigation that individuals possess.

Children's reliance on the internet has increased recently, notably in the wake of the covid-19 outbreak. Most of the children have begun spending much more time online since the lockdown, school closure, and online learning. As a direct result of the pandemic, internet use in India has surged by 50 percent.[3] As with many things, the Internet may have both a positive as well as negative influence on children's development. In this age of instant information, the Internet has become an indispensable tool. In addition to providing information and enjoyment, the Internet also exposes children to material that may be dangerous or improper. Child pornography, cyberbullying, cybersexual harassment, invasion of privacy, cyber grooming, and incitement to criminal behaviour are only some of the online crimes that can result from such exposure. As more and more children upload videos of their daily antics and other content to social media, stricter rules have become necessary to keep them safe while they're online.

Industry and academics have invested a lot of time and money in studying and developing youth cyber security education program in recent years. Although there are several phases of childhood. We have chosen the World Health Organization's, the United Nations Children's Fund's, and the Child Rights International Network's (CRIN) definition of "child" for the purposes of this research: everyone under the age of 18 is a child. (Prior & Renaud, 2020) and online privacy (Kumar et al., 2018, Zhao et al., 2019) are just a few of the areas that research

[3]UNICEF 2020, Childen at increased risk of harm online during global covid-19 pandemic, visited at September 13th, 2022.

has focused on to identify potential cyber security threats for children. There have also been numerous digital resources created to inform children about cyber safety.

II. CHILD PSYCHOLOGY AND BEHAVIOUR IN DIGITAL ENVIRONMENT

Research on the risk, children face online shows that when utilizing the worldwide network, they are more likely to share their impressions with friends and peers than with their parents. It is estimated that more than half of children who face threats do not talk to their peers about it. Similar to the rest of society, Internet use among children varies greatly by age. This variation can be seen in the context of either social networks or digital artefacts. There are three distinct age brackets that experts use to categorise Internet users: those younger than ten, those between the ages of ten and thirteen, and those between fourteen and seventeen.[4] Below is a brief overview of the risks faced by children of varying ages. Protecting children under seven on the internet. Games are a big part of life for children under 7, and they naturally excel at manipulating digital assets in games. Since children have just recently learned to read and write, they are restricted to visiting websites only when accompanied by an adult. According to the experts, this is because the psychology of children at this age means they just want to do what they want. Young people of this age learn new technologies quickly and are ready to download unethical films, malicious files, and harmful applications, as well as visit sites and chats that their parents have banned. They could come across predators and sexually explicit content while looking for a "buddy" online. The best thing parents can do for their children is to create a "White list".

The "White List" is a curated selection of safe websites that parents may feel good about sending their children to. As a result, the goal of these platforms is to safeguard children, protecting children aged 10-13 years online. Most children of this age have heard of the Internet and know how to use it to find what they need. Many people are eager to learn, read, and hear about these topics. Students in the 10-13 years of age are the most common Internet users for schoolwork. When children play online games, they develop an unhealthy reliance on their computers. This means that parents are ultimately responsible for setting limits on their children's screen time. It is recommended that any Internet-connected computers in the common area be placed under parental control, and that the corresponding software be written on a computer for safety of teenagers between the ages of 14 and 17 online. Compared to their

[4] John Mcalaney, Psychological and behavioral examination in cyber security 153-158(Premium reference source),2018.

parents, children of this age are more likely to use the Internet for social interaction. It is getting harder and harder for parents to manage. Therefore, it's important for parents and children to come to an understanding about how to keep each other safe while using the Internet. Adolescents nowadays are avid users of the internet in all its forms, including web searches, e-mail, IM, music and movie downloads, video games, and more. Teenage boys, especially those in the 14–17 years of age, have a wide range of interests. They often choose violent video games and inappropriate media. Girls of the same age enjoy frequent online communication and they are more likely to share or seek out unsuitable material or content when doing so [5]. It is important for parents to check the reports detailing their children's time spent online. They must demonstrate methods of spam prevention. Parents should instruct their teens to use their real e-mail address while accessing the Internet, to ignore spam, and to set up mail filters. Definitely, parents should be aware of the places their children are visiting. Internet use by minors should not be strictly prohibited. Instead of outright banning Internet use, parents should take the time to educate their children on the risks and benefits of various online activities, as well as set limits on frequency and duration of use.

III. CLASSIFICATION OF OFFENCES CHILDREN FACES WITH INTERNET

Children's usage of the Internet increases their vulnerability to a variety of physical and digital dangers. You face these risks when you become a target of criminals and are aware of hazardous information are Internet-dependent, play harmful games, use phishing technologies or download malware encountering criminals as an intended victim. People in an online chat are not actually there but their virtual selves are.[6]

Learning to recognize dangerous content, Cyberbullies and predators use the Internet to spread messages of religious, racial, national and social hatred as well as sexual exploitation. Included in this category are guides on how to use and make drugs, how to store and set off different dangerous and explosive chemicals at home, and incitement to acts of terrorism. There are cartoons and short films on the sites that appeal to children who may otherwise not be interested in terrorist organisations. Additionally, children may be influenced by the appealing promotional videos, non-ethical language and slangs, and immoral practises that are prevalent on the sites. Addiction to using online platform, some children spend all day online, either browsing or playing games. Their obsession with technology is harmful to their physical and

[5] Ibid

[6] Aditi Shrivastava 2021, cybercrime against women and children: escalation of cybercrime during pandemic and laws to curb, visited at September 13, 2022.

mental well-being. The pacing system of children who spend too much time in front of screens slows down, leading to the emergence of a wide range of disorders, giving rise to the common perception that these children have "penguin feet." Having to strain your eyes to see the screen up close is not healthy for your eyes. Because of this, the user's eyesight gradually deteriorates. As their passions grow, though, they can't help but rely on online resources. Individuals who are highly dependent on the Internet for their daily information needs are at risk of being victims and perpetrators of cyber-crime. The daily habit of chatting with "acquaintances" and "friends" in the virtual world and the eagerness to participate in interactive games takes children's attention away from such phenomena as time, space, and reality, fosters mistrust of their surroundings, disrupts their daily routines, and reduces their academic performance. They are so reliant on the internet that they'd be miserable without their laptops. Many nations already see Internet use as a health risk. In order to protect their children from the perils of the Internet, parents should encourage them to pursue other interests, such as athletics, art, etc. Reducing children's Internet use requires shaping their information culture and promoting information and behavioural standards.[7]

IV. PARENTS AND EDUCATORS CAN HELP TO ADOPT RIGHT SOCIAL MEDIA BEHAVIOUR

Students have a higher propensity to utilize social media platforms as a direct result of the widespread availability of smart phones. Although India's Internet penetration is only 27%, the country has the world's second-largest user base (355 million people) according to the 2017 Mary Meeker Internet trends report. The number of people who use the Internet increases by 40 percent every year. More than 35% of Internet users fall into the 15-24 years of age, and 72% of all Internet users are younger than 35, according to the survey.[8]

According to the survey, mobile internet access accounts for almost 80% of all internet use in India. This is far higher than the global average of 50%. It also states that 34% of all mobile usage is devoted to information-gathering activities like searching, social networking, and messaging, while 41% is spent on entertainment. Both on-demand media and cheap data contribute significantly to the latter.[9]

[7] Young K. Internet addiction: the emergence of new clinical disorder, cyber psychology and behavior, 1998, vol.1, pp.237-244.
[8] Rajeev Katyal, Parents and teachers may help students to adopt the right social media behavior, available at: https://digitallearning.eletsonline.com/2017/11 (Last Visited September 14th,2022).
[9] Survey conducted amongst the student aged 10-15 years.

If the statistics are any indication, the advent of social media has had a profound impact on our capacity to interact with one another and form and sustain connections. Living in a digital environment has some advantages, but it also has certain dangers. The children of today are missing out on developing important interpersonal skills because they spend so much of their spare time communicating with others through electronic media. The dangers of cyberbullying, harassment, and Facebook depression all rise in tandem with the number of hours spent online.

What we mean when we talk about "cyber bullying" is the spreading of malicious rumours or other online attacks with the intent to harm another person.

Both schools and parents have a role to play in preventing their students from becoming victims of cyber bullying and educating them on appropriate online conduct. When schools host workshops to help students and their families become more comfortable using social media, they may discover whether or not a student is being bullied online. Many guardians don't know that Facebook membership is restricted to those who are at least 13 years old. It's crucial to remember that there's no way to make children follow this guideline, but open communication can help guide them toward responsible online behavior.[10]

An open dialogue between parents and children about issues like cyberbullying and Facebook depression is more likely to occur in a warm and supportive family setting.

Teachers are a student's second most important role model after their parents. Teachers should be educated on how to qualitatively map their pupils' behaviour in response to stress. They need to learn how to engage with and monitor pupils on a daily basis. If a teacher sees a significant shift in a student's behaviour, they should bring it up with the class coordinator and counsellor. There must be curricular reform.

Life and societal developments necessitate that traditional curriculam be updated to reflect these realities. It is important that computer-based lessons in the classroom reflect the needs of the modern world. Teaching children, the value of privacy controls is an essential component of any computer education programme. Encourage them and instruct them on the significance of customizing their privacy settings to their individual online habits. It is also crucial to underline the need of encouraging users to read the privacy policies of each social networking site they use.

[10] Id at 7.

V. THE SIGNIFICANCE OF PARENTAL SUPERVISION AND DISCIPLINE

It's crucial to keep tabs on your children's online activity and intervene if necessary. If you're a parent, you should think about getting software that can monitor your computer's activity online. This has the potential to detect cyberbullying earlier on. It is crucial to keep tabs on the websites your child is accessing, but you shouldn't resort to spying or invading their privacy to do it. It is also important to monitor the child's online activity, including the games they play, the websites they visit, and the people they interact with. In addition, parents should teach their children to avoid giving their personal details on untrusted websites. It's crucial that parents keep tabs on the photos their children post online. Parents should consciously show their children their social media profiles to help them develop good habits. Furthermore, it is necessary to establish norms for mobile device usage. In the early years of a child's life, it is important to discourage them from using their phones late at night, to foster in them a love of reading, and to encourage them to participate in at least one sport.

While the negative effects of social media and Internet use on children are discussed, it is the role of parents and educators to teach young people that the information available on the Internet can be utilized to increase knowledge and their skills provided, they approach it with caution.

VI. EUROPEAN COMMISSION RECOMMENDATIONS

The new European strategy for a better internet for children (BIK+) emphasizes the need of online safety while simultaneously encouraging digital involvement and empowerment. As the European Digital Principles and the beginning of the next Digital Decade approached, on May 11, 2022, a new strategy for enhanced child-friendly internet access (BIK+) was established. With this strategy in place, children can enjoy a positive online experience without fear of harm. BIK+ is being modified for use with younger demographics. European Strategy for a Better Internet for Children (BIK), an earlier initiative, has been expanded with this new approach (BIK). Since 2012, there have been substantial developments in both technology and EU legislation, necessitating the drafting of a unified set of rules governing both.

The many perspectives of today's youth are especially valued in BIK+. When designing the approach and later when evaluating its effectiveness, children will play an essential role. Our goal is to make sure that no child throughout Europe is left behind in the digital era by giving them access to age-appropriate content and tools and creating an environment where they can feel respected, capable, and safe when using the internet.

The European Year of Youth 2022's flagship programme,[11] BIK+, offers programmes based on these three tenets: safe digital experiences to protect children from harmful and illegal content, behaviour, contact, and risks as young consumers and to improve their well-being in the digital realm by providing a safe, age-appropriate, child-friendly online space created with their best interests in mind, digital empowerment to guarantee that all children, including those i.e.The Better Internet for children's page will continue to be updated with new resources and examples as part of BIK+. To do this, we will cooperate with the EU-funded network of Safer Internet Centres in Member States to educate and empower parents, teachers, and children online.

The European Union (EU) should adopt a guideline on age-appropriate design, standardize age, assurance and verification across Europe, promote the speedy evaluation of unlawful and harmful content and ensure that the "116 111" number provides support to victims of cyber bullying[12]. Some recent efforts include the following, all with the goal of equipping today's youth with better, more tangible resources for navigating the internet in a way that is both safe and useful. It will be difficult to achieve these goals without the collaboration of the business sector and the member states.

The participation of children is still highly valued. By extending peer-to-peer activities on national, regional, and local levels, and requiring firms to interact with the young people who use their goods, BIK+ shows that it appreciates the input of children and young people and seeks to actively involve them in decision-making processes.

All of the EU Member States will be able to use the new strategy as a guide for future policymaking. The Commission will keep working to spread awareness of the need for a global plan to safeguard children's digital rights and will collaborate with other international groups to disseminate its findings and guiding principles. In 2021, the Rights of the Child (RoC) digital component of the EU Strategy will be implemented, and it will be known as BIK+.

VII. CYBER SECURITY AND LAWS IN INDIA

According to Norton's Cyber Safety Insight Report, both India and the United States experienced some of the highest rates of cybercrime over the past year. Greater than 3.13

[11] Brussels, A digital decade for children and youth new European strategy BIK+, European commission, available at: https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids, visited at 13th September, 2022.
[12] Ibid

million cyber incidents were reported in India in 2019. After the pandemic reports were seen due to online mode in everything this has raised the cyber crimes number higher.

Indian Laws- Child trafficking, cyberbullying, pornography and identity theft are the four main types of cybercrime that target children.

- To combat cybercrime, the government now enforces the Information Technology Act of 2000 and the Indian Penal Code of 1860.[13] In 2008, the law governing information technology was updated. Multiple provisions of the Information Technology (Amendment) Act, 2008 were revised to address new challenges posed by the proliferation of digital information and the rise of cybercrime.
- The Information Technology Act of 2000[14] Provisions Penalties for knowingly allowing a computer virus to compromise a system or network are outlined in Section 43. Data breach compensation is addressed under Section 43A.
- Identity theft is punishable by up to 3 years in prison or a fine of up to Rs. 1 million, according to Section 66C. When someone violates your privacy, you could face up to three years in prison and a fine of up to two million rupees (Rs. 2,000,000).
- Punishment for electronic dissemination of child pornography (Section 67B). These rules don't apply only to children but to everyone equally.

Punishment under the Indian Penal Code, 1860

- Cyberstalking and cyberbullying of women are both illegal in India and are punished by law under sections 354A and 354D of the country's penal code.[15] Both laws fail to address cybercrime against minors in any detail.

VIII. LAWS FOR PROTECTING CHILD RIGHTS IN INDIA

People who are connected with the sexual abuse or mistreatment of a child through the use of a computer are subject to legal action taken by law enforcement agencies in accordance with the provisions of the relevant laws. The Information Technology (IT) Act, 2000 has provisions that are sufficient to control the many forms of cybercrime that are now prevalent. In Section 67B of the Act, strict penalties are outlined for those who distribute, browse, or communicate juvenile sexual entertainment in an electronic format. In addition, the Indian Penal Code's

[13] Information Technology Act, 2000.
[14] Ibid
[15] Indian Penal Code, 1860 (Act 45 of 1860)

Sections 354A and 354D provide a legal framework for the discipline of online stalking and cyber harassment of females.

An important piece of legislation that covers sexual offences perpetrated against children is the Protection of Children from Sexual Offenses (POCSO) Act, which was passed in 2012. This law was enacted in 2012. POCSO makes it a crime to commit cybercrime against children. This includes acts such as child pornography, cyber stalking, cyber bullying, defamation, grooming, hacking, identity theft, online child trafficking, online extortion, sexual harassment, and invasion of privacy.

IX. ARRANGEMENTS TO ENSURE THAT A CHILD'S ONLINE INFORMATION IS PROTECTED UNDER THE PERSONAL DATA PROTECTION BILL OF 2019

After a protracted period of time, the governing body decided to push back the date of its inaugural. In December 2019, the Parliament debated and voted on the Personal Data Protection Bill, 2019. The purpose of the individual information assurance fee was to protect the individual's personal information and to establish a foundation for an information insurance expert for the equivalent of the individual. The processing of personally identifiable information and sensitive personally identifiable information pertaining to children is outlined in detail in Chapter IV of the Personal Data Protection Bill. The personal data protection bill was initially scheduled to be discussed in the parliament in December 2019, but it was postponed at that time. Then, in January, the Covid19 pandemic struck the Indian region, and the bill has since been put on hold. It will be brought up for debate once again in front of the "Parliament," after which it will receive official approval and become law.[16]

Multiple protections for children's privacy are included in the measure. The definition of child of 18 as the age of consent is a key provision. In order to process a child's personal information, a data fiduciary will need parental permission, as outlined in the new legislation. The paper also suggests that a data trustee who deals only with minors should formally register with the relevant data protection authorities. Processing children's data and delivering services to them are regarded qualifying factors for determining a substantial data fiduciary. The bill imposes new duties on data fiduciaries with a disproportionate amount of responsibility. It is against the

[16] Smitha krishna Prasad, Personal data protection bill,2019: Protecting children's data online 2020, visited at September 14th 2022.

law for data stewards to conduct surveillance or tracking of children's data or to utilise personal information in a way that could compromise their safety.

It is the intent of this law, which is a draught measure based on the findings of a joint parliamentary committee, to ensure that children's internet privacy was protected in 2019. But at present PDP bill has been taken back into consideration will look into the matter then it will be brought.

X. GOVERNMENT INITIATION

On September 20th, 2018, the Ministry of Home Affairs unveiled the National Cyber Crime Reporting Portal[17] as part of a programme called "Cyber Crime Prevention against Women and Children" (CCPWC), through which members of the public can report instances of child pornography or child sexual abuse material, rape or gang rape images, or sexually explicit content. The public can use this hub's "Report and track" feature or remain anonymous when filing a complaint.

The Ministry of Home Affairs has begun a Twitter campaign to raise awareness about cybercrime under the handle @CyberDost, and they have also published A Handbook for Adolescents/Students on Cyber Safety (downloadable here).[18]

The government of India has established national cyber security measures for a variety of reasons. Preventing and properly investigating cybercrimes, including those committed against children, is a primary goal of the policy. It establishes a sound legal framework for strengthening enforcement powers. Its ultimate goal is to raise people's consciousness about the importance of cyber security. As an added bonus, they measure safeguards individuals' information, forbids intrusions into their privacy, and compensates them for losses incurred as a result of cybercrimes like data theft etc,.

XI. CONCLUSION

Less safeguards are in place for children online than in the real world. Parents should first improve their own level of comfort with computers and Internet research. Parents should install "family control systems" and antivirus software on their computers to limit their children's access to inappropriate content online. Cyber security education and efforts to promote a more

[17] Cyber Crime, available at: (www.cybercrime.gov.in), visited on September 14th,2022.
[18] Ministry of home affairs, available at: https://www.mha.gov.in/, visited on September 14th,2022.

cautious approach to online activity are needed now more than ever. Topical challenges to be addressed in this field include raising public awareness about cybercrime, establishing support services, and creating safeguards to prevent children from being exposed to inappropriate material. For optimal safety from online dangers, it is necessary to combine efforts from the home, the classroom, and the government. In this regard, the following steps should be taken: - raising public awareness through the media of the psychological harm to children and adolescents posed by dangers on the Internet; - studying and introducing international experience; - establishing cooperation with the organisation Insafe; - creating a website for child safety on the Internet; - training a scientific personnel specialised in the relevant field; - creating social networks intended for child use. There are a number of ways in which parents, schools, and relevant competent authorities may protect children from online risks or help find the best answer to this issue.

Because of the epidemic, children and teenagers all over the world are choosing to remain at home rather than attending conventional educational institutions or enrolling into online learning platforms. Encourage your children to create accounts on social media so that they may continue their education. Young people in today's society give out their personal information online without giving it any thought. What are the implications or the risks that are not obvious? Children are often under the impression that clearing the data on their electronic devices would protect them from harm, despite the fact that this is not the case.

When information is saved online, it is considerably more difficult to remove than when it is stored on electronic devices, which may be destroyed without leaving a trace. The effects of the digital era will ensure that any information that is shared on the internet may be accessed eternally. "Although human forgetfulness is common, neither the Internet nor the individuals who use it are capable of losing their memories.

A thorough and determined endeavour to remove content off the internet ultimately results in the whole and comprehensive elimination of such content. These prints can still be found in this location. It has been said that in this day and age of digital technology, it is the exception to lose things forever and the rule to save things forever.

The issue of ensuring the safety of one's computer network in today's modern society is one of the utmost significance. The most effective way to counteract this risk is to make the data easily accessible to the general population. Strengthen the protective laws that are already in place

and bring people from all parts of the world together to discuss this matter. In addition to that, it is essential that the children get instruction on the themes of online safety and personal privacy. Through the implementation of a wide range of cyber-awareness programmes, which state governments operate both online and offline. This applies not only to national governments, but also to individual citizens, who have a responsibility to spread awareness about the significance of installing antivirus software and elevating the cyber security settings on their own devices who are enough for being virus free.

REFERENCES

1. Sokolov I.A., Kolin K.K. Development of the information society in India and actual problems of information security // Information Society. –2009, No 4-5, pp.98-106
2. Allahverdieva S.S. Problems of Children's Security on the Internet, Express-Information, Baku, Information Technology, 2016, 91 p.
3. UNICEF 2020, Children at increased risk of harm online during global covid-19 pandemic
4. John Mcalaney, Psychological and behavioral examination in cyber security 153-158
5. Aditi Shrivastava 2021, cybercrime against women and children: escalation of cybercrime during pandemic and laws to curb
6. Young K. Internet addiction: the emergence of new clinical disorder, cyber psychology and behavior, 1998, vol.1, pp.237-244.
7. Brussels, "A digital decade for children and youth new European strategy BIK+, European commission"
8. Indian Penal Code, 1860 (Act 45 of 1860)
9. Smitha Krishna Prasad, Personal data protection bill,2019: Protecting children's data online 2020