Research on the Obstacles and Countermeasures to the Protection of Children's Rights and Interests in the Network Environment

Chang Guo[1,a,*]

[1]*College of Politics and Law, Capital Normal University, Beijing, China*
a. 1210302005@cnu.edu.cn
**corresponding author*

Abstract: This survey is based on the background of the era of rapid development of the Internet and the tendency of the younger age of Internet users, as well as the problem of children encountering more and more risks in the Internet environment. At present, the safety of children's network use in China has received more and more attention, but the specific aspects of prevention of network safety problems still need to be improved. This paper analyses the common problems that children in the online environment are mainly exposed to the risks of cyberbullying, identity information leakage, and the influence of violent and bloody information. The analysis of this paper concludes that children's cybersecurity problems are characterized by hiddenness, children's lack of self-awareness, and insufficient social attention. Based on this, the paper makes the following recommendations, the protection of children's Internet use should be carried out in a combination of online and offline ways, and the government, companies, schools, families, and individuals should make a joint effort.

Keywords: Internet, Children's Rights and Interests, Security

1. Introduction

1.1. Background

Since 1994, when it gained full access to the international Internet, the speed of network development in China has increased by leaps and bounds. The Internet has also gradually expanded its functions in entertainment, socializing, and education. Since the outbreak of the epidemic in 2020, home office and home teaching have become the norm, and children have become more dependent on the Internet for online teaching and socializing [1].

According to the 5th National Survey Report on Internet Use by Minors, the size of China's underage Internet users in 2022 will be 193 million, and the Internet penetration rate of minors will be 97.2% [2]. Among them, the Internet penetration rate of urban minors reaches 97.5%, and the Internet penetration rate of rural minors is 96.5% [2]. The report points out several characteristics of China's minors' Internet use, the first of which is that the Internet penetration rate of minors is getting higher and higher, and has basically peaked; in addition, China's Internet penetration has further shown a trend of lower age [2].

While the rapid development and popularisation of the Internet have brought great convenience to children's lives, it has also triggered many problems. Internet users tend to be younger, but children's minds are not yet mature, and their values have not yet been well established. The current complex network environment is a challenge to the protection of children's rights and interests in the use of the Internet. Children face cyberbullying, online harassment, violent and threatening messages, identity leakage, and many other online safety issues. The United Nations Children's Fund (UNICEF) has spoken out repeatedly on the issues of cyberbullying and cyberharassment, calling attention to the threats to children's online safety.

1.2. Research Significance

The topic of children's cybersecurity, which is the focus of this study, has not yet attracted widespread attention in society, and there is a relative lack of relevant data. The study hopes to understand the cybersecurity problems faced by children in various countries through literature and interviews, collect countermeasures to protect children's rights and interests and reduce the occurrence of cybersecurity problems, draw on mature cybersecurity protection and prevention mechanisms for children, and put forward relevant recommendations for the local Chinese children's online environment, to continue to appeal for the protection of children's cybersecurity. ope that people from all walks of life, including the government, schools, enterprises, and families, will pay attention to this issue and make corresponding countermeasures.

1.3. Topic

The theme of this paper is Obstacles and countermeasures to protect children's rights and interests in the Internet environment. The article will comprehensively describe the threats and challenges faced by children in the Internet domain in each country, and explore the corresponding countermeasures to these problems, seeking the best countermeasures to protect children's rights and interests on the Internet and to prevent safety problems, and giving corresponding suggestions from the social, family and individual levels respectively. In addition, the definition of a child in this paper is based on the United Nations Convention on the Rights of the Child, "A child means every human being below the age of eighteen years unless under the law applicable to the child, the majority is attained earlier".

2. Internet Threats to Children’s Rights

2.1. Cyber Bullying

Cyberbullying accounts for a large portion of the online problems faced by children. The term cyberbullying refers to aggressive, hostile, and other attempts to cause harm in online communications. Including such things as, outing, hate speech, cyber drama, and cyber harassment, among other terms. The scope of cyberbullying extends to all aspects, including cyberstalking, insults and defamation, hate and bias speech, in addition to the most common forms of cyberbullying that include sexually related harassment. The study found that 15 percent of adolescents reported experiencing cyberbullying, compared to 36 percent who reported face-to-face cyberbullying [3]. Boys and girls experience cyberbullying to roughly the same extent. The extent of cyberbullying is roughly the same, but there are gender differences in specific cyberbullying behaviors [4]. Cyberbullying peaks at 13-15 years of age, slightly older than traditional bullying [4-6].

In addition, some researchers have found that many of the bullying incidents that occur online cannot be dissociated from offline incidents, with one study finding that two-thirds of online harassment incidents were de-connected with offline episodes [7].

Numerous studies have shown that people who are targets of cyberbullying may be adversely affected physically and psychologically, but many people who experience cyberbullying may remain silent out of embarrassment, fear, or shame. Minors who experience cyberbullying may cause or increase the chances of the following adverse effects: depression, anxiety, suicidal ideation, low self-esteem, social isolation, and more.

2.2. Information Disclosure and Internet Fraud

In addition to this, identity leakage is a growing cyber problem. Some researchers have reflected that more and more software will pop up the use agreement before starting to use, which usually contains the request for the use of personal identity information. But often if the user does not agree to the agreement will not be able to use the software. So this agreement is set in a certain way to a certain extent is hegemonic terms and conditions. Moreover, more and more software applications are acquiring identifying information not only within the scope of the software but also more identifying information that is contrary to the rights and interests of the user and beneficial to the company's interests. This is also the case with a wide range of game software. Moreover, these informed consent clauses are often lengthy and partly difficult to understand, which are not friendly enough to the careful protection of children's identities. When faced with an informed consent agreement, children often cannot distinguish whether or not their identifying information is being used correctly, and may not fully understand the content of the agreement or have the patience to read it through to the end [8]. When downloading and registering for software, children are extremely vulnerable to the leakage and improper use of their personal identifying information. The leakage of identity information is a trigger for online fraud, which may further compromise children's rights and interests.

In addition, ever-changing forms of online fraud are also being derived, such as fraud through webcasting and selling goods, fraud in the concert online ticketing services, and fraud by sending false information simulating shopping platforms, the current high-speed development of AI technology has further deepened the hidden dangers of network information security. There may be an AI face change, an AI simulation of the voice of the relatives to make a phone call, and other forms of fraud. To carry out fraud and given that small children's ability to distinguish and resist temptation is weaker, children are more likely to become victims of online fraud.

2.3. Dissemination of Violent or Terrorist Information

There is another part of the problem that is often overlooked but is present in large numbers on the Internet. That is to say, violent or terrorist information spread on the Internet. Some violent and bloody pictures can be seen everywhere on the Internet, some of them are posted by netizens, and some of them are put out by some people in an organized way to achieve some anti-social purposes. Through interviews, some children would often swipe through QQ groups or browse webpages to see randomly disseminated horror pictures, and even more so, images of extremist terrorist organizations killing innocent people. These gruesome and bloody pictures or information will bring more or less harm to children, especially the negative impact on mental health. Studies have shown that children who are exposed to gory and violent information for a long period have an increased tendency to depression and anxiety compared to the general population. In addition, they may also imitate the violent behavior in the gory images, resulting in self-harm or injuries to others, which may cause physical injuries [9].

3. Obstacles to Protect Children's Rights and Interests in the Internet Environment

3.1. The Particularity of Children's Identity

Children’s insufficient cognitive development makes it difficult to identify whether their rights and interests have been infringed. Minors are at a critical stage in their physical and mental development. According to Piaget's Stages of Cognitive Development, children under the age of 12, in particular, have limited cognitive development and may have difficulty recognizing and protecting themselves when faced with online safety issues. Some of the victimized underage children may be aware to a certain extent that they are being abused, but they do not know how to respond to these threats properly, which in turn leads to such undesirable psychological states as panic and nervousness, and even more so. Because these undesirable states are not dealt with promptly, they may be transformed into long-term psychological illnesses, such as depression and anxiety, and produce a somatization reaction. When children are attacked, it is very difficult for them to have self-consciousness for timely detection and effective self-protection. Especially in the face of the complexity of Internet information and the quality of Internet users, some adults are very likely to be abused, and children are even more vulnerable.

3.2. Difficult to Assess the Infringement of Rights and Interests

The number of specific people who have received the infringement of rights and interests in the network environment and the degree of infringement are not easy to measure. It is not just online safety that is a concern. Children also encounter many safety issues in their offline lives, but these may be more intuitive than online safety issues.

For example, in road traffic accidents, the number of injuries, the degree of injury, and the death can be counted [9].

Security problems in offline life are in front of people and are relatively easy to investigate and count. However, when confronted with online security issues, they are highly insidious [10]. In addition, the nature of harm suffered on the Internet is difficult to define. All of these factors make it difficult to investigate and intervene in the safety of children's online use.

3.3. The Problems of Children’s Internet Safety

Another issue regarding the protection of children's rights and interests in the online environment is that, with the development of the Internet, although the issue of children's online safety has received more attention and research data than it did two decades ago, research on the issue is still relatively limited compared to other social issues. First, there is a limited research base about the dynamics of some of the online dangers, so program developers are not always clear about how the harms arise, and for whom. Under the circumstances of the online environment, they are not always clear about how the harms arise and how to protect children's rights and interests. Second, there is extremely limited literature on what kinds of program messages and skills have the potential to protect children and youth from specific harms. Although the dissemination of programs has intensified, few have been evaluated using rigorous empirical methods [8].

In addition, there has not been much practical action on the issue from all sectors of society. There is still a need for the government, schools, families, and individuals to take action individually and work together to form a synergy to prevent the problems that children may encounter in the online environment and to protect their rights and interests.

4. Suggestions and Countermeasures to Protect Children's Rights and Interests

4.1. Family Education

Early family education is conducive to the prevention of cybersecurity problems in the future. From the perspective of the perpetrators, early education on cybersecurity can help them establish the correct concept of network use and, to a certain extent, reduce their future behavior of cyberbullying, network fraud, terrorist information dissemination, etc. It will strengthen their discipline, and establish a correct sense of morality and legal awareness. For the victims, they can also learn how to protect themselves early, avoid cyberbullying, and online harassment, and reduce such problems from the root as much as possible. In addition, family Internet safety education is also a remedial measure. Today's Internet problems are complicated and hard not to affect children's growth. Thus, parents can supervise their children's time on the Internet and the application software they use, preventing their children from over-exposure to the Internet while also helping them to identify and screen software that abuses their identities. Third, parents need to pay attention to the importance of sex education for children. Most of the contents of cyberbullying always revolve around "sex". For example, some people may post revealing pictures of themselves to harass others or harass others through sexually abusive words. Therefore, it is important that children are educated reasonably about sexual self-protection in the early stages of family education, and that they are told in an easy-to-understand way how to distinguish whether they have been sexually harassed.

4.2. School Education

School education is also an important part of protecting the rights and interests of children in the cyber environment. Schools can incorporate cyber safety education into the official curriculum to ensure that children can receive relevant education. Countries such as Singapore include cybersecurity education in the compulsory curriculum and popularise cybersecurity knowledge among children through regular lectures [11]. In addition, it is also necessary for schools to carry out targeted and more specific cyber safety education activities, rather than general talks, to teach students how to protect themselves in the face of complex and different cyber dangers, and what specific measures they can take, and so on.

4.3. Social Aspect

Relevant policies and laws shall be issued to specify specific measures for the protection of minors' rights and interests on the Internet. At present, the Unprotected Persons Act and the administrative norms that specifically regulate the rights and interests of minors on the Internet have not yet formed a complete legal system and lack accountability mechanisms [12]. Administrative norms on the rights and interests of minors on the Internet have not yet formed a complete legal system and lack responsibility and punishment mechanisms. They need to be further improved to provide a legal basis for the supervision and protection measures taken by law enforcement authorities and the various responsible parties.

Further improvements are needed to provide a legal basis for the supervision and protection measures taken by law enforcement authorities and the various responsible parties; strengthen technical supervision of the network environment; and Provide a variety of remedial measures, such as telephone hotlines for online rights violations, and the relevant rights protection organizations to protect children whose rights have been violated.

Software developers should focus on the privacy protection of minors, strictly screen the information published by netizens, and design network anti-addition systems to protect children in the online environment.

4.4. Children Themselves

Firstly, children themselves should consciously strengthen their knowledge of Internet safety, actively cooperate with their parents and schools, comply with government policies and laws, learn to use the Internet correctly and safely, and be able to detect and seek protection in case of danger.

Secondly, although children are a vulnerable group, they also have the right to speak out. Children should be bold enough to speak out, and if they are physically or psychologically harmed by the use of the Internet, they should not choose to remain silent but should dare to tell their parents and teachers and take the initiative to seek solutions, for example, by calling Internet safety hotlines and the police, and so on. Moreover, children should be brave enough to express their feelings about what needs to be done to improve the policies for protecting the rights and interests of the Internet environment. In addition, children should have the courage to express their feelings about the parts that need to be improved in the policy of protecting their rights and interests in the online environment and make suggestions on how to protect children online, so that society can hear the voice of children.

Thirdly, as network security issues are often associated with offline incidents, many violent incidents or sexual abuse of children may continue to extend from offline conflicts to the network. Therefore, children should also raise their awareness of offline safety, and be alert to and stay away from violent or sexually abusive people promptly.

5. Conclusion

In summary, the protection of children's rights and interests in the Internet environment is still facing many problems. Especially under the dual background of the aging of network users and the accelerated development of the Internet, more cyberbullying and cyber fraud against children has emerged. The current situation requires more detailed policies from the government, better supervision of software production by companies, better education in schools and at home, and a focus on self-protection by individuals, as well as the joint efforts of several major players. Hope in the future, there will be a greener and healthier environment for children to use the Internet, and further strengthen the protection of children's rights and interests on the Internet.

References

[1] Zhou, S. Q. (2023). A Study of the Law on the Protection of Children's Personal Information in the UK and its Implications for China. Shanghai International Studies University.

[2] Department for the Defence of Youth Rights and Interests of the Central Committee of the League. (2023). Release of the 5th National Survey on Internet Use by Minors. Retrieved from https://www.cnnic.cn/n4/2023/1225/c116-10908.html

[3] Modecki, K. L., Minchin, J., Harbaugh, A. G., Guerra, N. G., Runions, K. C. (2014). Bullying Prevalence across Contexts: A Meta-Analysis Measuring Cyber and Traditional Bullying. Journal of Adolescent Health, 55(5), 602–611.

[4] Sorrentino, A., Baldry, A. C., Farrington, D. P., Blaya, C. (2019). Epidemiology of Cyberbullying across Europe: Differences between Countries and Genders. Educational Sciences: Theory and Practice, 19(2), 74–91.

[5] Mitchell, K. J., Jones, L. M., Turner, H. A., Shattuck, A., Wolak, J. (2016). The Role of Technology in Peer Harassment: Does it Amplify Harm for Youth? Psychology of Violence, 6(2), 193–204.

[6] Tokunaga, R. S. (2010). Following You Home from School: A Critical Review and Synthesis of Research on Cyberbullying Victimization. Computers in Human Behavior, 26(3), 277–287.

[7] Mitchell, K. J., Jones, L. M., Turner, H., Blachman-Demner, D., Kracke, K. (2016). The Role of Technology in Youth Harassment Victimization (NCJ250079). Justice Research, National Institute Justice, Office of Juvenile Justice and Delinquency Prevention.

[8] Eikawa, B. (2023). Protection of Minors' Information Rights and Interests in Digital Background. Legal Expo, (23), 92-94.

[9] David, F., Kerryann, W., Lisa, J., Kimberly, M., Anne, C. (2020). Youth Internet Safety Education: Aligning Programs With the Evidence Base. Trauma, Violence, & Abuse, 1-15.

[10] Livingstone, S. (2013). Online Risk, Harm, and Vulnerability: Reflections on the Evidence Base for Child Internet Safety Policy. ZER: Journal of Communication Studies, 18(35), 13-28.

[11] Wan, X. L., Shi, Q. (2024). Research on Cyber Wellness Education in Singapore from the Perspective of Digital Ethics. Comparative Education Research, (02), 3-12.

[12] Zhang, X. D. (2023). Research on the Protection of Juveniles' Internet Rights and Interests. Market Weekly, (04), 175-178.