journal Of Legal and Economic Studies ISSN 2602-7321/ EISSN 2773- 2649
Vol : 05 No: 03 Year: 2023 Page : 1174 - 1188

Intellectual security protection against social media risks Legal sociological reading

Said ziouche* [1], University Center of Barika, Algeria, said.ziouche@cu-barika.dz

Ounnoughi nabil [2], University Center of Barika, Algeria, ounnoughi.nabil@cu-barika.dz

Send Article Date: 11 /06/2023 Date of acceptance of the article: 14/06/2023

Abstract:

Protecting intellectual security from the risks of social media is an important issue in our current era, as individuals and institutions are exposed to many threats and risks through these media. Where individuals and organizations must be aware of the dangers of social media and receive the necessary training to deal with it safely. Training courses can be provided to employees and workers in institutions to enhance awareness of the dangers of social media and teach them how to deal with it. The paper in our hands shows the importance of protecting intellectual security in light of the large increase in social media via the Internet. Preserving privacy Intellectual security cannot be protected from attacks that may be exposed to it, which requires us to search for mechanisms to ensure that these threats are confronted.

key words: Social networking, cyber-crimes, Protection mechanisms, Intellectual security.

Introduction:

On October 29, 1969, the Advanced Research Projects Agency (ARPA) in the United States was unaware of the magnitude of the service it would provide to humanity by creating the first network connecting four mainframe computers, with a connection speed of up to 50,000 pulses per second. Today, more than half a century later, data from the International Telecommunication Union confirms that internet usage continues to grow globally, with the number of internet users now reaching 4.1 billion people, accounting for 53.6% of the world's population[1]. One of the most significant outcomes of the tremendous development of the internet is the emergence and widespread use of social media platforms. These platforms have

* Said ziouche.

[1] International Telecommunication Union, International Telecommunication Union Newsletter, November 01, 2019, www.itu.int

become one of the most effective and influential means of communication. However, despite their positive aspects, they also entail significant negative implications and, in some cases, pose a major threat to societies and nations. The impact of social media varies across different domains of life, including economic, social, and political relationships. Nevertheless, its influence on intellectual life remains the most powerful and dangerous, given its ease of penetration into minds and its ability to attract and persuade through various factors.

Social networking sites have opened up a new era of cultural openness between people, transforming the world into a global village and a global family. Today, the international community has become aware of the danger posed by the virtual world due to the increasing threats emanating from it. Consequently, countries and international organizations have resorted to various mechanisms aimed at reducing the risks that threaten their interests and principles.

Research Problem:

The past two decades have witnessed an unprecedented revolution in the development of social media platforms due to the continuous advancement of digital devices and increased internet connectivity. This has brought about significant changes in the pattern and nature of relationships, especially in the social and intellectual realms. A study by Al-Yousef in 2006 emphasized that individuals' addiction to internet usage and other modern technologies has become a serious indicator. Additionally, the study highlighted the risks associated with the widespread availability and usage of the internet, particularly among university students, and the need to pay attention to this issue and develop mechanisms to control and regulate the use of these technologies. Another study by Gubta and Ananda[1] emphasized the negative influence of social media platforms on shaping and influencing the opinions of young people.

In this context, the research question is as follows: How can we protect the intellectual security of our societies from the dangers of social media platforms?

Research Objective:

The aim is to contribute to uncovering the most important legal and socio-psychological mechanisms to mitigate the risks posed by social media platforms to intellectual security.

Research Methodology:

The descriptive-analytical method was used, which is a scientific approach used to describe and analyze a specific phenomenon or problem. It involves collecting and analyzing quantitative data and information about the phenomenon or

[1] Abdulhamid, Soheir Safwat. 'The Role of Social Media in Spreading Rumors and Ways to Confront Them.' Conference on the Regulations for the Use of Social Networks in Islam, 2016

problem, classifying them, and subjecting them to detailed studies to obtain accurate and detailed knowledge about the research problem.

Research Terminology:

Social media platforms: These can be defined as "services that rely on the features provided by web 2.0, allowing users to create a public or semi-public profile, establish a list of users sharing certain characteristics, and establish a connection between them."[1]

Intellectual security: The concept of intellectual security has several advantages. It is a relatively modern term that gained prominence following the significant advancements in the world under the influence of the digital revolution, especially with the development of communication and transportation means, the ease of cultural exchange, and the mutual influence between cultures. Intellectual security refers to the intellectual and cultural invasion that threatens a nation in terms of its beliefs, security, and stability.[2]

Cybercrime: Also known as technology-related crime or high-tech crime, it can be defined as "crimes that cover all unauthorized actions related to information and communication technology, including hardware and software."[3]

Theoretical Framework:

Today's youth have grown up in an era of globalization, where conservative societies are exposed to changes resulting from global influences. These changes are a product of scientific and technological advancements that shape lifestyles, means, and requirements. As a result, many young people experience a split personality influenced by the ongoing conflict between inherited values and imported traditions. This has led to confusion, anxiety, and disorientation. The intense engagement and rapid interaction of young people with social media platforms raise alarm bells, as it has significant implications for the values that shape their behavioral patterns, attitudes, and inclinations toward family issues, social issues, and political matters.

THE FIRST TOPIC: CONCEPT OF SOCIAL MEDIA APPLICATIONS

FIRST REQUIREMENT: DEFINITION OF SOCIAL MEDIA APPLICATIONS

Social media refers to various online platforms or mobile applications that enable interactive two-way communication through user-generated content, as well as communication between users. Unlike traditional media that comes from a single

[1] Al-Mudhaini, Osama Ghazi. 'The Role of Social Media in Shaping Public Opinion among Saudi University Students.' Journal of Arts and Social Sciences, Sultan Qaboos University, 2015, p. 55.

[2] Al-Afaisan, Sulaiman Mutaib. 'The Level of Awareness of the Concept of Comprehensive Security among Students of King Saud University.' Master's thesis, Naif Arab University for Security Sciences, 2009, p. 68.

[3] Same previous reference, p. 69

source or fixed network location, social media platforms are designed specifically to allow users to create (produce) content themselves and interact with information and its source.[1]

SECOND REQUIREMENT: SOCIAL MEDIA APPLICATIONS

Social networking sites: Social networks have gained popularity since the late 2007 and are websites used for social interaction and networking. The most famous social networking sites include Facebook, Myspace, and LinkedIn. These sites are characterized by easy communication with others, staying updated on events, quick news transmission accompanied by vivid and expressive images, and real-time coverage directly from the location[2].

These social networks have empowered people to express their aspirations and demands in a free life by actively participating in sharing news, information, and contributing to the creation and management of media content. They have made people more engaged and involved in various issues.[3]

Blogs: Blogs are personal diaries on the web, created using simple programs that enable individuals to write personal information and opinions. The first blog of this kind dates back to October 1994 and is attributed to Dave Winer, a programmer who developed one of the most popular software programs called Manila. A blog is an internet application that works through a content management system. In its simplest form, it is a web page on the internet that displays dated and organized entries in ascending order. The number of published entries is controlled by the blog's administrator or publisher. The system also includes a mechanism for archiving old entries and ensures the stability of links without their degradation.[4]

Online Encyclopedias: These are websites that allow users to add and edit content. They function as collective shared databases. The most well-known example is Wikipedia, which includes millions of articles in various languages. Many websites have adopted wiki software, aiming to simplify the process of collaboration and cooperation in content development to the maximum extent.[5]

[1] International Foundation for Electoral Systems. Social Media - A Practical Guide for Electoral Management Bodies. Stockholm, Sweden, 2015, p. 72.

[2] Brintzenhoff، William ." Automated Language Processing; Exploring the Relationship of Social Media and Conflict in a Comparative Analysis of language Arabic Social Media and Conflict Events Reported in New Media "paper presented at the annual meeting of the international studies Association annual conference "Global Governance; Political Authority in Transition Montreal، Canada.2011. p 125.

[3] Al-Yousef, Shuaa. Modern Technologies: Benefits and Harms - Study of Negative Effects on Individual Health." Book of Al-Ummah, Qatar, 2006, p. 63.

[4] Same previous reference, p. 66.

[5] Al-Ghamdi, Qinan Abdullah. "Compatibility and Incompatibility between Traditional Media and Electronic Media." Research Paper presented at the Conference on Media and Cybersecurity, Prince Naif University for Security Sciences, Riyadh, 03-03-2012, p. 08.

Forums: Forums are specialized programs that allow the presentation of ideas and opinions on issues or topics for discussion on the website. Users or participants are given the opportunity to respond to and discuss them in real-time, whether in favor or against the presented ideas or opinions, with minimal restrictions imposed by the forum administrators through the control and management system of the program. Forums are one of the applications of participation, interaction, and alternative media introduced by the internet, providing an avenue for people to express their opinions. They emerged around 1995 when forums began to appear.[1]

THE SECOND TOPIC: CONCEPT OF INTELLECTUAL SECURITY

FIRST REQUIREMENT: THE MEANING OF INTELLECTUAL SECURITY

Security, in all its forms, has been a fundamental human requirement since the beginning of time. Intellectual security is considered one of the most crucial aspects because the essence of human beings lies in their thoughts. If one's thoughts are violated, their independence, freedom of speech and action, and even their beliefs are compromised. Intellectual security ensures that the intellectual energy of the individuals forming a society is protected from deviations and impurities that may lead to behaviors conflicting with the values and goals of that society. Intellectual security serves as the foundation for all other forms of security because individuals are a reflection of their thoughts, and a society is a reflection of its members. Therefore, both official and unofficial state institutions have the responsibility to safeguard the intellectual security of their individuals as a vital requirement for preserving their identity, value system, social structure, and national security.

SECOND REQUIREMENT: INTELLECTUAL SECURITY AND INFORMATION OVERLOAD

The information explosion we are experiencing today has dramatically changed the world around us. It has saved us time, effort, and money in delivering information, and has shortened distances. However, it has also inundated us with information that is supposed to be useful but often proves otherwise. The internet is filled with websites that spread rumors, scandals, and fakes news. They may invade people's privacy and exploit it for profit or to increase followers. The situation may have been less harmful before the emergence of social media, where information channels were unidirectional, from sender to receiver, without much interaction. However, with the interactive nature of social media platforms available to everyone today, deviations in this regard have escalated to the point where social media has become a medium for social disintegration and even criminal activities in not a few cases.

[1] Same previous reference, p. 15.

THE THIRD TOPIC: NEGATIVE EFFECTS OF SOCIAL MEDIA ON INTELLECTUAL SECURITY

FIRST REQUIREMENT: SOCIAL AND CULTURAL IMPACTS

Spreading Rumors and Fake News: There is no doubt that social media plays a crucial and dangerous role in shaping public opinion, mobilizing and rallying groups around specific ideas, opinions, and trends, regardless of their geographical dispersion. This poses a significant threat to intellectual security when these platforms are used to spread rumors and false news[1]. Electronic rumors contribute to the destruction of the value system and social order. They seek to generalize feelings of frustration in society, create a barrier that obscures the truth, and create a confusing environment for members of society. They also affect the credibility of public opinion and pave the way for the spread of lies and news based on malicious intentions. All of this generates negative energy in society, contributing to its destabilization. The danger of rumors increases when they target symbols and leaders of a particular state or touch upon issues related to social security and the existential issues of citizens, leading to the incitement of strife, animosity, and deepening divisions among different segments of society.[2]

Cultural Separation and Dilution of Identity: Identity is the common denominator of general characteristics that distinguish a civilization of any nation from other civilizations. Islamic identity means believing in the creed of this nation, taking pride in belonging to it, respecting its civilizational and cultural values, highlighting Islamic rituals, taking pride in adhering to them, and feeling distinctiveness, individual and collective independence. Islamic identity is the result of the historical experience of the nation, and it is distinct from other identities. This distinctiveness preserves the nation's survival, culture, and uniqueness, preventing it from dissolving into the cultures or identities of other nations. Moreover, it is defined by clear characteristics that accurately determine its function, purpose, and goal in this life.[3]

Access to social media has opened up the world without restrictions, allowing a close look at the cultures of other nations, their systems of life, and getting to know their behaviors. This has led to a state of coexistence and interaction between these cultures, and the matter has gone beyond interaction to admiration.[4]

[1] Al-Mudini, Osama Ghazi. "The Role of Social Media in Shaping Public Opinion among Saudi University Students." Journal of Arts and Social Sciences, Volume 5, Issue 856, Sultan Qaboos University, 2015, p. 68.

[2] Abdulhamid, Suheir Safwat. "The Role of Social Media in Spreading Rumors and Ways to Confront Them." Conference on Guidelines for the Use of Social Media in Islam, Riyadh, 06-05-2016, p. 31.

[3] Abdulhamid, Suheir Safwat. "The Role of Social Media in Spreading Rumors and Ways to Confront Them." Conference on Guidelines for the Use of Social Media in Islam, Riyadh, 06-05-2016, p. 31.

[4] Al-Khayyat, Sami. "Threats of Social Media Networks to Civil Peace and Social Security." Conference on Guidelines for the Use of Social Media in Islam, Riyadh, 06-05-2016, p. 103.

SECOND REQUIREMENT: RELIGIOUS AND PSYCHOLOGICAL EFFECTS

The chaos of fatwas and intellectual confusion: Due to the chaos of fatwas through social media, our youth have become scattered in their goals and purposes. They are unable to distinguish between right and wrong, which can lead to a crisis of thought, causing some young people to rebel against society and its values.[1]

Spread of extremist ideologies: Extremist ideologies are usually associated with closed-mindedness, intolerance towards others, and rejection of differing opinions, ideas, and perspectives. Extremists view society negatively, rejecting the idea of diverse opinion and perspectives, refusing dialogue and coexistence, and being unwilling to change their views and beliefs. This can lead to degrading and marginalizing others based on political, religious, ethnic, or sectarian reasons. The behavioral extremism, manifested through violence such as killing, bombings, and the use of various violent means, is a reflection of the saturation of prior extremist thoughts and beliefs.[2]

Social media platforms have provided a golden opportunity for extremists to spread their misleading ideas that contradict ethical, social, and moral values. This tarnishes the image of Islam, alienates people from it, and provides enemies of Islam with a chance to attack and undermine it.[3]

Electronic addiction as a gateway to intellectual deviation: One of the negative aspects of social media that affects intellectual security is electronic addiction. Spending long periods of time on these networks makes young people susceptible to ideas that can infiltrate their lives.[4]

Electronic addiction is a phenomenon that leads to psychological disturbance and is similar to psychological addiction associated with substance abuse. Electronic addicts increase their usage hours to satisfy their growing desires, experience stress and anxiety when disconnected from the internet, and become overly fixated on online activities.[5]

[1] Al-Muaiyathir, Reem Abdullah. "The Impact of Social Media on Intellectual Security among Female University Students." Journal of Education, Volume 88, Issue 1009, Al-Azhar University, Egypt, 2015, p. 66.

[2] Munad, Salima Abu Shakrah. "Media Treatment and its Contribution to Promoting or Combating Intellectual Extremism." The 12th Doha Conference on Interfaith Dialogue, Qatar, 03-04-2016, p. 124.

[3] Ahjo, Rokia. "The Impact of Social Media on Undermining Intellectual Security." The 12th Doha Conference on Interfaith Dialogue, Qatar, 03-04-2016, p. 155.

[4] Al-Sha'ir, Zuhair. "Practices of Using Websites and Social Media in Confronting Intellectual Insecurity." Conference on Guidelines for the Use of Social Media Networks in Islam, 06-05-2016, p. 45.

[5] Bouguezza, Reda. "The Internet and its Relationship to the Acquisition of Deviant Behavior among Adolescents." PhD thesis, Mohamed Lamine Debaghine University, Setif, Algeria, 2017, p. 99.

THIRD REQUIREMENT: CRIMINAL EFFECTS

Crime as a deviation in human behavior: Crime involves actions or omissions that violate protected rights or interests and are deemed illegal by the legal system. The legal system acknowledges the illegitimacy of such acts, and they are subject to penalties based on legal provisions. Legislators usually criminalize acts that violate individual rights, public interests, or societal norms.

Cybercrimes are a category of crimes, where the means used may vary, but their victims are diverse. Cybercrimes can target intellectual property or individuals by obtaining personal information through illegal means, followed by extortion of the victims both financially and morally. In some cases, particularly in conservative societies, if the victims are minors or females, the series of extortion may lead to suicide or other crimes related to honor.

These crimes can also target nations and their institutions by attacking infrastructure and network systems. Government employees and citizens may be targeted to destabilize governance systems. Additionally, hidden recruitment of terrorist groups can occur on social media platforms.

It's important to note that many legislations, especially in Arab countries or those aiming to protect their ethical systems, have not kept up with the pace of cybercrime in the digital world. As a result, they become vulnerable to cybercriminal activities without the ability to enforce deterrent punishment based on the principle of legality. Examples include crimes like "adultery" and "honor crimes" committed through various social media platforms.

THE FOURTH TOPIC: PROPOSED MECHANISMS TO MITIGATE THE RISKS OF SOCIAL MEDIA ON INTELLECTUAL SECURITY

In order to achieve rational use of social media, effective efforts should be consolidated to establish a set of principles related to the use of these platforms and impose enhanced mechanisms for that purpose. Therefore, in this article, we propose the most effective mechanisms based on what the international community has presented up to the present day.

FIRST REQUIREMENT: EDUCATIONAL MECHANISMS FOR REGULATING THE USE OF SOCIAL MEDIA

"Digital citizenship" is considered one of the most important educational mechanisms for regulating the use of social media and reducing its harms. It includes a set of values distributed across nine main axes as follows:[1]

Axis of Digital Culture: It requires "eradicating digital illiteracy" to help raise a responsible digital citizen who uses social media platforms correctly, thereby avoiding becoming a victim of misuse.

[1] Rida Bogherza, previous reference, p. 120.

Axis of Digital Access: Digital access is one of the most important mechanisms to eliminate digital illiteracy.

Axis of Digital Behavior Rules: The virtual world has ethics and manners that digital citizens must adhere to in order to be respectful and preserve the rights of others. In this context, "digital psychology" has recently emerged, which enables us to address inappropriate digital behaviors in the virtual world.

Axis of Digital Health and Well-being: Digital citizenship is concerned with protecting individuals from the risks of "digital life" by training them to use advanced technologies reasonably and responsibly, and by raising awareness about the negative effects on their health and social relationships.

Axis of Digital Commerce: Digital citizenship is concerned with protecting the digital economy and the digital consumer by training them to deal with trustworthy commercial websites and not to be swayed by advertising offers.

Axis of Digital Communication: Individuals have the right to receive and send information in various forms within the limits allowed by the law and in accordance with the rights and responsibilities defined in this field. This communication is realized through social media platforms, and in return, individuals are required to bear the full ethical and legal responsibility for the content of their communication.

Axis of Digital Rights and Responsibilities: The standards of appropriate behavior in the use of information technology require us to respect various rights, especially those related to intellectual property, with the possibility of disseminating personal opinions, intellectual and scientific products, with or without compensation.

Axis of Digital Security: It focuses on developing digital security awareness in order to ensure the safety of programs and personal information.

Axis of Digital Law: It focuses on disseminating sufficient awareness of digital law, which regulates most aspects of digital citizenship. Any violation of this law entails penalties according to the specified procedural and objective texts.

SECOND REQUIREMENT: DIGITAL DIPLOMACY FOR REGULATING THE USE OF SOCIAL MEDIA

Social media platforms and websites enable reaching the largest possible number of individuals at the same time. Digital diplomacy should utilize these tools professionally, thus having a positive impact on individuals and institutions. This allows for a response to various intellectual and political campaigns that may affect the interests of individuals and the state, thereby solidifying the concept of citizenship among individuals and enhancing the relationship between the state and its partners in various fields and specialties. This reduces the chances of negative ideas being disseminated by extremist and terrorist groups.

Moreover, digital diplomacy plays an active role in correcting concepts and clarifying policies, especially when it comes to mobilization campaigns that manipulate public opinion and provide misleading interpretations contrary to reality. This leads to tarnishing the image of the state internally and externally, especially since most members of society no longer rely on traditional media channels such as television and radio stations but have turned to social media platforms as a source of information. Based on this information, beliefs are formed, which are the source of all actions and reactions. Therefore, diplomacy must be present and strong on all social media platforms and work to clarify any point that may mislead public opinion, whether domestically or internationally, and this intervention should swift and in effective methodologies.[1]

THIRD REQUIREMENT: DETERRENCE MECHANISMS FOR REGULATING THE USE OF SOCIAL MEDIA PLATFORMS

Criminalization is considered the most important legal mechanism for regulating the behavior of offenders. However, it is not easy in the virtual world, which has led many international organizations, including countries, to seek the development of legal, objective, procedural, compatible, and effective texts to combat criminal deviance on various networks and social media platforms. Among the important texts recommended for adoption in this regard are:

United Nations Resolutions: The United Nations seeks to secure the safety of using technology and information networks by establishing standards for protection. It has issued a series of resolutions, including:

- Resolution 45/121 in 1990, and the publication of the Guide to Preventing and Combating Computer-Related Crimes in 1994.
- Resolution 57/239 on "Building a Global Culture of Cybersecurity" in December 20, 2002, and General Assembly resolutions 57/239 on January 31, 2003, and 58/199 on January 30, 2004, regarding "Building a Global Culture of Cybersecurity," which calls for cooperation and the promotion of a cybersecurity culture.
- Paragraph 18 of the "Vienna Declaration on Crime and Justice: Meeting the Challenges of the 21st Century," adopted by the General Assembly in Resolution 55/59 on December 4, 2000, and paragraph 36 attached to General Assembly Resolution 56/261 on January 31, 2002, on "Action Plans for the Implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the 21st Century."

[1] "Lahcen Nani. Protecting the Digital Economy: Between Criminal Policy and Digital Citizenship," Journal of Electronic Economics, Istanbul Institute for Economic Studies and International Cooperation, Issue 1, Volume 1, 2018, p. 124.

- Commission on Narcotic Drugs Resolution 48/5 on "Enhancing International Cooperation for the Prevention of Drug-Related Crimes through the Internet."

International Telecommunication Union Plan: The International Telecommunication Union provides a "strategic" platform for cooperation among its members as a specialized agency within the United Nations. It works to assist governments in agreeing on common principles that benefit governments and industries relying on information technology and communication infrastructure. The International Telecommunication Union has developed a plan "to enhance global cybersecurity" consisting of seven main objectives, including:

- Developing strategies for developing cyber legislation that can be applied locally and globally.
- Developing a global strategy to facilitate the capacity building of human and institutional capabilities to enhance knowledge and awareness in various sectors and fields of information.

Budapest Convention on Cybercrime: The European Committee on Crime Problems worked on the draft of the convention adopted by the European Parliament in 2001. The convention aims, in particular, to harmonize elements of local criminal law with provisions related to cybercrimes, provide the necessary legal procedures for investigation and prosecution of computer-related crimes, and include general principles related to international cooperation on various topics related to the content of the convention.

Arab Convention on Combating Information Technology Crimes: Adopted in Cairo on December 21, 2010, the convention requires each contracting state to adopt legislation and procedures in its domestic law for the crimes specified in the convention. It also covers any other crimes committed through information technology and the collection of evidence electronically. The convention emphasizes the necessity of bilateral cooperation and assistance.

The Arab Convention on Combating Information Technology Crimes: Edited in Cairo on December 21, 2010, which obliges each member state to adopt in its domestic law the legislation and procedures stipulated in the Convention regarding the specified crimes, in addition to any other crimes committed through information technology and the electronic collection of evidence. The Convention also emphasized the necessity of bilateral cooperation and assistance.[1]

The Penal Code Amendment and Completion Law (Democratic and Popular Republic of Algeria): The Algerian Penal Code was amended in 2004 by Law No. 04-15[2] to include objective rules regarding offenses against computer

[1] The Public Prosecution of the State of Palestine. Electronic Crimes Prosecution, accessed on November 25, 2022, www.pgp.ps.

[2] The General Secretariat of the Algerian Government. Law 04-15 amending and completing the Penal Code, Official Gazette, Issue 71, 2004, p. 8.

systems. It was further amended by Law 20-06, which introduced Article 196 bis, criminalizing and penalizing the dissemination of false or malicious news or information to the public that could undermine public security or public order. Prior to that, the Algerian legislator had issued Law 20-05 concerning the prevention of discrimination and hate speech[1], which imposed severe criminal penalties of up to ten (10) years of imprisonment for anyone who establishes, manages, or supervises a website dedicated to disseminating information promoting discrimination and hatred in society.

THE FIFTH TOPIC: CONTROL MEASURES FOR SOCIAL MEDIA USE

Monitoring deviant or criminal users of social media platforms does not give any party the right to violate the rights and privacy of others. Instead, it should primarily focus on the Universal Declaration of Human Rights adopted in 1948, which states in Article 19: "Everyone has the right to freedom of opinion and expression, including the freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers." This confirms the principle of equality among individuals in accessing information.

Therefore, countries and their agencies should not abuse the use of precautionary or deterrent measures to the extent of violating the rights and freedoms of individuals, especially considering the international trend towards redefining the framework of public freedoms in the digital realm. This includes the right to access the internet, freedom of expression and communication, the right to privacy, and the protection of personal data.

Moreover, it is necessary to strengthen human values and methods of preserving the warmth of social and familial relationships while preserving time. Additionally, the role of family supervision and regulation by service providers and official bodies should be activated to control these platforms from the technical and technological chaos we currently experience.

Conclusion:

Protecting intellectual security from the risks of social media is an important issue in our current era, where individuals and institutions are exposed to numerous threats and risks through these mediums. Here are some measures that can be taken to protect intellectual security.

Awareness and Training: Individuals and institutions should be aware of the risks of social media and receive the necessary training to safely navigate them. Training courses can be provided for employees and individuals in institutions to enhance awareness of social media risks and teach them how to use them safely.

[1] The General Secretariat of the Algerian Government. Law 20-06 amending and completing the Penal Code, Official Gazette, Issue 25, 2020, p. 10.

Policy Development and Guidelines: Institutions and organizations should develop strict policies and guidelines for the use of social media. These policies should include clear directives on what can and cannot be shared or published on these platforms, as well as clarifying the potential consequences of violating these policies.

Verification of Credibility: Before sharing or circulating information on social media, it is important to verify the credibility of the source and the accuracy of the information. Tools such as search engines and fact-checking websites can be used to ensure the accuracy of information before sharing it.

Privacy Preservation: Individuals should be cautious when sharing personal information on social media. Evaluating privacy settings and restricting access to personal information from unwanted individuals is essential.

Use of Security Tools: There are various tools and applications aimed at protecting intellectual security on social media. Anti-virus programs and content filtering software can be used to minimize potential risks.

Time Management: Individuals should be aware of how they use their time on social media. These platforms can be detrimental to productivity and focus, so setting specific times for their use and avoiding excessive immersion is important.

Reviewing Settings and Updates: Users should regularly review and update the security and privacy settings of their social media accounts. Policies and settings on these platforms can change, so users should stay informed about the latest developments.

Protecting intellectual security on social media relies on awareness, caution, and adherence to digital security principles. It is crucial for individuals and institutions to be aware of the risks and threats and follow best practices to safeguard their intellectual security and protect their sensitive information.

References:

1. Abdelhamid, Sohair Safwat (2016): The Role of Social Media in Promoting Rumors and Ways to Counter Them, Conference on the Controls of Using Social Networking Sites in Islam.
2. Ahjou Raqia (2016): Social Media and Its Impact on Undermining Intellectual Security, 12th Doha Dialogue on Religions, Qatar.
3. Al-Afaisan, Suleiman Mutab (2009): Awareness of the Concept of Comprehensive Security among Students of King Saud University, Master's thesis, Naif Arab University for Security Sciences, Riyadh.
4. Al-Ani, Khalil (2009): Islamic Identity in the Era of Cultural Globalization, Center for Islamic Research and Studies, Iraq.
5. Al-Ghamdi, Qinan Abdullah (2012): Compatibility and Contrast between Traditional Media and Electronic Media, Research Paper presented at the

Media and Electronic Security Seminar, Prince Naif bin Abdulaziz University for Security Sciences.

6. Al-Khayat, Sami (2016): Threats of Social Networking Sites to Civil Peace and Social Security, Conference on the Controls of Using Social Networking Sites in Islam.
7. Al-Muaither, Reem Abdullah (2015): The Impact of Social Networking Sites on Intellectual Security among Female University Students, Faculty of Education Journal, Al-Azhar University.
8. Al-Mudhni, Osama Ghazi (2015): The Role of Social Networking Sites in Shaping Public Opinion among Saudi University Students, Journal of Arts and Social Sciences, Sultan Qaboos University.
9. Al-Sha'er, Zuhair (2016): Practices of Using Websites and Social Media in Confronting Intellectual Security Challenges, Conference on the Controls of Using Social Networking Sites in Islam.
10. Al-Yousuf, Shuaa (2006): Modern Technologies: Benefits and Harms, Study of Negative Effects on Individual Health, Book of the Nation, Qatar.
11. Bougarza, Reda (2017): The Internet and Its Relationship to the Acquisition of Deviant Behavior among Teenagers, PhD thesis, Mohamed Lamine Debaghine University, Algeria.
12. Brintzenhoff، William (2011)" Automated Language Processing; Exploring the Relationship of social media and Conflict in a Comparative Analysis of language Arabic social media and Conflict Events Reported in New Media "paper presented at the annual meeting of the international studies Association annual conference "Global Governance; Political Authority in Transition Montreal، Canada.
13. General Secretariat of the Algerian Government (2004): Law 04-15 Amending and Supplementing the Penal Code, Official Gazette.
14. General Secretariat of the Algerian Government (2020): Law 20-05 on Prevention of Discrimination, Hate Speech, and Their Combating, Official Gazette.
15. General Secretariat of the Algerian Government (2020): Law 20-06 Amending and Supplementing the Penal Code, Official Gazette.
16. International Foundation for Electoral Systems (2015): Social Media - Practical Guide for Electoral Management Bodies, Stockholm, Sweden.
17. International Telecommunication Union, (2019): International Telecommunication Union Bulletin, November 1, 2019, www.itu.int.
18. Lahcen Nani (2018): Protecting the Digital Economy between Criminal Policy and Digital Citizenship, Electronic Economy Journal, Istanbul Institute for Economic Studies and International Cooperation, Issue 1, Volume 1.

19. Minad, Salima Abu Shaqra (2016): Media Treatment and its Contribution to Promoting or Combating Intellectual Extremism, 12th Doha Dialogue on Religions, Qatar.

20. Palestinian Public Prosecution (2021): Electronic Crimes Prosecution, November 25, 2021, www.pgp.ps.