

Digital Citizenship: A Societal Mechanism for Protecting Society from Cybercrime



Sara ADJEROUD

University of Batna 1, Algeria sara.adjeroud@univ-batna.dz

Reasearch Lab. LSRMPUDI

Received date: 28/05/2025

Accepted date: 17/06/2025

Publication date: 01/07/2025

Abstract:

In recent years there have been successive leaps in communication and information technology, accompanied by changes in individuals' abilities to interact with technology towards ease, convenience, and speed in communication and accessing information sources. Undoubtedly this modern technological revolution has resulted in behaviors that vary between positive, when utilized effectively, and negative, when users rebel against the ethical rules and legal regulations governing human affairs. The difference between these outcomes lies in how individuals choose to use it. Therefore, this study focuses on understanding the impact of this revolution on society and how a digital citizenship approach can be relied upon to address some of the negative effects on the community.

Keywords: Citizenship; digital citizenship; Electronic crime; society.

* Corresponding author: Sara Adjeroud, sara.adjeroud@univ-batna.dz

Introduction:

With the increasing reliance on information and communication technology that has invaded the world since the mid-1990s, and the rapid use of communication technologies alongside societal dependence, there has been a shift in the perception of the importance of digital citizenship as a mechanism to protect society from the risks of the internet. Here, we recall the statement by the French journalist "David Colombini" in his book "Digital Citizen": "The world is currently experiencing a significant and critical turning point in its entire history, moving towards a new civilizational model by adopting internet culture, or what is known as the digital empire, which has placed prevailing human cultures, established for thousands of years, in the face of real challenges. Various sectors of human activity have undergone a genuine shock, and each sector must confront what the author calls 'digital invasion' in its own way. The transformations that have occurred are both significant and qualitative."

From this statement, it is clear that the term digital citizenship emerged during the search for successful and preventive policies against the dangers of technology and the new digital revolution, This is due to the fact that many values of societies and the lifestyles of their individuals have become highly endangered due to the infiltration of digital revolution mechanisms into the fabric of societies. These societies have taken preventive measures to protect what is called "social privacy," as safeguarding this privacy preserves many of the fundamentals of these communities. This is because the values that traditionally fell under the term citizenship have transformed due to the digital revolution, making this citizenship digital, the love for the homeland digital, and expressing loyalty to the group manifested through "likes and comments," while defending the homeland and its interests occurs through electronic denunciation and publishing across interactive spaces.

Thus, the following problem is raised: How can digital citizenship contribute to protecting society from cybercrime? To answer this problem, the following axes have been adopted:

Section 1: An Etymological Approach to the Study

Section 2: Causes of the Rise of Cybercrime in Society

Section 3: The Role of Digital Citizenship in Protecting Society from Cybercrime

Section 1: An Etymological Approach to the Study

a. On the Concept of Digital Citizenship:

Before delving into the concept of digital citizenship, we will first define the term citizenship.

1. Citizenship:

- Citizenship is defined as: "A social, political, and legal connection that carries the meaning of the legal right of nationality, existing between an individual and the state, granting them religious, economic, and cultural rights, as well as the exercise of their political rights, provided they are not completely or partially deprived of this right due to the loss of their fundamental legal right (loss of nationality) or due to a criminal conviction (loss of civil rights) (Ould Yeb, 2010, p. 59).
- In contemporary thought, it is also defined as: "The belonging of an individual to a specific regional state, which requires the existence of a state in the modern sense, an active homeland or a defined territory, and a social relationship between the individual and the state, along with a commitment to peaceful coexistence among members of society. This includes participation in rights and duties, respect for the state system, and the relationship with the ruler at the constitutional, legal, and political levels. The citizen expresses their opinions and interests freely under established guarantees" (Jidour, 2016, p. 700).
- Digital citizenship can also be defined as: "The belonging of an individual to the state in which they were born or to which they have migrated, subject to the laws issued by that state, enjoying equal rights with other citizens and being committed to fulfilling their duties. It thus represents the relationship between the individual and the state as defined by the laws of that state." (Fawzi, 2007, p. 10).

2- Digital Citizenship:

Based on the previous definitions of citizenship, we can define digital citizenship as follows:

- Digital citizenship is defined as: "... a form of social identity shared by individuals regardless of gender, custom, or religion. It encompasses a set of rights and obligations and represents a collection of norms, values, ideas, and principles that guide the optimal use of technology. It also involves practicing positive citizenship values through interaction with the internet, represented by the rights and duties that must be adhered to. The degree of awareness of digital citizenship can be measured through assessments individuals receive regarding ethical, technical, political dimensions, and general awareness concerning the role of internet networks..." (Abdul Zahra & Saadi, 2021, p. 04).
- Digital citizenship is also defined as: "A collection of ideas, principles, programs, and methods that parents, teachers, and technology supervisors need to understand in order to guide children, students, and technology users in general. In other words, it is an approach that aims to hold parents and supervisors accountable in addressing this massive challenge. It also seeks to guide scientific

research to find optimal means for directing and protecting youth, striving to identify the best ways to protect teenagers and children without resorting to strict control, especially since it has practically become impossible to control what children and teenagers access on the internet and via mobile phones." (Al-Maghawry, 2016, p. 09).

- Others define digital citizenship as: "A set of rules, standards, norms, ideas, and principles followed for the optimal and proper use of technology, which citizens, both young and old, need in order to contribute to the advancement of the nation. In short, digital citizenship is guidance and protection—guidance towards the benefits of modern technologies and protection from their dangers; it is intelligent interaction with technology.") (Al-Maghawry, 2016, p. 10).

From the previous definitions of digital citizenship, its objectives can be identified as follows: (Fahd Fayez, 2023, p. 211).

- ✓ Raising awareness among learners about digital citizenship by focusing on concepts, skills, and values.
- ✓ Equipping learners with continuous learning skills and optimal ways to handle digital information.
- ✓ Representing the state in the best light through proper digital behavior.
- ✓ Maintaining national security by combating harmful ideas that infiltrate minds through the internet.
- ✓ Informing learners about safe job opportunities available online.
- ✓ Addressing many social and cultural issues facing society by enhancing awareness and values regarding duties and responsibilities.
- ✓ Promoting volunteer services and charities to serve the community by leveraging the virtual world, which supports extensive collaboration among community members while saving time, effort, and money.
- ✓ Transforming the concept of strict monitoring and lack of privacy into a concept of self-monitoring in accordance with Islamic principles and social values.
- ✓ Equality in rights and digital access for all segments of society.
- ✓ Avoiding academic theft and harming the digital work of others.
- ✓ Enhancing protection in the e-learning environment by providing a social space free from violence, racism, and extortion, among others.
- ✓ Making informed decisions when purchasing online.
- ✓ Reducing the physical and psychological risks caused by digital addiction.

3- Digital Citizenship vs. Traditional Citizenship: A Comparison of Similarities and Differences

It can be said that traditional citizenship means being a citizen of a specific country, with associated rights, duties, and responsibilities. In contrast, digital citizenship refers to the same concept but in the digital context, where we have rights and duties in the online world, such as protecting privacy and avoiding negative behaviors on social media platforms.

Below is a comparison highlighting the similarities and differences:

Point of Comparison	Traditional Citizenship	Digital Citizenship
Definition	It is a live practice carried out by the citizen, fulfilling their duties in exchange for obtaining the rights guaranteed by the constitution and law, reflecting the connection and commitment between them and the state. They integrate into society and participate actively and positively at all human and community levels, driven by their strong belonging, loyalty, and love for their homeland.	It is the interaction of individuals with others using digital tools and resources, such as computers in their various forms, as well as the information network as a medium for communication with others using various technological means.
Nature of Society	A real interactive community where individuals interact face-to-face, without any intermediaries.	A virtual digital community where individuals interact by using technological means as a medium.
Nature of Individuals	Real individuals.	Virtual characters represent real people.
Interaction Environment	Natural/Traditional.	Electronic/Digital.
Trust	Complete security in all sources.	There is no complete security in all of its sources.
Engagement	It revolves around belonging, rights, and duties of individuals toward the homeland and land.	It revolves around the standards, skills, and rules of conduct necessary for dealing with technology.
Participation	Small participation.	Significant participation.
Intellectual Property Rights	Intellectual property rights are protected.	Intellectual property rights are not well protected.
Communication	Face-to-face communication.	Ease of communication from a distance, anywhere in the world.
Learning It	Values develop within the individual socially, through interactions in the community.	Courses and programs that evolve with age development.

Source: Prepared by the author

b. On the Concept of Cybercrime:

There are several definitions of cybercrime, including:

- Cybercrime is defined as "the intentional commission of a socially harmful act or a serious prohibited act punishable by law. Cybercrimes represent a set of illegal acts and activities carried out through electronic devices or the internet, or

broadcast through it. This type of crime requires specialized knowledge of computer technology and information systems to commit, investigate, and prosecute its perpetrators..." (Bounaâra, 2015, p. 277).

- It is also defined as: "Any unlawful, immoral, or unauthorized behavior related to the automated processing and transmission of data, where technology serves either as a means used to commit the act, or as the environment in which the crime occurs, or as the goal of committing the prohibited act. In other words, the medium is a technological device, such as a computer, which is always a means for committing electronic criminal acts, without neglecting other technical devices like third-generation mobile phones." (Abdel Qawy, 2015, p. 02).
- It is also defined as: "Offenses committed against individuals or groups of individuals motivated by crime, aimed at harming the victim's reputation or causing physical or mental harm to the victim, either directly or indirectly, using communication networks such as the internet (such as chat rooms, email, mobile phones, etc.)." (El-Badaina, 2014, p. 03).

Thus, by exploring the various definitions of cybercrime, a number of characteristics emerge, the most important of which are: (Jimawi, 2021, p. 133).

✚ The concealment of the crime and the rapid evolution in its commission are notable, as cybercrimes are often hidden and obscure, allowing the victim to be unaware of them even while on communication networks. This is because the perpetrator possesses technical skills that enable them to commit their crime with precision, such as sending destructive viruses, stealing or destroying money and private data, spying, and intercepting calls. Some of these crimes can occur in a second or a fraction of a second.

✚ Cybercrimes are committed in a digital information environment based on computer information systems, hardware, and software.

✚ They are carried out by criminals with specific characteristics and capabilities (informatic knowledge), who use their knowledge and professional methods to commit their crimes.

✚ Cybercrime requires innovative methods of evidence collection, relying on continuous specialized education and training in computer science. Therefore, it necessitates the presence of cyber police, electronic investigators, electronic judges, as well as electronic experts to uncover the crime, track the perpetrators, and prosecute them. Consequently, consulting experts becomes essential to uncover, analyze, and interpret forensic evidence that proves innocence or guilt.

✚ Obtaining physical evidence in such crimes is challenging, as the electronic nature of the evidence predominates. The difficulty of uncovering evidence increases, especially when the crime is committed in the workplace by employees against their own institutions. Due to the trust placed in them, it becomes easier for them to commit their crimes without leaving traces that could lead back to them.

2. Causes of the Rise of Cybercrime in Society

The spread of cybercrime can lead to a general disruption that threatens the entire society in terms of its economy, sovereignty, and national security. Cybercrimes

also contribute to family disintegration and conflicts among individuals due to defamation, the spreading of false news, the theft of personal files, and their publication on the internet and communication networks, among other negative impacts that threaten the security and safety of society. These effects arise from several causes at the societal level, including:

- a. **Urbanization:** This is one of the main causes of cybercrime in general. The significant migration from rural areas to cities and urban regions often involves young people who are unable to cope with the high costs of urban life, which sometimes require advanced skills. As a result, large segments of migrants find themselves unable to meet the demands of urban life, living instead in slums and marginal neighborhoods. Consequently, people find themselves in competition that they cannot keep up with, leading them to turn to investing in cybercrime, which does not require substantial capital.
- b. **Unemployment:** Like traditional crime, cybercrime is associated with unemployment and difficult economic conditions, particularly among large sectors of youth. Therefore, young people who possess knowledge may invest that in engaging in electronic criminal activities. (El-Badaina, 2014, p. 14).
- c. **General Pressures:** The general pressures faced by society, such as poverty, unemployment, illiteracy, and difficult economic conditions, create stress on the community, particularly on the youth sector. This generates negative feelings among large segments of the population against their circumstances and society, leading them to adopt negative coping strategies, such as human and sex trafficking, as well as cybercrime.
- d. **The Pursuit of Wealth:** Humans seek pleasure and avoid pain, as stated by the general theory of crime. People often turn to socially unacceptable means to achieve socially acceptable goals. According to Merton's "anomie theory," the desire for wealth faces significant obstacles when pursued through socially acceptable and legal methods. Consequently, some individuals resort to cybercrime, where the targets are larger, the execution is easier, the returns are quicker, and the risks are lower. (Rashad & Jibril, 2016).
- e. **Schools and Educational Institutions:** Alongside the teaching and educational activities, schools or educational institutions also have a formative role in shaping the youth personally. They instill a system of moral and behavioral values. The failure to adhere to public monitoring laws and allowing the introduction of electronic devices, especially smartphones, facilitates their use away from family supervision. This creates a clear path for sexual crimes directed against children, electronic blackmail, and cheating in exams. Schools play a significant role in mitigating or influencing criminal behavior, as Victor Hugo said: "For every school that opens, a prison closes." (Jimawi, 2021, p. 133).
- f. **Weak Law Enforcement and Application in Cybercrime:** Many countries have not developed their legislation and justice systems to keep pace with advancements in cybercrime and its methods. This issue extends beyond legislation to include police, investigations, and the judiciary, as well as how to handle digital evidence at the national level, similar to the situation at the international level. The

absence of criminal legislation and weak judicial, police, and prosecutorial practices in investigating and prosecuting cybercrimes often lead to inadequate technologies and a shortage of experts capable of monitoring and pursuing cybercrime within communities and across national borders (Rashad & Jibril, 2016).

These reasons have resulted in the danger of cybercrime at the societal level, as they impact individuals and their reputations, leading to defamation, violations of personal freedom, and crimes that undermine public morals and behavior. These crimes have increased with the rise of social media platforms such as Facebook and Twitter, as well as discussion forums. If these platforms are not used for beneficial purposes, such as gaining knowledge, culture, and connecting with friends, they can have serious social repercussions on families and communities.

3. The Role of Digital Citizenship in Protecting Society from Cybercrime

The negative effects resulting from modern technology pose a threat to society, particularly concerning ignorance in its use on one hand, and ethical threats on the other. Digital citizenship can help mitigate the impacts of cybercrime if certain fundamental aspects are provided, including:

- a. **Digital Access and Full Electronic Participation in Society:** Digital citizenship promotes equal opportunities for all individuals regarding access to and use of technology, ensuring equal digital rights and supporting electronic access while rejecting the principle of digital exclusion that hinders growth and prosperity. It aims to reduce the digital divide— the gap between those who can access and use various forms of technology and those who cannot. Technological access may be limited for some individuals due to economic or political conditions, which is why digital access rates are generally higher in developed countries compared to developing ones. Currently, there are many global programs aimed at enhancing the right to digital access for individuals in economically challenged countries or in those nations that restrict certain forms of technology from their citizens, such as internet access. (Shuqoura & Hassan, 2017, p. 17).
- b. **Digital Commerce:** Buying and selling goods electronically: A significant portion of today's market economy operates through technology and its various channels. Digital citizenship educates individuals about the issues related to this process, including the laws and regulations governing the use of technology, particularly regarding security and safety as well as state laws. Despite the numerous advantages of e-commerce, caution is necessary for those who wish to buy or sell online.
- c. **Digital Communication:** Electronic exchange of information: One of the most notable advancements in modern technology is the development of communication in all its forms and techniques. Thanks to this, the world has become a small village, providing everyone the opportunity to connect and collaborate with others anywhere in the world at any time. In this context, digital citizenship emphasizes the importance of individuals being able to make informed decisions among the many available digital communication options and being aware of how to use them (Abdel Qawy, 2015, p. 07).

d. **Digital Literacy:** The process of teaching and learning technology and using its tools: The modern measure of literacy is now linked to an individual's ability to use technology. Therefore, contributing to digital literacy is both an individual and collective responsibility. Efforts must be combined to provide learning, education, and training opportunities for the optimal use of technology and its various tools. As technology has permeated all areas of an individual's life, digital citizenship focuses on educating individuals and providing them with the digital skills they need, using technology appropriately, benefiting from its positives, and avoiding its negatives. It also aims to equip individuals with information literacy skills (Shuqoura & Hassan, 2017, p. 26).

e. **Digital Etiquette (Netiquette):** Digital standards of behavior and procedures: We all strive to conduct ourselves with courtesy when interacting with others in person, and some may need training to acquire this skill, as it is governed by standards and procedures. The same applies when interacting with others digitally. A digital citizen with good etiquette, whether in person or online, is important. Digital citizenship aims to promote a "culture of digital etiquette" among individuals and train them to act responsibly in a new digital society, respecting values, principles, and standards of good behavior (Al-Maghawry, 2016, p. 20).

f. **Digital Law:** Social responsibility regarding actions and behaviors: These are the laws in the digital society that address issues of digital ethics, aiming to expose and punish unethical use of technology, known as digital or cybercrimes, to protect individual rights and ensure digital security. There are several laws established by the digital community that must be observed, and any violators are subject to these laws, such as hacking into others' information, stealing data, or spreading viruses, among other cybercrimes. Digital law addresses four key issues: copyright, privacy, ethical issues, and piracy. A digital citizen respects digital laws, promotes them, and encourages others to adhere to them (Hashish, 2018, p. 417).

g. **Digital Rights & Responsibilities:** The freedoms enjoyed by everyone in the digital world: Just as the state defines the rights of its citizens in its constitution, the digital citizen also enjoys a set of rights, such as privacy and freedom of expression. It is essential to understand these rights correctly in the context of the digital world. Alongside these rights come duties and responsibilities; they are two sides of the same coin that cannot be separated. A digital citizen must learn how to use technology appropriately to become productive and effective (Zarqout, 2020, p. 236).

h. **Digital Health & Wellness:** Mental and physical health in the digital technology world: Improper use of technology can lead to physical and psychological problems affecting individuals. This has led to the emergence of ergonomics, which focuses on the physical and psychological compatibility between machines and the humans who interact with and use them. Digital citizenship emphasizes raising awareness and culture regarding the healthy and proper use of technology and applying ergonomic standards (Al-Maghawry, 2016, p. 24).

i. **Digital Security (Self-Protection):** Measures to ensure digital prevention and protection: No society is free from individuals who engage in unlawful activities

such as theft and defamation, and the digital community is no exception. Therefore, necessary measures must be taken to ensure the prevention, protection, and security of individuals. Just as we lock the doors of our homes and install alarms to provide a certain level of protection, similar procedures must be applied in the digital community. This includes backing up data, installing antivirus and anti-hacking software, and other measures in the digital realm. A responsible digital citizen must take security precautions to protect their data and privacy from any external invasion (Idais, 2015).

j. **Culture of Digital Citizenship:** Digital citizenship allows any citizen to become a producer of culture, facilitating the diversification of their creative inputs using modern digital technologies. It enables them to express their opinions on any other cultural product and even present their own creations, whether a short film on YouTube, an art exhibition shared on social media, or a creative blog inviting people to read it online. Thus, cultural actions transcend the boundaries that previously restricted such expressions, becoming a common activity shared by various social groups. Without guardianship from this side or that, and possessing intellectual independence away from all fundamentalist calls that try to tame individuals and diminish their sense of capability to be active, exceptional intellectuals—producers, distributors, and consumers at the same time—cultural production should be a free industry that adheres only to aesthetic trends and its ability to attract the attention of consumers anywhere on Earth. Digital citizenship, when addressed based on the legal principles of a new society characterized by freedom, justice, sovereignty, and civil culture, embodies these values (Abdul Zahra & Saadi, 2021, p. 13).

In addition to these major essential aspects, there are several key roles that digital citizenship can play in protecting society from cybercrime:

1. **Awareness and Education:** By promoting awareness of the risks associated with cybercrime and teaching individuals how to protect their personal information.
2. **Responsible Online Behavior:** Encouraging ethical use of the internet and fostering values of respect and cooperation among users.
3. **Reporting Crimes:** Motivating individuals to report suspicious activities and creating secure channels for reporting cybercrimes.
4. **Enhancing Cybersecurity:** Supporting initiatives aimed at improving cybersecurity at the community level and participating in workshops and training courses related to digital security.
5. **Community Engagement:** Collaborating with government and non-governmental organizations to combat cybercrime and engaging in community awareness campaigns to disseminate knowledge about digital security.
6. **Developing Laws and Policies:** Supporting the development of laws that protect individuals from cybercrime and participating in discussions about digital policies.

Conclusion:

What can be concluded from this study is that the tremendous development in the field of communications information technology, and its media has opened many avenues for benefit, However it has also led to the emergence of new types of crimes and fraud due to the openness imposed by these technologies, providing information that can be used for both the benefit and harm of humanity, thus establishing a new type of crime: cybercrime and information-related offenses, Cybercrimes differ fundamentally from traditional crimes, but the damage they cause should not be underestimated, Therefore it is essential to combine efforts to limit the spread of these crimes, especially with the information openness experienced by countries worldwide. We have found that digital citizenship plays a crucial role in mitigating these crimes, particularly at the community level, This involves implementing appropriate strategies to promote digital citizenship culture among all segments of society, preparing a responsible digital generation through programs and projects beginning with the family and extending to all educational institutions and civil society organizations,....Only then can we truly enhance the protection of society from the increasing negative impacts of technology while maximizing its benefits to contribute to the development of a knowledge society and building a digital economy for the nation Consequently, it is imperative for everyone individuals and institutions alike to assume responsibility for this vital issue.

Footnotes:

The term "crime" can be defined as an act that contradicts societal and legal standards, as well as constitutional norms. It involves infringing upon and violating the rights of others and is punishable by law due to the prohibition of such actions legally and religiously. Crimes are legally and religiously divided into four main types: economic crimes, sexual crimes, political crimes, and revenge crimes. It is noted that there are fundamental theories of crime, including the geographical, economic, and biological theories. For more details, see: (Ghaith, 1989)

• **Bibliography:**

1. Abdel Qawy, A. (2015). Cybercrime and International Efforts to Mitigate It. *Journal of Financial and Banking Studies (01)*.
2. Abdul Zahra, J., & Saadi, A. (2021). Digital Citizenship: A Theoretical Study. *Journal of Law and Political Science (01)*.
3. Al-Maghawry, T.-M. (2016). Digital Citizenship: Challenges and Aspirations. *Cairo: Alexandria University*.
4. Bounaâra, Y. (2015). Cyber Crime. *Al-Maiyar Journal (39)*. .
5. El-Badaina, D. (2014). Cyber Crimes: Concept and Causes. *Paper presented at the Scientific Forum on: Emerging Crimes in Light of Regional and International Changes*. Amman: Septembre 2-4.
6. Fahd Favez, A.-S. (2023). Digital Citizenship: An Analytical Study of the Concept. *Academic Journal for Research and Scientific Publishing (46)*.

7. Fawzi, S. (2007). *Citizenship*. Cairo: Cairo Center for Human Rights Studies.
8. Ghaith, M. A. (1989). Dictionary of Sociology. *Egypt: Egyptian General Book Organization*.
9. Hashish, N. (2018). Digital Citizenship Skills Required for Basic Education Students. *Journal of Studies in University Education Cairo* (39).
10. Idais, K. (2015). *Digital Citizenship*. Récupéré sur Al-Quds Open University. Retrieved from: <https://bit.ly/4mrgNdT>.
11. Jidour, H. (2016). *The Impact of the Digital Revolution and the Intensive Use of Social Networks on the New Concept of Citizenship*. From Ordinary Citizen to Digital Citizen" Political and Legal Notebooks (15).
12. Jimawi, N. (2021). Cyber Crime and Its Impact on Social Security. *Laboratory Notebooks Journal* (02). .
13. Ould Yeb, S. (2010). *The State and the Dilemma of Citizenship*. Amman: Dar Knowledge for Publishing and Distribution.
14. Rashad, M., & Jibril, I. (2016, August 9). *Cyber Crimes: Goals, Causes, Methods, and Treatment*. Récupéré sur The Democratic Arab Center. retrieved from: <https://bit.ly/4kzgrJ> Accessed on: 04/05/2025.
15. Shuqoura, A., & Hassan, H. (2017). The Role of Secondary School Teachers in Gaza in Promoting Digital Citizenship to Address the Phenomenon of Cultural Pollution Among Students and Ways to Activate It.
16. Zarqout, S. (2020). Results of Adopting a Culture of Digital Citizenship in Higher Education: A Case Study of the International City University. *Journal of Business Economics* (01).