Journal of Law, Society and Authority (ISNN) 2253-0266
Volume (13), Issue (2), September 2024; pp. 38 - 56 (EISSN) 2600-6219

Mechanisms for Achieving Cybersecurity for Children in Algeria: A Study of the Practical Guide for Protecting Children on the Internet

Hassina Benreguia*
Salah Boubnider Constantine 3 University - Algeria

Submission date: 06-02-2024 **Acceptance date: 13-09-2024** **Publication date: 24-09-2024**

Abstract:

Cybersecurity for children has become a critical focus within Algeria's e-government initiatives, reflecting the growing need to safeguard young users in the digital realm. This study aims to explore the practical guide issued on July 15, 2020, by the Ministry of Post and Telecommunications, designed to assist parents, guardians, and educators in protecting children online. The guide provides essential strategies and recommendations that equip caregivers with tools to monitor and regulate children's internet usage. These measures include guidance on setting parental controls, recognizing potential online threats, and fostering safe online behavior.

However, while the guide offers a practical framework that parents and guardians can follow, the study reveals that relying solely on such recommendations is insufficient to guarantee comprehensive cybersecurity for children. The digital environment is highly complex, with constantly evolving threats, which means that personal efforts by parents, although crucial, cannot fully address the risks children face. Without robust legislative measures and a structured legal framework, these guidelines remain limited in their effectiveness.

In addition to parental intervention, there is an urgent need for comprehensive legal support that enforces regulations, provides strict penalties for cybercrimes involving children, and ensures the consistent monitoring of harmful online content. Therefore, this study emphasizes the necessity of combining both practical and legal efforts to create a safer digital space for children in Algeria. Collaboration between government bodies, legal institutions, and civil society is essential to ensure a secure online environment where children can safely navigate the internet without exposure to harmful content or cyber threats. The findings suggest that only through the integration of these efforts can Algeria achieve the level of cybersecurity necessary to protect its youngest digital users.

[*] Corresponding author.

Keywords: *Cybersecurity; Internet; E-Government; Legislation; Protection.*

Introduction:

The significant and rapid development of the Internet with its various services and websites has made it the most used means and technological medium in the world. It has become the greatest influencer in the daily lives of individuals in various aspects, including economic, political, social, and especially family aspects. The World Wide Web, which is one of the most important services of the Internet, is no longer appealing to young people only; it has become a focus of interest and desire for children of all ages due to the opportunities it offers for entertainment, fun, games, and enjoyment.

Children have become more attached to their parents' phones, and many parents buy smartphones and computers for their children and connect them to the Internet throughout the year. Many schoolchildren in Algeria, as in other countries of the world, use smartphones, tablets, laptops, and desktops, all connected to the Internet for various purposes, as a primary means of distance learning, preparing school assignments, communicating with relatives and friends, or participating in interactive games, with or without parental supervision.

Many uses, websites, advertisements, and destinations target children on the web without them realizing their nature and seriousness. This is due to the lack of community awareness of the dangers of some web content on the child's mental health, personality, and balance. The responsibility for protecting them from the dangers of cyberspace is not only familial but also primarily social. It is the responsibility of the entire social environment. For example, the school's role should not be limited to teaching, and the family's responsibility should not be limited to providing food and clothing. Still, their role is mainly to protect the child from all the surrounding dangers in reality and cyberspace morally, religiously, and culturally.

The child's environment of friends, colleagues, peers, and relatives plays a significant role in pushing them towards specific uses and content on the Internet, which may be positive or negative. The matter becomes more dangerous and complicated in the absence of parental supervision of their children. Children's use of websites without any parental supervision has increased the risk of their exposure to harmful content far from the culture and values of the community. Students spend long hours on social media sites, neglecting their academic achievement. They are also exposed to watching pornographic images and videos, which negatively affects their moral values and social behavior.

Despite the many benefits that a child can gain from using the Internet, they remain unable to distinguish between useful content without the help of adults. The negative effects of using the web on children are the most visible. Using the computer and the Internet for long hours daily affects children's psychology significantly and increases their feelings of distress and anxiety. Exposure to violent scenes may increase the likelihood of them learning and practicing violent behavior in reality, making them more violent. This raises many questions about cybersecurity and ways to protect children from the dangers of the Internet.

Many documents and decisions issued by human rights organizations concerned with childhood have emphasized the need to respect, protect, and fulfill the rights of every child in the digital environment and enable children to access age-appropriate digital content from reliable sources.

Every technological development must be accompanied by security development that protects the user and ensures their safety. Cybersecurity is one of the most important security challenges facing the world, including Algeria, which has decided to move towards e-government in an attempt to implement the e-government project. It has also approved several reforms and procedures to help it achieve its cybersecurity in various political, security, and economic aspects, paying more attention to the social dimension, including the safety of the child in cyberspace and empowering them with the right to safe use of the network.

This study aims to identify the various experiences and efforts made by the Algerian state to protect children's cybersecurity, the latest of which was the practical guide for parents, guardians, and educators to protect children on the Internet issued on July 15, 2020, by the Ministry of Post and Telecommunications. This guide was prepared based on the experiences of Algerian children. It describes the child's behavior in the world of the Internet and reveals the risks to which the child is exposed, taking into account different age groups. It includes a set of guidelines, suggestions, and behaviors that parents should adopt when they discover a danger threatening the child on the Internet.

The research aims to provide a sufficient answer to the main question in its following complex form:

What are the guidelines offered by the practical guide for protecting children on the internet? And how effective is it as a measure in strengthening the protection of children from the dangers of the network?

I. Concepts definition :

The study was based on the following key concepts :

1. Defining the concept of cybernetics :

The world is increasingly interested in defining the concept of cybersecurity due to the enormous impact of internet-based threats on various aspects of life. These threats affect all countries and all social systems, and their impact has even extended to national security, as evidenced by the hacking and destruction of websites belonging to sovereign political bodies and the wiretapping and spying on senior leaders.

As for the US Department of Defense, it defines cyberspace as : "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data through communication network systems and the associated physical infrastructure"[1].

2. Operational Definition of Cybersecurity :

In this study, the concept of cybersecurity refers to all the legal, organizational, and technical measures used to activate the protection of information systems, communication networks, government programs,

[1] . Herbert Lin, Cyber Conflict in International Humanitarian Law. International Review of the Red Cross. Vol. 94. No. 886, (2012). p. 516.

and devices from digital attacks and cybercrime that affect systems and individuals, including child safety from the dangers of the internet.

II - Methodological Procedures of the Study :

1. Research Methodology :

The nature of the study required the adoption of a descriptive-analytical approach to describe the document, the subject of the study, "The Practical Guide to Protecting Children from the Dangers of the Internet", which is directed at parents, guardians, and educators. The purpose was to collect and analyze information from the document in its basic form to assess its adequacy as a measure to enhance child protection from the dangers of the internet.

2. Research Tools :

This study relied on documentary analysis to collect information from the document, "The Practical Guide to Protecting Children on the Internet". This involved selecting and analyzing important information in the document that is directly relevant to the topic of the study and serves its objectives, and allows for answering the research questions.

3. Study Sample :

The "Practical Guide to Protecting Children on the Internet" was chosen purposefully as the subject of the study because it meets the requirements of addressing the issue of cybersecurity for Algerian children. It is a guidebook directed primarily at educators, parents, and guardians, which makes it closer to the Algerian child and family compared to legal texts that are difficult for the general public to understand.

III- Results of the Analytical Study of the Content of the Practical Guide for Child Protection on the Internet

The Practical Guide for Child Protection on the Internet contains a set of guidelines accompanied by explanations of the risks that a child may face while using the internet. It also includes preventive measures that parents, guardians, and educators should follow to protect children and enable them to use the internet in the best possible way.

We have divided the guide into the following sections :

First : Childhood Stages in the Practical Guide for Child Protection on the Internet :

The Practical Guide for Child Protection on the Internet relies on psychological studies to divide childhood into three stages : early childhood, middle childhood, and adolescence. The analysis of the guide shows that it links the definition of each stage of childhood to the ways in which children interact with new information and communication technologies and the internet.

The guide also takes into account the characteristics and requirements of each stage to distinguish the dangers of the internet for children and the ways in which they interact with its websites.

1. Early Childhood :

This stage usually begins at the end of the third year and lasts until the sixth year of life. It is the years before children enter school. During this stage, children's growth and emotional development accelerate, and they begin to learn to speak. They also become more curious and eager to explore their surroundings. They tend to learn more about objects, including the devices that adults leave around them.

According to the guide, children in the pre-school stage begin to discover digital devices. Their first readings and online experiences are through playing, watching videos, and using different search engines. They may even download games, music, or pictures if they are used to using devices. Children in this stage are still trying to adapt to the real world and are therefore not yet ready for the virtual world.

2. Middle Childhood :

This stage begins at the end of the seventh year of a child's life and may last until the end of the ninth year. During this stage, children become more interested in their surroundings and more eager to explore them, thanks to their entry into school.

They tend to meet new people, such as peers and neighbors, and become independent from their parents outside the home and closer to their peers. The process of socialization begins in the school environment, which is one of the most important educational institutions. Children learn language and math skills, and how to integrate and communicate with others.

According to the guide, curiosity is the main characteristic of this stage of a child's life. It drives children to seek out the unknown, which makes them vulnerable to various harms, such as forming new friendships online. Children in this stage do not realize that sharing their photos and videos is a dangerous act that can have serious consequences.

3. Adolescence :

The age of adolescence varies from person to person and from society to society, but it can be agreed that it is the transitional stage between childhood and adulthood. During this stage, children learn how to perform the roles of adults and older people.

They also experience a series of physical, psychological, social, and moral changes. In this stage, children are more able to understand the world and what is happening around them.

Since adolescents spend a lot of time with their friends, their influence on them increases over time, while their interest in family matters decreases. Adolescents also become more interested in their appearance, and during this stage, they experience a growing sense of anxiety and insecurity.

The guide therefore considers adolescents to be the age group most vulnerable to the dangers of the internet and its harmful content. In adolescence, children try to interpret what they see and seek clarification for what they hear from adults. With the availability of the internet as a means of inquiry into everything they want, they become exposed to information that can corrupt their values.

Second : Warning Contents Presented by the Practical Guide for Child Protection on the Internet :

The "Practical Guide for Child Protection on the Internet" identifies a set of dangers that parents and guardians should consider when dealing with children at different stages. The guide illustrates the dangers that children face at each stage of childhood using images, illustrations, and symbols.

1. Dangers Faced by Children in Early Childhood :

According to the Practical Guide for Child Protection from Internet Risks, some of the most important dangers faced by children in the early childhood years include :

- Excessive exposure to screens can have negative effects on some of the child's cognitive functions, such as speech and language, or attention. It can also have serious consequences for their physical health (sleep disturbance, myopia due to exposure to blue light, inactivity, and weight gain).

- Exposure to inappropriate sexual images or content, whether intentional or unintentional.

- Exposure to inappropriate visual content, such as scenes of violence and dehumanization in videos, applications, and online games.

2. Dangers Faced by Children in Middle Childhood :

According to the Practical Guide for Child Protection from Internet Risks, some of the most important dangers faced by children in the middle childhood years include :

- Communicating with virtual people (avatars) without realizing who is behind them.

- Lack of communication and refusal to build social relationships, leading to isolation and introversion.

- Enticement by sexual predators through social media and online games, which can lead to sexual exploitation of the child and may even lead to kidnapping and suicide.

- Exposure to disturbing and unwanted content.

3. Dangers That Adolescents Face :

According to the practical guide for protecting children from online dangers, some of the most important dangers that adolescents face during their teenage years include :

A. Dangers of Internet Communication Content :

According to the practical guide for protecting children from online dangers, some of the communication content on the internet is harmful. The most important dangers that internet communication content can pose to children include :

- Exposure to content that promotes extremism and racism, including content that incites terrorism.

- Sites that display real images of accidents, torture, or "bloody" mutilation that shock adolescents and push some of them to commit such acts that are dangerous to the child's psyche and behavior.

- Violent and dangerous games and applications that threaten your child's mental and physical health.

- Spam or unwanted emails, viruses, and malware.

B. Risk of Publishing Personal and Private Information :

According to the "Practical Guide to Protecting Children from Internet Risks," children are at risk of having their personal and private information published, especially since they are not aware of the dangers of sharing it.

1. Disclosing personal information about a child that leads to their defamation or damage to their reputation.

2. Accepting "friend requests" from strangers who have never been met before.

3. The risks of sending messages or texts with sexual content :

- Identity theft, Examples :

- Misuse of your child's image and appearance : This can include using their photos without permission, creating fake profiles or accounts using their name and likeness, or even impersonating them online.

- Creating fake accounts using your child's identity : This can involve using their personal information, such as their name, date of birth, and Social Security number, to open fraudulent accounts in their name. This can have serious financial and legal consequences for your child.

D. Dangers resulting from interacting with the virtual community :

The "Practical Guide for Protecting Children from Internet Risks" identifies a number of dangers resulting from interacting with others in the virtual community. The most important of these dangers include :

- **Online encounters and grooming :** This involves adults using social media, forums, and gaming websites to exploit children by pretending to be their peers.

- **Cyberbullying and harassment :** This includes mockery, defamation, isolation, insults, rumors, and threats through comments, messages, photos, videos, and so on.

- Hacking into children's accounts to obtain private photos or videos of them in compromising situations and threatening them with them later.

- Interacting with virtual personas (avatars) without knowing who is behind them.

Third : Guidance Content Provided by the Practical Guide for Protecting Children Online :

The "Practical Guide for Protecting Children Online" identifies a set of guidelines that are intended as tips for parents and guardians to consider when dealing with children at different stages of childhood. The guide presents these instructions in pictures, illustrations, and symbols that can help protect the child at every stage of childhood, as follows:

1. Guidelines for protecting children in early childhood:

In this section, the "Practical Guide for Protecting Children Online" provides a set of guidelines to help parents guide their children towards the best ways to protect themselves from the dangers of cyberspace in early childhood. These guidelines include:

- Setting limits on whether children are allowed to use their mobile phones to access the internet and how often they can use them.

- The type of content that can be downloaded using your digital devices.

- Children under the age of three are prohibited from using electronic screens.

2. Guidelines for protecting children in middle childhood:

In this section, the "Practical Guide for Protecting Children on the Internet" provides guidelines specifically for middle childhood that are tailored to the nature of children at this stage and the conditions for dealing with them:

- Ensure that the child uses the internet in a family-friendly space, such as the living room, instead of being alone in their room.

- Organize your child's free time and direct them towards sports and cultural activities, etc.

- Always be present with your child and develop honest and open communication with them so that they can express their experiences on the internet.

- Encourage the download of parental control applications and programs to filter access to certain content, in order to reduce the risk of exposure to content that is not suitable for children at this stage.

- Accompany the child while they are browsing the internet and talk to them about what they are doing while browsing.

3. Guidelines for protecting children during adolescence :

The "Practical Guide for Protecting Children from Internet Risks" provides a set of guidelines for dealing with children's internet usage during adolescence. These guidelines are divided into three categories :

A. Guidelines related to the communicational content of the internet :

- Take an interest in your child's online gaming activities, especially games with chat features.

- Guide your child to websites that are appropriate for their age.

- Adjust the privacy settings on your child's accounts.

- Check your child's browsing history and downloaded apps.

- Observe how your adolescent handles their newfound independence if they have a laptop, tablet, or smartphone.

B. Guidelines related to publishing personal and private information :

- Review your child's friend list.

- Educate your child about the risks they face online, which can follow them throughout their lives.

- Make sure you have the passwords for all of your child's social media accounts and electronic devices.

- Monitor your child's online activities and mobile phone usage.
- Check whether your child is posting and sharing information that reveals their identity and lifestyle on various social media platforms.

C. Guidelines related to communicating with the virtual community :

Define what is acceptable and unacceptable in terms of :

- The types of chat topics your child can participate in online and the language that is considered inappropriate for chat use.
- The chat rooms and forums they can participate in. In this case, they should only participate in supervised chat rooms.
- Talking to your child about grooming, explaining its meaning, and drawing attention to the groomer's personality and behavior.
- Monitor the use of cameras on mobile phones, tablets, and smartphones, as well as the posting and sharing of photos and videos online.

Fourth : The adequacy of the practical guide for protecting children on the internet as a measure to ensure children's cyber security :

Despite the existence of Law No. 15-12 on Child Protection and several other laws that regulate the cyber space and protect individuals, including children, from the dangers of cybercrime and punish its perpetrators, these laws have not been able to stop these crimes or achieve cyber security for children or other groups.

All the legal procedures and bodies that were put in place to monitor and prosecute cybercrime that appeared before the publication of the "Guide for Protecting Children on the Internet" were not enough to deter the perpetrators of chaos in the cyber space. Although this guide is not as strict as the law, it is sufficient to educate and guide parents on ways to prevent cybercrime so that their children do not become victims of violations whose effects on the child can be difficult to avoid in the future.

It is a complementary measure to the legal and regulatory measures that preceded it, which the government aimed at protecting children from the dangers of the internet and its various sites.

Therefore, the last page of the guide is dedicated to directing parents and guardians to the legal texts and administrative bodies responsible for prosecuting cybercrime. It includes the contact numbers of the security services, the national gendarmerie, and the green number, as well as a brief definition of the Child Protection Law :

"Law No. 15-12 on Child Protection, this law aims to define the rules and mechanisms for child protection in Algeria. Its publication is a significant and important step forward in the fight against violence against children. This law establishes the rules of the general legal framework that includes social protection and legal protection for the child, regardless of his legal status"[2].

We also refer to the following bodies and laws :

1. National Authority for the Prevention and Fight against Crimes Related to Information and Communication Technologies :

Established by Law No. 04-09 of August 5, 2009, on the prevention and fight against crimes related to information and communication technology, the National Authority's tasks include activating international judicial and security cooperation, managing and coordinating preventive operations, and providing technical assistance to judicial and security authorities.

It can also be assigned to carry out judicial expertise in cases of attacks on information systems that threaten state institutions, national defense, or the strategic interests of the national economy.

"This authority was established by Presidential Decree No. 15-261. It is an independent administrative authority under the Minister of

[2] Practical Guide to Protecting Children Online, Ministry of Post and Telecommunications, (July 15, 2020). p. 15.

Justice. It operates under the supervision and control of a committee headed by the Minister of Justice. The committee mainly includes government members concerned with the subject, officials of security services, and two judges from the Supreme Court appointed by the Supreme Council of the Judiciary"[3].

2. Units of the National Security Forces:

The National Security Forces has three units responsible for investigating and prosecuting cybercrime :

- The Central Laboratory of Scientific Police in Algiers : This is the main laboratory for scientific police in Algeria. It is responsible for providing technical assistance to judicial and security authorities in the investigation of cybercrime.
- The Regional Laboratory of Scientific Police in Constantine : This laboratory is responsible for the investigation of cybercrime in the eastern region of Algeria.
- The Regional Laboratory of Scientific Police in Oran : This laboratory is responsible for the investigation of cybercrime in the western region of Algeria.

In 2010, the General Directorate of National Security created 23 cells to combat cybercrime. These cells are located in the central, eastern, western, and southern regions of Algeria. They are responsible for investigating cybercrime and providing technical assistance to judicial and security authorities.

3. Units of the National Gendarmerie Command :

The National Gendarmerie Command has a number of units responsible for investigating and prosecuting cybercrime. The most important of these units is the National Institute of Criminal Evidence and Criminology, located in Bouchaoui. This is a national institution with an administrative character. It was established by Presidential Decree No. 04-183 of June 26, 2004.

[3] . Samir Bara, Cybersecurity in Algeria : Policies and Institutions. Algerian Journal of Human Security. No. 4, (2017). p. 274.

The National Institute of Criminal Evidence and Criminology has a number of tasks, including :

- Providing technical assistance to judicial and security authorities in the investigation of cybercrime.
- Conducting research and studies on cybercrime.
- Raising awareness of the risks of cybercrime.
- Training judicial and security officers in the investigation of cybercrime.

4. The Law on the Prevention and Fight against Crimes Related to Information and Communication Technology :

This law organizes crimes related to information and communication technology and everything related to the information system, information data, service providers, and data related to the management of electronic communications. It includes :

- Monitoring and inspecting information systems when necessary.
- Seizing information data.
- Storing data related to traffic.
- Defining the obligations of Internet service providers.
- Establishing the tasks of the National Authority for the Prevention and Fight against Crimes Related to Information and Communication Technology.

In addition to the various actors involved in this field, there are a number of important institutions that play a key role in the fight against cybercrime in Algeria, including:

- The Central Office for Combating Cybercrime of the National Security Directorate.
- The Center for the Prevention of Computer and Cybercrime of the National Gendarmerie.

- The National Authority for the Protection and Promotion of Childhood.
- The Ministry of Post and Information and Communication Technologies.
- The Center for Research in Scientific and Technical Information.
- Civil society organizations and associations.
- Individual and corporate initiatives.

5. Amendment of the Penal Code :

The Algerian legislator issued Law No. 04-15 amending the Penal Code. Section 7bis of this law deals with cases related to interference with automated data processing systems. This section includes eight articles, of which Article 394bis punishes anyone who enters or remains by fraud in all or part of an automated data processing system or attempts to do so.

Article 394bis of the same law also states that anyone who enters by fraud all or part of an automated data processing system shall be punished by imprisonment from three months to one year and a fine of 50,000 to 100,000 dinars.

6. Civil Code :

The rules of tortious liability set out in the Civil Code, Order No. 75-58 of November 2, 1975, concerning the Civil Code, can be applied to claim compensation for harm caused by a third party to a child through the use of any means, including the internet.

Conclusion :

The analytical study of the practical guide for protecting children on the internet for parents and educators shows that it is a well-structured guide based on an integrated awareness and guidance approach. When parents follow its guidelines, they can protect their children of all ages from the dangers of the internet and its sites, which have had a growing impact in recent years and have captured the minds of children and adolescents.

The study reached a general conclusion that the practical guide is a preventive and advisory measure that can enhance child protection from the dangers of cyberspace. This is achieved through the guidance content that the practical guide for protecting children on the internet provides.

It includes guidance for parents, guardians, and educators on the most effective ways to protect children from the dangers of the network from early childhood, middle childhood, and adolescence.

It also relies on the involvement of all actors in their environment, from parents and guardians to educators. It includes the following main axes :

- Highlighting the dangers and harms that children face when accessing the internet and defining the concepts and elements of communication (vocabulary) related to these dangers.
- Clarifying the practices and behaviors that parents, guardians, and educators should teach children to ensure safe internet use.
- Providing technological tools to frame internet use, such as software and applications to protect against harmful and offensive content for children.
- Clarifying the procedures and means available for parents and educators to interact with the competent authorities to report cases of child exploitation on the internet.

Since the practical guide for protecting children on the internet is a guiding and educational measure that aims to raise awareness among parents and educators about the dangers of the network on children and suggests a set of guidelines that can be used to address them, it is a complementary measure to a series of legal and deterrent measures that are all mechanisms for protecting children from the dangers of the network.

The study also reached a set of recommendations and suggestions to reduce the dangers of the internet on children, which are listed below :

- Parents should monitor their children's use of internet sites while being careful not to restrict them and to raise their awareness of the danger of some internet sites on them.
- Parents should look for effective ways to protect their children from the harmful content of the network, by using protection systems that block harmful content that is not suitable for children's age.
- Universities should intensify studies to reach effective solutions to the problem of harmful content on the internet for children.
- Software developers should develop programs specifically for children that meet their entertainment and educational needs, with advanced systems to block harmful content.
- Civil society, in all its institutions, should play its role in raising awareness among parents, educators, and children about the dangers of some internet content on children through seminars, conferences, and other activities.
- The Algerian legislator should issue legislation specifically for protecting children from the dangers they face in cyberspace.