

Digital Citizenship in the Context of Global Digital Transformation

المواطنة الرقمية في ظل التحول الرقمي العالمي

Menasria saamiha , lecturer A *

University of khenchela

E-mail: menasria.samiha@univ-khenchela.dz

The date of Submission: 18-04-2025

The date of revision: 28-06-2025

The date of publication: 10-07-2025

Abstract:

The acceleration of technological transformation globally has led to the emergence of new concepts, with **e-citizenship** standing out as a central idea. It involves the legal and ethical participation of individuals in the virtual space. This paper aims to establish a clear conceptual framework for **e-citizenship** by distinguishing it from its traditional counterpart and examining its legal, rights-based, and behavioral aspects. Furthermore, the study highlights the absence of cohesive legal regulation particularly in Arab countries and advocates for the development of a legal structure that protects the rights of digital citizens while outlining their corresponding responsibilities.

Keywords : Citizenship ; Digitization; Security; freedom of expression,

الملخص:

لقد أدى تسارع التحول التكنولوجي على مستوى العالم إلى ظهور مفاهيم جديدة، ويعد المواطنة الإلكترونية من أبرز هذه المفاهيم. فهي تشمل المشاركة القانونية والأخلاقية للأفراد في الفضاء الافتراضي. تهدف هذه الورقة إلى وضع إطار مفاهيمي واضح للمواطنة الإلكترونية من خلال تمييزها عن نظيرتها التقليدية، واستكشاف جوانبها القانونية والحقوقية والسلوكية. كما تسلط الدراسة الضوء على غياب التنظيم القانوني المتكامل خصوصاً في الدول العربية وتدعو إلى تطوير هيكل قانوني يضمن حماية حقوق المواطنين الرقميين ويحدد مسؤولياتهم المترتبة على ذلك.

الكلمات المفتاحية: المواطنة ، الرقمنة ، الامن ، حرية التعبير ،

* Menasria saamiha .

Introduction:

In recent decades, the technological revolution has triggered profound changes that have reshaped both public and private life, giving rise to new forms of social, political, and legal interaction. Amidst this widespread transformation, there has been a growing need to rethink the relationship between individuals, the state, and society within the virtual domain. Consequently, the concept of e-citizenship has emerged as both a conceptual, ethical, and legal response to this evolving reality.

Electronic citizenship is among the most notable examples of how classical concepts of civic belonging are being reshaped to fit a technologically advanced context—one defined by transparency, swift data flow, and varied means of communication and involvement. It encompasses more than the functional operation of online platforms; it involves a conscious understanding of individual entitlements and obligations in the online sphere, along with adherence to the normative and moral standards that regulate it.

Despite its growing prominence in modern academic and policy arenas, the notion still suffers from a lack of precise codification within the majority of national legislative systems. This lack of clarity prompts several inquiries regarding its theoretical exactness, the breadth of its implementation, and its effectiveness in promoting ethical behavior across virtual platforms while safeguarding fundamental rights and individual freedoms in the online sphere.

In light of this, the study seeks to answer the following central research question:

How can the concept of e-citizenship be articulated within a coherent and comprehensive legal structure?

Accordingly, this study seeks to address the following central question:

How can the concept of e-citizenship be articulated within a coherent and comprehensive legal structure?

This overarching question gives rise to a set of sub-questions:

- What are the theoretical underpinnings of e-citizenship in the context of worldwide technological evolution?
- In what ways has this evolution redefined the interaction between individuals and the state within online environments?

To explore these dimensions, the study employs a combination of descriptive and analytical methods, organized into two main sections:

Part One: The conceptual basis of electronic citizenship.

Part Two: The key elements of e-citizenship and its practical domains.

1. The conceptual basis of electronic citizenship. Revisiting Classical Citizenship

The rise of technological advancements necessitates a renewed examination of classical frameworks that define the relationship between individuals and the state—most notably, the concept of citizenship. In this context, **electronic citizenship** has surfaced as a modern paradigm that blends formal affiliation with active participation in online spaces. Establishing its foundations requires a clear articulation of its linguistic and conceptual boundaries, while also drawing distinctions between this emerging model and its traditional counterpart within the context of a rapidly evolving digital era.

1.1 - Traditional Citizenship

Traditionally, citizenship is understood as a legal and moral connection between an individual and their nation, grounded in mutual allegiance, the entitlement to rights, and the performance of responsibilities. Hans Kelsen defines it as “the legal bond that determines an individual’s political affiliation with the state¹, granting them access to civil and political rights in return for fulfilling legal obligations.” From a political theory perspective, it represents a status through which individuals engage in public affairs, assert their civic and political entitlements, and contribute to shaping collective decisions. In modern legal discourse, citizenship is regarded as a formal status that confers membership in a nation-state, accompanied by a range of rights and responsibilities protected by both domestic and international legal frameworks.

1.1.1- Citizenship

Electronic citizenship represents a contemporary extension of the traditional notion of civic belonging, shaped by the rapid advancement of digital technologies. It concerns the way individuals navigate virtual spaces in alignment with ethical norms and existing legal structures that regulate those environments. Mike Ribble—one of the foundational thinkers behind the term—defines it as “the ability to use technology in a responsible, ethical, and safe manner across various aspects of life, including education, social interaction, and civic engagement”²

Cyber citizenship constitutes a modern development of the citizenship model, born from the digital revolution. It's about how individuals behave in new environments in accordance with the ethical principles and regulatory frameworks that govern those spaces. Mike Ripple – one of the first architects of this concept – defines it as "knowing how to use technology responsibly, ethically, and safely in all areas of life, from education to social interaction and civic engagement."

1.1.2- Legal Definitions of E-Citizenship

From a legal perspective, e-citizenship refers to the recognized status of an individual operating within digital environments, combining ethical responsibility with lawful engagement. It involves the exercise of rights specific to online contexts—such as data privacy, freedom of expression, and access to information—balanced with obligations like adherence to cyber regulations and the avoidance of harm to others in virtual interactions. This concept also implies a mindful and active observance of one's duties, encompassing respect for personal data, the secure use of technological tools, and meaningful, responsible participation in online communities³.

¹ - Hans Kelsen General Theory of Law and State Harvard University Press, 1945, p180-185.

² -Cristina Hennig Manrique, Ana Vargas Sánchez ,Erika Duque Bedoya, Digital Citizenship, A Theoretical Review of the Concept and Trends in the Last Ten Years, ERIC – Education Resources Information Center 2019, Past Ten Years, published on the website, <https://files.eric.ed.gov/fulltext/EJ1211194.pdf>. (Accessed: 18 April 2025).

³ -Ana Maria and others, Adolescents' Digital Citizenship, A Conceptual Approach, IEEE – Proceedings of the 2021 XI International Conference on Virtual Campus (JICV) September 2021.

1.2- Traditional vs. E-Citizenship

As the world undergoes rapid technological transformation, the notion of e-citizenship has emerged as a modern evolution of the classical civic model, redefining how individuals relate to virtual spaces within ethical and legal boundaries.

Whereas conventional civic identity is rooted in territorial belonging and political involvement within a physical state, the digital counterpart expands the scope of participation to include rights and obligations in online spheres. This shift necessitates a comparative understanding, as it mirrors the changing dynamics between the individual and state institutions in the age of connectivity¹.

At its core, citizenship refers to the legal and political relationship binding a person to a state, granting rights and imposing duties. The traditional form of this relationship is defined by physical presence within national borders, civic responsibilities such as voting, taxation, and adherence to laws, and participation in public affairs.

In contrast, e-citizenship has been shaped by the growth of virtual engagement. It encompasses activities like expressing opinions online, protecting personal data, and contributing to public debates through digital channels. Unlike its territorial predecessor, this newer model operates across borders, creating legal complexities around jurisdiction, regulatory consistency, and the safeguarding of digital rights.

Ultimately, the distinction between the two is not merely about where or how civic engagement occurs, but reflects a deeper reconfiguration of the individual–state connection in an increasingly digitized world.

1.3- The relationship between electronic transformation and the emergence of digital citizenship

Technological transformation is one of the most prominent civilizational transformations that the world has witnessed in recent decades, as its impact was not limited to aspects related to it, but extended to reshaping traditional legal and social concepts, foremost of which is the concept of citizenship. In light of rapid digitization, new patterns of interaction between individuals and institutions have begun to emerge, relying on new media instead of traditional means, which has led to the emergence of the concept of "digital citizenship" in response to this transformation.

Researcher Manuel Castells pointed out that this revolution has not only changed the means of communication, but has changed the nature of the social and political space itself, as identities and practices are formed within cyber networks that do not recognize geographical boundaries. This is what prompted jurisprudence to view digital citizenship as a new form of citizenship, carried out through non-physical spaces, allowing the individual to exercise his rights, interact with the state, and participate in public life, in a different way, requiring a special legal framework².

The essence of the relationship between the remarkable transformation and the emergence of digital citizenship lies in the fact that it has not only produced new tools for

¹ - Mike Ribble, Digital Citizenship in Schools, Nine Elements All Students Should Know, International Society for Technology in Education (ISTE), 2011.

² -Castells, Manuel. The Rise of the Network Society, 2nd ed, Wiley-Blackwell, 2010, pp. 25-26.

interaction, but also created a different legal and societal environment that imposes a review of rights and duties, and calls for redefining the traditional One of the most pressing imperatives of this new reality is cultivating a legally.

Perhaps one of the most prominent imposed by this new reality is the need to build a legal culture, which makes the citizen not only a user of technology, but an active and responsible person, aware of his rights and duties within cyberspace, which Karen Mossberger stressed by saying: "Digital citizenship is a product of enabling individuals to use technology in a conscious and legal manner, which enhances their participation in this new society)¹.

2. Components of Digital Citizenship in the Context of Global Digital Transformation

Global digital transformation represents one of today's most significant challenges, reshaping the very contours of state and society and demanding a thorough reassessment of traditional legal concepts chief among them, citizenship. This shift has altered the modalities through which rights are exercised and has redefined the citizen's role within the public sphere, giving rise to the notion of "digital citizenship" as a framework suited to this evolving landscape. This section examines the dimensions of that change by analyzing how digitization affects the individual–state relationship and by detailing the specific rights and duties now practiced through digital channels.

2.1- Digital Rights and Obligations

Under digital transformation, citizenship no longer signifies solely a conventional bond between individual and state; rather, it is founded on a set of rights and obligations enacted within a complex cyber-environment that demands continually updated legal and ethical awareness.

- Digital Privacy: At the forefront is the right to digital privacy, a fundamental safeguard of personal dignity against unauthorized tracking or exploitation of one's data. As digital platforms proliferate, data protection has become central to contemporary legislation, exemplified by frameworks such as the European Union's General Data Protection Regulation (GDPR), which enforces binding standards for processing personal information online².
- Cybersecurity as Right and Duty: Cybersecurity functions both as a protective right and a shared responsibility. States must secure critical digital infrastructures and counter cyberattacks that threaten public safety, while citizens are expected to remain vigilant and comply with technical and legal protocols when engaging with digital media. Several modern constitutions—including that of Estonia (2015)—explicitly recognize digital security guarantees as part of citizens' fundamental rights within the online sphere.

¹ -Mossberger, Karen, et al. Digital Citizenship: The Internet, Society, and Participation, MIT Press, 2008, p 1

²- General Data Protection Regulation (GDPR), European Parliament and Council, Regulation (EU) 2016/679 of 27 April 2016.

Together, these rights and duties form the bedrock of responsible digital citizenship, ensuring that individuals can exercise their freedoms safely and ethically while contributing to the resilience of the digital public domain¹.

2.2 - Freedom of Expression and Digital Responsibilities

Freedom of expression in the digital sphere constitutes one of the most visible exercises of digital citizenship. However, like its offline counterpart, it operates within legal bounds designed to balance individual opinion with the protection of public order, the prevention of hate speech, and the preservation of human dignity. Legislators therefore face a dual challenge: opening channels for unfettered dialogue without permitting an “information chaos,” on the one hand, and avoiding undue restrictions on fundamental liberties, on the other. Achieving this balance requires a calibrated approach that upholds free speech while safeguarding information security and the public interest.

While digital rights represent the outward face of new-age citizenship, digital duties are of equal importance. A digital citizen must respect cyber-law provisions, exercise discretion when publishing content, and refrain from harmful practices such as disinformation, privacy breaches, or participation in cybercrimes which are subject to legal sanction. Moreover, citizens are expected to foster a positive digital culture that encourages respectful coexistence online and values pluralism of opinion.

- Digital Citizenship Education: Fostering Responsible Online Conduct

Amid accelerated digital change, simply providing access to technology is no longer sufficient; it is imperative to instill a culture of conscious and responsible use. Digital behavior now reflects not just personal habits but the individual’s engagement in public digital life within organized legal and ethical frameworks.

Digital citizenship education aims to equip individuals especially younger generations with a clear understanding of their rights and duties online, hone critical thinking skills to identify misinformation, safeguard personal data, communicate responsibly, and respect others in cyberspace. These objectives have been integrated into progressive educational policies worldwide. For instance, Canada and Finland have incorporated digital citizenship modules into their school and university curricula, recognizing responsible digital engagement as a strategic pillar in cultivating empowered and conscientious members of the digital community².

- Shared Responsibility in Digital Citizenship Education

Education in digital citizenship extends beyond formal schooling or institutional programs; it is a collective endeavor involving the state, educational institutions, media, families, and civil society. Strengthening responsible digital conduct demands an inclusive, multi-actor approach. Familiarity with cybercrime statutes, personal data protection principles, and digital communication ethics is crucial for bolstering societal cybersecurity.

¹ - Estonian Constitution, amended 2015, Chapter II: Fundamental Rights, §43-1 on Digital Security

² - Ribble, Mike, Digital Citizenship in Schools: Nine Elements All Students Should Know, International Society for Technology in Education (ISTE), 2011, pp. 15–28.

Digital citizenship education functions as a preventive shield against ethical lapses and legal breaches online. It is the primary mechanism for instilling respect for the rule of law, tolerance, pluralism, and accountability thereby balancing digital freedoms with the requirements of harmonious coexistence in an advanced technological society.

2.3- Legal Challenges of Digital Citizenship: Balancing Rights Protection with Regulatory Complexity

As the digital realm grows exponentially and individuals engage across every facet of life, intricate legal challenges have arisen that require precise regulatory frameworks. Ensuring that digital citizens can exercise their rights without undermining digital public order is paramount.

- **Data Protection:**

Unregulated data processing, unauthorized marketing, and malicious breaches give rise to legal questions surrounding informed consent, the right to be forgotten, and information security. The European Union's General Data Protection Regulation (GDPR) offers a pioneering model, yet it faces implementation hurdles in jurisdictions with diverse legal traditions¹.

- **Cybercrime:**

Cyber offenses such as fraud, extortion, forgery, incitement of hatred, and privacy violations pose a significant threat to both individual and national cybersecurity. Combating these offenses necessitates the modernization of domestic laws and enhanced international judicial cooperation to address crimes that transcend borders².

- **Digital Censorship:**

Regulating online content provokes debate between safeguarding public order and hate-speech prevention on one side, and upholding freedom of expression and access to information on the other. Overzealous control can result in "prior restraint," stifling fundamental liberties, or "covert censorship," which undermines transparency and trust in the digital ecosystem...

Here is the completed translation of the Digital Censorship subsection, incorporating your added sentence:

- **Digital Censorship:**

Regulating online content provokes a debate between the imperatives of protecting public order and countering hate speech on one hand, and safeguarding freedom of expression and access to information on the other. Overzealous measures can lead to "prior restraint," stifling fundamental liberties, or to "covert censorship," practiced by unaccountable algorithms—which undermines transparency and trust in the digital ecosystem and calls for a reassessment of traditional legal frameworks to embed principles of transparency and ethical algorithmic governance³.

¹ -De Hert, Paul & Papakonstantinou, Vagelis. "The GDPR: New Horizons for the EU's Data Protection Regime", Computer Law & Security Review, Vol. 34, No. 2, 2018, p. 179–194.

² -Brenner, Susan W. Cybercrime: Criminal Threats from Cyberspace, Praeger, 2010.

³ -Taddeo, Mariarosaria & Floridi, Luciano, "How AI Can Be a Force for Good", Science, Vol. 361, Issue 6404, 2018, p. 751.

• **Jurisdictional Authority in Cyberspace**

Finally, the question of judicial jurisdiction emerges as one of the most complex legal dilemmas in the digital sphere. It is often difficult to identify which court has authority over disputes stemming from cross-border digital acts.

Addressing this problem calls for the development of new legal concepts such as “cyber courts,” extraterritorial jurisdiction, and the mutual recognition of digital evidence¹. These challenges are not mere obstacles; they constitute a call to rethink classical legal doctrines and to build a coherent digital legal system that responds to contemporary transformations, protects rights, and respects freedoms.

2.4- Digital Citizenship in International and Arab Legislation

• **International Legislation**

International frameworks form the backbone of digital regulation. The European Union’s General Data Protection Regulation (GDPR) stands as a leading example: it imposes stringent standards for safeguarding privacy and personal-data rights in modern electronic transactions.

• **Arab Legislative Initiatives**

Meanwhile, several Arab states have begun to craft legislation addressing multiple facets of digital citizenship. Some have enacted cybercrime laws and personal-data protection statutes designed to regulate the citizen–digital-space relationship by defining responsibilities and penalties for technology-related violations. For instance, certain national “Information Crimes” laws include provisions that govern digital-media use and authorize limited monitoring of online activities to preserve cybersecurity without undermining user rights. Regional initiatives further aim to harmonize these legal approaches and share expertise among Arab countries, thereby laying the groundwork for an integrated legal framework that aligns with international norms while respecting cultural particularities and local challenges. This legislative diversity offers an opportunity to develop more flexible and effective legal mechanisms that uphold digital-citizen rights and foster stability in the online environment.

Conclusion:

Digital citizenship has emerged as a necessary legal and cultural response to the profound transformations reshaping the relationship between individuals, the state, and society within the digital sphere. This study has underscored the pressing need to establish a comprehensive legal framework that safeguards the balanced and secure exercise of digital rights and responsibilities, while fostering a culture of responsible civic behavior online. The legal analysis of this topic has led to several key findings, followed by practical recommendations.

I. Results

- Digital citizenship is a multidimensional concept that extends traditional notions of citizenship into the digital environment and requires a clear and well-defined legal foundation.
- The digital transformation has created new patterns of interaction between citizens and the state, necessitating the revision of public policy frameworks.

¹ -De Hert, P., & Papakonstantinou, V. (2018). The GDPR: New Horizons for the EU's Data Protection Regime. *Computer Law & Security Review*, 34(2), 179–194.

- Digital citizenship requires a delicate balance between upholding freedom of expression and ensuring cybersecurity.
- Arab legislative systems remain fragmented and insufficiently adapted to the demands of digital citizenship.
- Legal protection for digital rights varies widely among countries, resulting in notable legal and human rights gaps at the international level.
- Educating future generations on the principles of digital citizenship is essential to developing a digitally aware society capable of exercising its rights responsibly.
- The growing complexity of legal challenges in cyberspace, including data protection, jurisdiction, and cybercrime, calls for reinforced international cooperation.

II. Recommendations

- Integrate digital citizenship education across all levels of the academic curriculum to promote awareness and responsible digital behavior.
- Enact unified Arab legislation that upholds digital rights while respecting cultural specificities.
- Develop balanced regulatory mechanisms that ensure cybersecurity without infringing upon fundamental freedoms.
- Promote academic research focused on digital citizenship from both legal and technological perspectives.
- Establish independent bodies dedicated to monitoring digital issues and protecting users in cyberspace.
- Strengthen international collaboration to combat cybercrime and establish clear rules governing cross-border jurisdiction.
- Launch national awareness campaigns aimed at promoting responsible digital conduct and informing citizens of their rights and obligations in the online environment.

List of references :

1-Books:

- Castells, Manuel, The Rise of the Network Society, 2nd ed, Wiley-Blackwell, 2010.
- Mossberger, Karen, Caroline J, Tolbert, and Ramona S. McNeal, Digital Citizenship, The Internet, Society, and Participation, MIT Press, 2008.
- Ribble, Mike. Digital Citizenship in Schools: Nine Elements All Students Should Know, International Society for Technology in Education (ISTE), 2011.
- Brenner, Susan W. Cybercrime: Criminal Threats from Cyberspace, Praeger, 2010.

2-Journals

- De Hert, Paul, and Vagelis Papakonstantinou, "The GDPR, New Horizons for the EU's Data Protection Regime", Computer Law & Security Review, Vol. 34, No. 2, 2018, pp. 179–194.
- Taddeo, Maria Rosaria, and Luciano Floridi, "How AI Can Be a Force for Good", Science, Vol. 361, Issue 6404, 2018.

3-Scientific forums

- Ana Maria, and others, "Adolescents' Digital Citizenship, A Conceptual Approach", IEEE – Proceedings of the 2021 XI International Conference on Virtual Campus (JICV), September 2021.

4- Websites

-Cristina Hennig Manrique, Ana Vargas Sánchez, Erika Duque Bedoya. Digital Citizenship: A Theoretical Review of the Concept and Trends in the Last Ten Years, ERIC – Education Resources Information Center, 2019. Available at:
<https://files.eric.ed.gov/fulltext/EJ1211194.pdf> .