

The Role of Cyber Sovereignty in Protecting the Digital Identity of Algerian Citizens

دور السيادة السيبرانية في حماية الهوية الرقمية للمواطنين الجزائريين

Received: 31/10/2024

Accepted: 24/11/2024

Published: 31/12/2024

Samir Mebarkia ^{*1}

University Mohamed Boudiaf- Msila- (Algeria)

Email : samir.mebarkia@univ-msila.dz

Farhat Mahiddine ²

University August 20, 1955- Skikda- (Algeria)

Email : m.farhat@univ-skikda.dz



Journal of research and human studies
Issue 18 N°02 Year 2024 p.p. 20-35
ISSN : 1112-8151 EISSN : 2588-2317

Abstract :

This study aims to explore the role of cyber sovereignty in protecting the digital identity of Algerian citizens, given the increasing technical and security challenges Algeria faces. The study seeks to analyze the effectiveness of the country's digital infrastructure in securing digital identity and protecting it from cyber threats. It also focuses on the difficulties that hinder achieving comprehensive protection of digital identity, including technical and security challenges. Additionally, the study reviews Algeria's efforts to balance protecting digital identity with ensuring individual privacy rights, with emphasis on adopted cyber policies. The study concludes with practical recommendations and suggestions to improve digital identity protection and overcome existing technical and legislative challenges.

Keywords: cyber sovereignty , digital identity , digital privacy, cybersecurity, technical challenges.

الملخص :

تهدف هذه الدراسة إلى استكشاف دور السيادة السيبرانية في حماية الهوية الرقمية للمواطن الجزائري، وذلك في ظل التحديات التقنية والأمنية المتزايدة التي تواجه الجزائر. تسعى الدراسة إلى تحليل مدى فعالية البنية التحتية الرقمية في البلاد ودورها في تأمين الهوية الرقمية، وحمايتها من التهديدات السيبرانية. كما تركز الدراسة على الصعوبات التي تحول دون تحقيق حماية شاملة للهوية الرقمية، بما في ذلك التحديات التقنية والأمنية. بالإضافة إلى ذلك، تستعرض الدراسة جهود الجزائر في تحقيق التوازن بين حماية الهوية الرقمية وضمان حقوق الخصوصية الفردية، مع تسليط الضوء على السياسات السيبرانية المعتمدة. وتختتم الدراسة بتقديم مجموعة من التوصيات العملية والاقتراحات التي تهدف إلى تحسين حماية الهوية الرقمية، وتجاوز الصعوبات التقنية والتشريعية القائمة.

الكلمات المفتاحية : السيادة السيبرانية؛ الهوية الرقمية؛ الخصوصية الرقمية؛ الأمن السيبراني؛ التحديات

التقنية.

1. Introduction

Amid today's global digital revolution, the concept of digital identity has become a focal point in discussions surrounding cybersecurity and privacy protection. Like other countries, Algeria faces significant challenges due to increasing reliance on digital technologies across vital sectors, such as e-government, banking, and telecommunications. These technological developments have heightened the level of cyber threats targeting citizens' digital identities, making cyber sovereignty a strategic necessity for the state in securing and protecting personal data. Cyber sovereignty encompasses not only control over the national cyberspace but also the development of secure digital infrastructure and the adoption of legal and regulatory policies to ensure information protection and individual privacy. However, Algeria faces substantial challenges in achieving this goal, including underdeveloped technical infrastructure and increasing security threats. This study explores the role of cyber sovereignty in protecting the digital identity of Algerian citizens, focusing on technical and security challenges, and proposing practical solutions to achieve a balance between protection and privacy.

2. Problem Statement

The increased reliance on digital technology in Algeria in recent years has made protecting citizens' digital identities a pressing concern. Digital identity facilitates access to services and provides institutions with accurate data, but it is also vulnerable to various risks, such as identity theft, data manipulation, and cyberattacks. In this context, cyber sovereignty plays a crucial role in protecting the digital space and ensuring the security of personal information. However, Algeria faces numerous challenges in achieving comprehensive digital identity protection, from underdeveloped digital infrastructure and a lack of specialized skills to legal challenges in effectively enforcing legislation. Additionally, balancing digital identity protection with guaranteeing citizens' privacy rights remains a complex task. These challenges raise questions about the extent to which cyber sovereignty can provide effective protection for digital identity in Algeria.

Main Question:

How does cyber sovereignty contribute to protecting the digital identity of Algerian citizens in light of increasing technical and security challenges?

Sub-questions:

1. How does the current digital infrastructure in Algeria affect the state's capacity to protect digital identity within the framework of cyber sovereignty?
2. What are the primary technical and security challenges Algeria faces in protecting its citizens' digital identity?
3. How can Algeria achieve an effective balance between protecting digital identity and ensuring individual privacy rights in light of cyber requirements?

3. Study Objectives

- Analyze the role of cyber sovereignty in protecting Algerian citizens' digital identity, highlighting efforts to secure personal information in the digital space.
- Explore the technical and security challenges Algeria faces in securing digital identity, including inadequate infrastructure and increasing cyber threats.
- Provide practical recommendations to improve digital security through infrastructure enhancement, legislative development, and balancing cybersecurity with privacy rights.

4. Study Methodology

This study adopts a descriptive-analytical approach to understand and analyze the role of cyber sovereignty in protecting Algerian citizens' digital identity. Information is gathered by reviewing prior literature and legislation on cyber sovereignty and digital identity, along with analyzing technical data on Algeria's digital infrastructure. The study also includes a comparative analysis of Algeria's adopted policies with those of leading countries in digital identity protection, offering recommendations based on these comparisons and observations.

5. Cyber Sovereignty and its Importance

Cyber sovereignty refers to a state's ability to fully control its digital space, which includes protecting sensitive data, securing digital infrastructure, and regulating online activities within its borders. This concept is integral to national security in the digital age, enabling states to protect their citizens from cyber threats such as cyberattacks, identity theft, and digital crimes. Cyber sovereignty extends beyond technical aspects to encompass legal and political dimensions, enhancing a state's ability to secure its digital security and enforce its policies in

its cyberspace (Demchak & Dombrowski, 2011, p. 35). Additionally, cyber sovereignty is essential in countering transnational digital threats and collaborating with other countries to secure digital safety at both local and international levels.

5.1 Dimensions of Cyber Sovereignty

- **Legal Dimension:** This aspect pertains to the legal framework a state adopts to regulate its digital space, including laws on data collection, storage, and protection and legislation that penalizes cybercrimes. Legal sovereignty ensures that both domestic and foreign digital activities are subject to national laws aimed at protecting citizens and digital infrastructure. For example, regulations like the European Union's General Data Protection Regulation (GDPR) grant countries legal sovereignty over citizens' personal data, compelling companies to adhere to stringent data protection standards (European Commission, 2018, p. 10).
- **Technical Dimension:** This involves the technological infrastructure required for a state to secure its digital space. It includes developing protection systems against intrusions and cyberattacks, secure networks, and advanced threat detection capabilities. State investments in advanced technologies like artificial intelligence and big data analytics are vital to quickly responding to cyberattacks. This underscores the importance of a robust digital infrastructure that allows the state to protect citizens from internal and external digital threats (Singer & Friedman, 2014, p. 58).
- **Political Dimension:** This aspect involves decisions and policies a state adopts at the international and local levels to protect its cyber sovereignty. It also covers managing relations with other states concerning cybersecurity and cross-border cooperation to counter transnational digital threats. Developing a clear and adaptable national cyber strategy is essential to ensuring that a state can protect its digital sovereignty while balancing digital space protection with internet freedom (Mueller, 2010, p. 76). Moreover, inadequate political oversight may leave a state vulnerable to cyberattacks that could have serious national security implications.

2. Understanding Digital Identity and Its Importance

Digital identity represents an electronic version of information related to individuals or organizations, used to identify them in digital space. This information ranges from basic data, such as name, birth date, and address, to more sensitive information, such as biometric data (fingerprints or eye scans), financial details, and online transaction records. This form of identity is fundamental to modern digital interactions, where individuals use digital identities to access government, banking, healthcare, and even social services.

The significance of digital identity lies in its ability to provide individuals with quick, secure access to various services, both public and private. Digital identity also enables institutions to manage user data more efficiently, allowing them to provide personalized and faster services. In Algeria, for example, the e-government project promotes digital identity for citizens by offering remote governmental services, such as issuing official documents and registering property transactions online (Boucebaa, 2020, p. 82).

Additionally, digital identity serves as a tool to facilitate the digital economy by enabling businesses to verify their customers' identities and provide tailored services. However, the importance of digital identity is not limited to facilitating processes; it also relates to protecting personal data from unauthorized use. In the Algerian context, digital identity is a cornerstone of digital development, especially in the ongoing shift towards expanding digital services across economic and social sectors (Whitley, 2014, p. 44).

6.1 Threats to Digital Identity

Despite the considerable advantages of digital identity, risks related to it have increased with technological advancement. One of the primary risks is identity theft, which occurs when an unauthorized person gains access to someone else's digital identity information and uses it for illegal purposes. This type of cybercrime can lead to significant financial losses and damage the reputation of individuals and institutions (Gonzalez, 2017, p. 70). Globally, millions of cases related to digital identity theft are recorded annually, making it one of the fastest-growing cybercrimes.

In Algeria, digital identity theft poses a real threat, especially as the country increasingly relies on digital systems to manage public and private services. Reports indicate a sharp rise in cyberattacks targeting personal data in recent years, with vulnerabilities in digital infrastructure often exploited to target users. According to Bouceb (2020, p. 85), protecting digital identity in Algeria requires

developing comprehensive strategies that include strengthening personal data protection laws and improving digital awareness among users

Beyond identity theft, there are other threats, such as digital forgery, where stolen identities are used to open bank accounts or apply for financial services in the victim's name. Such crimes cause significant financial losses for both individuals and institutions and create complex legal challenges. Therefore, Algeria needs to invest in protective technologies such as advanced encryption and biometric recognition systems to ensure digital identity security (Bounjed, 2019, p. 103). Furthermore, Gonzalez (2017, p. 72) highlights that government-private sector collaboration is essential to counter these cyber threats by sharing information and enhancing digital security.

In this context, the country needs preventive strategies to address future threats to digital identity, such as artificial intelligence-based attacks and big data analytics to exploit system vulnerabilities. Public awareness of the importance of digital identity protection remains one of the most crucial factors in reducing the risks of identity theft and digital fraud, particularly in Algeria, which is experiencing a rapid digital transformation.

7. Algerian Legislation and Policies for Digital Identity Protection

In recent years, Algeria has made increasing efforts to strengthen its legislative framework for digital identity protection due to the rapid expansion of digital technology use across various sectors. One of the primary legislations for digital identity protection is Law No. 18-07 on personal data protection, a significant step toward enhancing Algeria's cyber sovereignty. This law requires public and private institutions to take appropriate measures to protect citizens' digital data and imposes penalties on violators.

Additionally, this law mirrors several international regulations, such as the European Union's GDPR, which sets strict global standards for personal data protection. Although Algeria strives to align its policies with international standards, it faces significant challenges in enforcing these laws due to weak digital infrastructure and a shortage of specialized cybersecurity skills (Cavoukian, 2013, p. 88). At the same time, implementing these laws requires developing effective monitoring tools to ensure compliance, particularly as reliance on digital services in Algeria grows.

Other challenges in Algerian legislation on digital identity protection include weak institutional oversight, as many companies still do not fully adhere to

required standards for protecting citizens' digital data. Schoeman (2018, p. 108) explains that this issue is not unique to Algeria but is common among many developing countries that rely heavily on imported technology without developing effective national data protection policies.

7.1 The Role of Government Institutions

Algerian government institutions play a key role in implementing cyber policies, with the National Authority for the Protection of Personal Data (NAPDP) at the forefront. This authority is responsible for overseeing the implementation of data protection legislation and ensuring compliance among public and private institutions. It evaluates the compliance of digital systems with digital identity protection standards and provides necessary recommendations to improve cybersecurity. The authority's role extends beyond oversight to enhancing public awareness of the importance of digital identity protection through awareness campaigns and educational programs aimed at improving citizens' understanding of their digital rights.

On the other hand, the Ministry of Post and Telecommunications plays a strategic role in formulating national policies for cyberspace. The ministry supervises national projects for digital infrastructure development, such as the e-government project, which aims to digitize public services and foster trust between citizens and the digital government (Hamidi, 2021, p. 66). The main challenge lies in developing this infrastructure to resist cyber threats, especially given the rising number of cyberattacks targeting government institutions. According to McDermott (2020, p. 162), Algeria's efforts in this field are beginning to show results; however, improved collaboration between public and private sectors is needed to ensure the effective implementation of cyber policies.

7.2 National Initiatives to Strengthen Cyber Sovereignty

Algeria has launched several initiatives to bolster cyber sovereignty and protect digital identity, including the "Smart City" project, which aims to create a secure digital environment using advanced technologies like the Internet of Things (IoT) and artificial intelligence. This project enhances the government's ability to monitor and control the digital space. Zalnieriute and Bennett Moses (2020, p. 255) indicate that these projects are not only a means of enhancing governmental services but are also a strategy for reinforcing digital infrastructure to combat cyber threats.

In the educational field, Algeria has launched various programs aimed at training a new generation of cybersecurity specialists. These programs include partnerships with national and international universities that offer specialized courses in data protection and security software development. Gray (2017, p. 95) emphasizes that these educational initiatives play a crucial role in strengthening national capabilities to counter cyberattacks and protect digital identity. However, Bouznina (2021, p. 83) notes that the full success of these initiatives depends on improving the country's technological environment and increasing investments in cybersecurity research and development.

8. Technical and Security Challenges in Protecting Digital Identity

Algeria faces significant challenges in developing the necessary digital infrastructure to protect citizens' digital identities.

8.1 Technical Challenges

Despite progress achieved in recent years through projects like the "Smart City" and digital transformation in certain government sectors, Algeria's technical infrastructure still falls short of meeting the increasing demand for data protection and digital identity security. Algeria suffers from weak communication networks and limited internet speeds, which hinder the state's capacity to build a secure and stable digital environment.

Stable and high-speed communications are crucial for developing data protection systems and ensuring that encryption and protection systems function effectively. In Algeria, studies indicate that most individuals and companies lack stable high-speed internet, opening up potential cyberattack vulnerabilities due to security gaps (Dine, 2020, p. 45). Furthermore, Algeria's lack of investment in upgrading digital infrastructure makes it unable to implement advanced digital identity protection solutions, such as biometric and secured network systems. Lipton (2019, p. 35) asserts that this lack of investment exacerbates the risk of citizen data being exposed to breaches and cyberattacks.

8.1.1 Additional Technical Challenges

Other technical challenges include the absence of modern and robust technologies for digital identity verification, with some government and private institutions relying on outdated systems that are difficult to protect against growing cyber threats. Cloud computing systems, which could play a role in securely storing data, still face considerable obstacles in Algeria regarding infrastructure and technical support (Zalnieriute & Moses, 2020, p. 256).

8.2 Security Challenges

Like many other countries, Algeria faces increasing cyber threats, particularly concerning digital identity protection. With the expanded reliance on digital systems and the widespread use of electronic services across various fields, citizens' digital identities are becoming more vulnerable to attacks. One of the main security challenges is the weak encryption systems that institutions use to protect user data; many institutions still rely on outdated or unsecure encryption systems, making it easier to compromise personal information (Lipton, 2019, p. 41).

In addition, the shortage of skilled technical personnel in cybersecurity remains one of the significant barriers to Algeria's efforts in protecting digital identity. Mansouri (2020, p. 85) states that the lack of cybersecurity engineers and specialists hampers the country's ability to build strong protective systems and respond to cyberattacks promptly. Many institutions also lack contingency plans or specialized teams to deal with breaches, increasing the risk of personal data exposure.

8.3 Types of Cyber Attacks and Their Impact on Digital Identity

Cyber attacks that threaten digital identity come in various forms. One of the most severe methods is phishing, where users are tricked into revealing their personal data through fake emails or websites. Studies show that Algeria has witnessed a significant increase in such attacks in recent years, resulting in substantial financial losses for individuals and institutions (Adel, 2019, p. 70).

There are also ransomware attacks, in which hackers encrypt a victim's data and demand a ransom to restore access. These attacks have a significant impact on digital identities as they prevent users from accessing personal or financial data. Zalnieriute and Moses (2020, p. 258) note that the impact of these attacks is amplified in countries with weak digital infrastructure like Algeria, where the state struggles to respond to these attacks effectively. Other types of cyber attacks include Distributed Denial of Service (DDoS) attacks, which aim to flood digital systems and cause them to fail, disrupting government and financial services and compromising digital identities.

According to Mansouri (2020, p. 87), developing local capabilities in cybersecurity requires collaboration between the public and private sectors to ensure information sharing and effective strategies against these attacks. This emphasizes the importance of building partnerships with international

organizations to adopt the latest technologies and strategies to counter cyber threats.

9. Balancing Digital Identity Protection and Individual Privacy Rights

Digital privacy refers to individuals' right to protect their personal data collected and stored online or on any other digital platforms. This concept encompasses the ability of individuals to control who can access their personal information and how it is used. Digital privacy is now an essential part of human rights in the digital age, as personal information (such as names, addresses, financial and health data) is highly valuable and requires stringent legal protection to prevent misuse or abuse.

In Algeria, digital privacy forms part of citizens' rights, which the state aims to protect through legislation safeguarding personal data. Although Law No. 18-07 on personal data protection represents a significant step in this direction, there remains a need for more awareness about digital privacy and associated challenges, especially amid rapid digital technology expansion. Debbache (2020, p. 45) notes that many Algerian users lack sufficient awareness of digital privacy risks, making them vulnerable to cyberattacks.

9.1 Balancing Cyber Sovereignty and Privacy Protection

Balancing the protection of cyber sovereignty and ensuring digital privacy rights presents a significant challenge for many countries, including Algeria. On one hand, the state needs to assert sovereignty over digital space to protect citizens' digital identities and secure sensitive data from cyber threats. On the other, the state must ensure it does not infringe upon individuals' rights to digital privacy, leading to tension between security demands and privacy rights.

Despite Algeria's efforts to enhance cyber sovereignty through legislation to protect digital identity and restrict unauthorized access to data, concerns are growing about the potential misuse of such legislation in ways that could infringe on individual privacy rights. Ben Said (2020, p. 70) argues that government policies aimed at controlling cyberspace may sometimes result in legal excesses that threaten individuals' digital privacy rights, particularly in the absence of a clear legal framework that strikes a balance between privacy protection and cybersecurity requirements.

The main challenge in this context is to establish policies capable of achieving a balance between digital security and privacy rights. Technologies such as

encryption and biometric-based identity verification can contribute to protecting sensitive data, but clear laws are also necessary to ensure transparency and accountability in data usage. To achieve this balance, the Algerian government should adopt strategies that allow citizens to understand how their data is collected and used while ensuring their rights to access and protect their data.

9.2 Reviewing Algerian Laws in This Context

Law No. 18-07 on personal data protection in Algeria is among the most prominent legislative efforts to protect individuals' digital privacy rights. This law obliges public and private institutions to take necessary measures to protect individuals' data and grants individuals the right to know how their data is used and to object to its use if it affects their privacy.

Despite these laws, Debbache (2020, p. 48) points out that the main challenge lies in their effective implementation. Many companies do not fully comply with international data protection standards, leaving room for violations that negatively impact individual privacy. Furthermore, monitoring compliance with these laws remains weak, necessitating improvements in the legislative and regulatory framework to ensure a balance between cyber sovereignty and privacy protection.

Ben Said (2020, p. 72) suggests that Algeria could enhance its existing laws by providing more effective mechanisms to monitor personal data usage and offering a clear legal framework that delineates boundaries between digital security and individual privacy rights. These laws must adapt to rapid technological developments to ensure sustainable protection for digital identity and individuals' digital privacy rights.

3. Study results

Based on the sub-questions and data analyzed in the study, the following findings were made:

1. Impact of Algeria's Current Digital Infrastructure on Cyber Sovereignty and Digital Identity Protection:

The study reveals that Algeria's digital infrastructure still faces significant challenges impacting the state's ability to protect digital identity effectively. Weak internet networks, limited high-speed communications, and inadequate investments in developing encryption and digital security systems are the primary factors hindering the application of cyber sovereignty policies. The underdeveloped digital infrastructure makes it challenging for the state to implement modern technical solutions to protect

digital identity, such as biometric systems and complex verification mechanisms, increasing the risk of personal data breaches and cyberattacks. This technological gap directly affects the effectiveness of cyber sovereignty in securing Algeria's digital space.

2. Main Technical and Security Challenges Algeria Faces in Digital Identity Protection:

The study identifies several technical and security challenges that hinder digital identity protection in Algeria. Technically, a shortage of skilled cybersecurity professionals and the unavailability of modern identity verification technologies are major obstacles. Many government and private institutions rely on outdated and insufficiently protected systems, making them vulnerable to cyberattacks. On the security front, cyber threats such as phishing and ransomware attacks pose serious risks to digital identities in Algeria. The country also lacks emergency teams specialized in handling these attacks, exacerbating the damages caused by such breaches.

3. Achieving an Effective Balance Between Digital Identity Protection and Individual Privacy Rights in Algeria:

The study highlights that balancing digital identity protection with ensuring individual privacy rights remains a significant challenge in Algeria. Despite legislation like Law No. 18-07 on personal data protection, there remains a substantial gap in effectively implementing these laws. While the state needs to assert sovereignty over digital space to secure digital identity, it must also respect individual privacy rights. This tension necessitates developing balanced policies that account for cybersecurity demands without compromising privacy rights. To achieve this balance, Algeria needs to enhance transparency in data collection and usage and adopt advanced technologies, such as strong encryption, to protect personal data while limiting unauthorized access.

11. Recommendations

Based on the findings, the following recommendations are made to enhance digital identity protection in Algeria:

- **Enhancing Digital Infrastructure:** Algeria needs to increase investments in digital infrastructure development, including improving high-speed internet networks and updating technical systems in both government and private institutions. The country should strengthen its encryption technology

capabilities and develop robust verification systems for digital identity protection.

- **Developing Local Cybersecurity Expertise:** Algeria should focus on training a new generation of cybersecurity specialists by offering specialized educational programs in universities and technical institutes and enhancing partnerships with international organizations to benefit from their expertise.
- **Strict Enforcement of Legislation:** Improved enforcement of current personal data protection laws, such as Law No. 18-07, is crucial. Authorities must strengthen oversight of public and private institutions to ensure full compliance and take strict legal action against violators.
- **Increasing Public Awareness of Digital Privacy:** Algeria should launch awareness programs targeting citizens and businesses to raise awareness of the importance of digital privacy and the risks of cyberattacks. Such programs could encourage citizens to take proactive steps to protect their personal data.
- **Balancing Cyber Sovereignty and Privacy Rights:** The state should develop policies to balance cybersecurity and individual privacy rights. This requires adopting technologies like advanced encryption and ensuring transparency in data collection and usage practices.

12. Conclusion

Algeria faces substantial challenges in protecting its citizens' digital identities within the framework of cyber sovereignty, primarily due to underdeveloped digital infrastructure, a lack of specialized skills, and increasing cyberattacks. Although Algeria has made legislative efforts to enhance digital identity protection, practical implementation remains flawed, necessitating improvements in infrastructure, training, and oversight.

Achieving an effective balance between digital identity protection and individual privacy rights requires integrated efforts that include legislative development, infrastructure improvement, and public awareness. These efforts should be supported by modern technologies and transparent legal frameworks to ensure sustainable protection for citizens' digital identities. Ultimately, Algeria has the potential to confront these challenges by enhancing its technological capabilities and fostering partnerships between the public and private sectors to achieve effective cyber sovereignty and comprehensive digital identity protection.

13. Bibliography List

13.1 Books

1. Cavoukian, A. (2013), *Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era*, Information and Privacy Commissioner of Ontario, Canada.
2. Gonzalez, R. (2017), *Digital Identity and Its Role in Modern Society*, Cambridge University Press, UK.
3. McDermott, Y. (2020), *Data Protection, Cybersecurity, and International Law: Privacy in the Digital Age*, Cambridge University Press, UK.
4. Mueller, M. (2010), *Networks and States: The Global Politics of Internet Governance*, MIT Press, USA.
5. Singer, P. W., & Friedman, A. (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, USA.

13.2 Journal Articles

6. Adel, B. (2019), Digital Infrastructure in Algeria: Challenges and Opportunities, *Journal of Digital Economy*, 12(2), Algeria, 65-75.
7. Amrouche, H. (2021), Privacy Protection in the Digital Age: Algerian Legislation between Reality and Challenges, *Journal of Digital Law*, 9(1), Algeria, 80-90.
8. Bendib, A. (2021), Algerian Policies for Personal Data Protection and Individual Rights, *Journal of Law and Policies*, 5(3), Algeria, 65-75.
9. Bendib, A. (2022), Algerian Policies in Personal Data Protection, *Journal of Law and Policies*, 5(3), Algeria, 70-80.
10. Ben Saad, M. (2020), Legal Challenges of Digital Privacy Protection in Algeria, *Journal of Legal Studies*, 12(2), Algeria, 65-80.
11. Bounad, A. (2019), Cyber Threats and Digital Identity Theft in Algeria: Challenges and Solutions, *Journal of Social Sciences*, 12(4), Algeria, 100-105.
12. Bousaab, A. (2020), Protection of Digital Identity in Algeria: Reality and Challenges, *Algerian Journal of Communication*, 18(2), Algeria, 80-90.
13. Debacha, K. (2020), Cyber Legislation in Algeria and Its Impact on Digital Privacy Protection, *Journal of Cybersecurity*, 7(1), Algeria, 40-55.
14. Dini, A. (2020), Technical and Security Challenges in Algeria: Digital Identity Protection as a Case Study, *Journal of Security Studies*, 5(1), Algeria, 40-55.

15. Hamidi, M. (2021), Cyber Sovereignty in Algeria: Legislation and Challenges, *Journal of Law and Political Science*, 18(1), Algeria, 60-70.
16. Mansri, A. (2020), Cybersecurity in Algeria: Challenges and Solutions, *Journal of Technology and Security*, 8(3), Algeria, 80-90.
17. Bousnina, M. (2021), Impact of Cyber Policies on Digital Identity Protection in Algeria, *Journal of Political Science*, 15(2), Algeria, 75-85.
18. Demchak, C. C., & Dombrowski, P. (2011), Rise of a Cybered Westphalian Age, *Strategic Studies Quarterly*, 5(1), USA, 32-61.
19. Gray, A. (2017), Digital Citizenship and the New Governance Framework, *Journal of Cyber Policy*, 2(3), UK, 90-100. <https://doi.org/10.1080/23738871.2017.1365088>.
20. Lipton, J. D. (2019), Cybersecurity in Developing Nations: Securing the Next Billion, *Journal of Information Policy*, 9, USA, 30-50. <https://doi.org/10.5325/jinfopoli.9.2019.0030>.
21. Schoeman, M. (2018), Privacy, Data Protection, and Cybersecurity in Africa, *International Data Privacy Law*, 8(3), UK, 100-120. <https://doi.org/10.1093/idpl/ipy002>.
22. Whitley, E. A., Gal, U., & Kjaergaard, A. (2014), Who Do You Think You Are? A Review of the Complex Interplay Between Information Systems, Identification, and Identity, *European Journal of Information Systems*, 23(1), UK, 42-57. <https://doi.org/10.1057/ejis.2013.34>.
23. Zalnieriute, M., & Bennett Moses, L. (2020), Privacy, Sovereignty, and the Development of Digital Identity Systems, *International Journal of Law and Information Technology*, 28(3), UK, 245-260. <https://doi.org/10.1093/ijlit/aaaa013>.

13.3 Internet Websites

24. European Commission. (2018), General Data Protection Regulation (GDPR), detailed web site: https://ec.europa.eu/info/law/law-topic/data-protection_en (consulted on 03/10/2024).