

CYBER SECURITY AND ITS ROLE IN ACHIEVING LEGAL SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION IN ALGERIA: A STUDY OF LEGAL AND INSTITUTIONAL MECHANISMS

La ciberseguridad y su papel en la consecución de la seguridad jurídica en el contexto de la transformación digital en Argelia: un estudio de los mecanismos jurídicos e institucionales

1. PhD Student. Djihane yahi

University of Mohamed El Bachir El Ibrahimi Bordj Bou Arréidj, faculty of law and political sciences.
djihane.yahi@univ-bba.dz

Universidad Mohamed El Bachir El Ibrahimi de Bordj Bou Arréidj, Facultad de Derecho y Ciencias Políticas, Argelia.

2. Dr. Abdelmoumene Si Hamdi

University of Mohamed El Bachir El Ibrahimi Bordj Bou Arréidj, faculty of law and political sciences.
abdelmoumene.sihamdi@univ-bba.dz

Universidad Mohamed El Bachir El Ibrahimi de Bordj Bou Arréidj, Facultad de Derecho y Ciencias Políticas, Argelia.

3. Dr. Asma Krika

University of Mohamed El Bachir El Ibrahimi Bordj Bou Arréidj, faculty of social and human sciences.
asma.krika@univ-bba.dz

Universidad Mohamed El Bachir El Ibrahimi de Bordj Bou Arréidj, Facultad de Ciencias Sociales y Humanidades, Argelia.

4. Dr. Alaeddine Youcefi

Institute of Law
Governance Horizons Laboratory for Sustainable Local Development, University Center of Barika / Algeria
alaeddine.youcefi@cu-barika.dz

Instituto de Derecho
Laboratorio Horizontes de Gobernanza para el Desarrollo Local Sostenible, Centro Universitario de Barika, Argelia.

Abstract

Digital transformation has reshaped the requirements of legal security, making cybersecurity increasingly important to the protection of rights and the predictability of legal relations in digital environments. This study examines the relationship between cybersecurity and legal security in Algeria, focusing on the legal and institutional mechanisms intended to safeguard these interests. It clarifies the conceptual framework and objectives of cybersecurity and considers how they intersect with the requirements of legal security. The analysis further examines Algeria's regulatory approach to cybersecurity and the extent to which its legal and institutional arrangements support the protection of legal security amid digital transformation. By bringing these dimensions together, the study provides a framework for assessing the role of cybersecurity governance in maintaining a secure and legally predictable digital environment.

Keywords: cybersecurity; legal security; digital transformation; legal and institutional mechanisms; Algeria.

Resumen

La transformación digital ha redefinido las exigencias de la seguridad jurídica, otorgando a la ciberseguridad una importancia creciente en la protección de los derechos y la previsibilidad de las relaciones jurídicas en los entornos digitales. Este estudio examina la relación entre la ciberseguridad y la seguridad jurídica en Argelia, centrándose en los mecanismos jurídicos e institucionales destinados a salvaguardar estos intereses. Delimita el marco conceptual y los objetivos de la ciberseguridad y analiza su vinculación con las exigencias de la seguridad jurídica. Asimismo, examina el enfoque regulatorio argelino en materia de ciberseguridad y evalúa en qué medida sus disposiciones jurídicas y estructuras institucionales contribuyen a proteger la seguridad jurídica en el contexto de la transformación digital. Al integrar estas dimensiones, el estudio proporciona un marco para evaluar el papel de la gobernanza de la ciberseguridad en el mantenimiento de un entorno digital seguro y jurídicamente previsible.

Palabras clave: ciberseguridad; seguridad jurídica; transformación digital; mecanismos jurídicos e institucionales; Argelia.

Introduction:

Like other concepts, the concept of legal security has undergone a profound evolution in its substance and mechanisms in the context of digital transformation and increasing reliance on information and communication technologies; it has shifted from a concept focused primarily on the clarity of legal texts, the stability of legal rules, the safeguarding of individuals' acquired rights, and ease of access to legal information within a traditional environment, to concepts primarily linked to the digital environment; it now encompasses electronic services, artificial intelligence, digital rights and freedoms, and other elements. Given the risks that may threaten the foundations of digital legal security, it has become necessary to establish protective mechanisms in line with this modern concept; various countries, including Algeria, have therefore worked to achieve this by enshrining the concept of cybersecurity. Cybersecurity is considered a fundamental and essential element for achieving legal security within the digital environment. In light of the above, we pose the following question: How can cybersecurity ensure legal security in the context of the current digital transformation? To answer this question, we pose the following sub-questions:

- What is the concept of cybersecurity?
- What is the concept of digital legal security?
- What mechanisms are in place to ensure that cybersecurity contributes to legal security?

The aim of our study is to examine the concept of cybersecurity and its components, to examine the concept of digital legal security and its components, and to identify the most important institutional and legal mechanisms in place to achieve cybersecurity.

In our study, we have adopted a two-part structure comprising two sections: the first section is devoted to examining the concepts of cybersecurity and digital legal security, whilst the second section addresses the most prominent legal and institutional mechanisms for achieving cybersecurity and enhancing digital legal security.

Section One: Cyber Security and Digital Legal Security.

The emergence of digital legal security is linked to the development of information and communications technologies, and to individuals' awareness of the need to embrace the digital environment due to its advantages. However, communication within the digital environment exposes individuals in particular, and the state in general, to a range of actions that may infringe upon individuals' rights and freedoms, as well as potentially harm their personal and financial interests. This has necessitated the development of a mechanism to protect individuals within this digital environment; consequently, states, including Algeria, have moved to establish security frameworks, known as cyber security.

In this paper, we shall attempt to shed light on the concept of digital legal security as a modern concept, whilst also defining the concept of cyber security, with the ultimate aim of identifying the relationship of influence between the two.

Section 1: The conceptual framework of cyber security and digital legal security.

Cyber security and digital legal security are relatively recent concepts, linked to developments in information technology and the digital revolution in society, which necessitates our examination of them.

Section One: The Concept of Cybersecurity.

First: Definition of cyber security.

Cyber security is a tool, technology or process used to protect the information assets of a cyber security system; it enables cyber security, adds value to networks and is geared towards both flexible and rigid infrastructure. **The components of the hard infrastructure** refer to the hardware and software required to protect the system and data from threats and security risks originating from outside or within the system, whilst **the components of the flexible infrastructure** refer to the policies, processes, protocols and guidelines that protect the system and data from various sources.¹

The Saudi National Cybersecurity Authority has defined cybersecurity as: "the protection of networks, information technology systems, operational technology systems and their hardware and software

¹ - Bouali Boujaltia Ahmadi, 'Cyber-terrorism and Ways of Countering It at the Arab Level: A Study of the Saudi and Qatari Experiences', **Academic Journal of Social and Humanitarian Studies**, Issue 16, June 2016, p. 183.

components, the services they provide, and the data they contain, from any unauthorised intrusion, disruption, modification, access, use, or exploitation. This concept also encompasses information security, electronic security, digital security and the like”¹.

The International Telecommunication Union defines it as: “A description of the set of tools, policies, guidelines, risk management approaches, procedures, training, best practices, safeguards and technologies that can be used to protect the availability, integrity and confidentiality of assets in the connected infrastructure of governments, private organisations and citizens. These assets include connected computing devices, personnel, infrastructure, digital applications and services, and communications and data systems in the digital environment.”²

Secondly: The fundamental controls for cyber security.

The core controls of cyber security are as follows³:

- **Cyber Security Governance:** This encompasses cyber security strategy, cyber security management, cyber security risk management, cyber security roles, etc.

- **Cyber Security Defence:** This includes email protection, network security management, protection of systems and information processing devices, data and information protection, mobile device security, encryption, penetration testing, and web application protection.

- **Cyber Security Resilience:** This encompasses aspects of cyber security resilience within business continuity management.

- **Third-party and cloud computing cybersecurity:** This includes cybersecurity relating to cloud computing and hosting, as well as cybersecurity relating to third parties.

Section Two: The Concept of Digital Legal Security:

Before defining digital legal security, we must clarify the meaning of digital security in the traditional sense

Firstly: The definition of legal security.

1. Linguistic meaning:

The phrase ‘legal security’ is composed of two terms:

Security: This is defined as protection against fear; given that ‘legal security’ is the literal translation of the term, we must therefore examine the linguistic meaning of the term ‘security’ in the context of the French concept of ‘sécurité juridique’ – ‘sécurité’, which refers to the psychological state characterised by a sense of safety and reassurance, and the absence of fear and danger.⁴

As for the second word, ‘law’, it is a Greek word meaning ‘straight rod’.

By combining the two preceding words, legal security can be defined linguistically as security, the absence of fear and a sense of reassurance within a specific sphere, namely the law.⁵

2. The technical meaning of legal security:

- The jurisprudential meaning of legal security:

The meaning of legal certainty is complex and multifaceted, making it difficult to formulate a comprehensive and exhaustive definition that encompasses all its aspects and manifestations.

Nevertheless, legal scholarship has attempted to define it as follows: ‘A principle comprising two meanings: firstly, the rule that ensures stability and certainty amongst citizens; and secondly, the principle based on the clarity, quality and enforceability of legal texts. This definition emerged after legal

¹ - **Presentation on cyber security**, Manashat, General Authority for Small and Medium-sized Enterprises, 2022, p. 3, published on the General Authority for Small and Medium-sized Enterprises website, accessed on 4 November 2025 at 20:55.

<https://www.monshaat.gov.sa/sites/default/files/2023-03/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%20.pdf>

² - Strategic Action in the Field of Cybersecurity: **A Guide to Preparing the National Cybersecurity Strategy**, Vol. 02, 2021, p. 12, accessed on 17 November 2025 at 19:00, published on the website:

<https://ncsguide.org/wp-content/uploads/2024/05/508938A.pdf>

³ - Basic Cybersecurity Controls, Saudi **National Cybersecurity Authority**, 2024, ECC02, accessed on 4 November 2025 at 22:00, published on the Authority’s website

https://cdn.nca.gov.sa/api/files/public/upload/29a9e86a-595f-4af9-8db5-88715a458a14_ECC-2-2024---NCA.pdf

⁴ - Belkhir, Mohamed Aït Oudieh, **Legal Security and its Foundations in Administrative Law**, Dar al-Khaliduniya, 2018, p. 19.

⁵ - Fatih Khaloufi, **The Powers of the Administrative Judge in Interpretation**, Dar Houma for Printing, Publishing and Distribution, Algiers, 2017, p. 183.

scholarship began to distinguish between rights and the law, and recognised that the legal system is founded on obligation rather than rights'.¹

- Judicial interpretation:

The French Council of State defined it in its 2006 report, given its importance, stating: "To achieve legal certainty, citizens must be able to determine what is permitted and what is prohibited under the law in force, without having to make any additional effort to reach this conclusion; laws must be clear and comprehensible and must not be subject to excessive, and in particular unexpected, changes over time."² As for the French Constitutional Council, it did not define legal certainty but merely accorded it constitutional status by addressing the safeguards necessary to achieve it, given its importance in safeguarding public rights and freedoms. This was to prevent rights and statuses acquired under legislative provisions from being regarded as definitive, such that the legislature would have no right to introduce legislative amendments affecting them.³

As for digital security, and by extension from the foregoing, it is: "a legal framework that guarantees the protection of users of the digital space, through rules governing and protecting personal data, digital identity, electronic signatures and electronic transactions over the internet."

Secondly: The objectives of the principle of digital legal security

Legal security aims to achieve stability and social peace in society by providing a clear and objective legal framework that defines the rights and duties of individuals and various entities, and ensures the fair and equitable application of laws to all individuals without discrimination or bias.

Legal security encompasses several aspects, such as public security, criminal security, civil security, economic security, and other aspects of security relating to the maintenance of social stability and well-being.

Legal security is the foundation for the protection of human rights and the realisation of justice and equality in society; it is one of the state's fundamental objectives and requires continuous efforts to develop laws, improve justice systems and provide a suitable legal environment for the realisation of legal security.⁴

Second Point: The Impact of Cybersecurity on Legal Security

The objectives of legal security—namely the protection of acquired rights and the stability of transactions—are affected by the presence or absence of cybersecurity, which poses a threat to them in the context of digital transformation. In this section, we shall outline the positive and negative impacts of cybersecurity on legal security.

Section One: The Positive Effects of Cybersecurity on Legal Security.

The existence of a cyber security framework serves to strengthen the protection of legal security in the context of digital transformation, as is clearly demonstrated by:

Firstly: the protection of digital rights and freedoms

Digital rights are defined as: 'the right of every individual to access, use, create and disseminate digital content, and to use computers, other devices, software or communication networks without any restrictions.

From this stem numerous other rights and freedoms, such as freedom of opinion and expression, freedom of information, the right to privacy, the right to development and knowledge, and other rights and freedoms."

Cyber security has a significant impact on these digital rights and freedoms; by protecting privacy, freedom of expression and information, and safeguarding economic rights.

¹- Husam Bouhajar, 'The Concept and Foundations of the Principle of Legal Certainty', paper presented at the local symposium on legal certainty, 15 October 2024, University of Guelma, p. 4.

²- Mohamed Ben Daima and Samir Shaaban, 'The Enshrinement of the Principle of Legal Certainty in Light of the Specific Nature of Commercial Criminal Law in Algerian Legislation', *Al-Bahith Journal of Academic Studies*, Vol. 10, No. 02, June 2023, p. 442.

³- Dalal Loushan and Fatiha Bouaqal, 'Legal certainty between legislative guarantees and the risks of judicial discretion', **Al-Bahith Journal of Academic Studies**, University of Batna, Vol. 5, No. 12, January 2018, p. 260.

⁴ - Abdelhay Yahya, 'The Principle of Legal Certainty and Its Applications in the Jurisprudence of the Council of State', doctoral thesis submitted for the degree of Doctor of Science, specialising in Public Law, Faculty of Law and Political Science, Martyr Hamma Lakhdar University, El Oued, academic year 2022–2023, p. 37.

It is well known that, in light of the digital transformation, and the Algerian state's drive to digitise all sectors of the state, the personal data of users or those affiliated with these sectors now exists within a digital environment, making it easier for such data to be breached. This necessitates a robust cybersecurity infrastructure capable of protecting the personal data of digital users from theft and breaches, thereby safeguarding privacy.

Furthermore, strengthening cybersecurity helps to protect news websites and blogs from sabotage or deliberate blocking, particularly as the digital news landscape has become one of the most modern means of finding out what is happening in the world and of giving a voice to those whose rights and freedoms have been violated.

Given the widespread use of electronic transactions and the exchange of personal and banking information, particularly via electronic media, this exposes users to the risk of hacking whilst making online payments.

Cyber security plays a role in protecting companies from all cyber attacks, such as ransomware attacks, fraud, blackmail and hacking.

Secondly: Protection of electronic contracts

Electronic contracts are defined as: 'an agreement concluded between two or more parties via electronic media, such as websites, applications, email and other means'.

The role of cybersecurity in protecting this form of contract is to safeguard the contract itself by protecting the contracting parties' personal data – including personal information, financial details and commercial information – from unauthorised access or impersonation.

It also protects electronic signatures by ensuring they cannot be forged or tampered with; in 2015, Algeria moved to enact legislation guaranteeing the protection of electronic authentication and signatures.

Furthermore, cybersecurity protects electronic contracts from digital fraud, thereby reducing the use of stolen cards, identity theft, the creation of fraudulent platforms and other such activities.

Section Two: The Negative Impacts of Cybersecurity on Legal Security

Cyber security has a negative impact on the stability of legal security by exposing it to cyber threats or limiting it.

Cyber threats are defined as: 'those attacks and risks carried out using internet mechanisms, networks and computer systems, aimed at causing damage to electronic devices and networks connected to the internet; such threats vary and differ from one country to another depending on the level of technological development and its prevalence.'¹

Applying this concept to the aforementioned objectives of legal security, it becomes clear to us that cyber security affects two of the objectives of legal security, namely: digital rights and freedoms, and the stability of legal transactions.

Firstly: digital rights and freedoms.

The absence or inadequacy of effective mechanisms in the field of cyber security results in the violation of digital rights and freedoms.

Weak cybersecurity results in violations of the right to privacy, infringements of the right to the protection of personal data, and harm to the right to digital property; through the theft of personal data, digital identity theft and impersonation, and the theft of funds from online accounts.

Furthermore, weak cybersecurity facilitates the commission of cybercrimes that damage individuals' reputations: such as defamation via electronic media, including social media platforms and websites, or by hacking into their accounts to obtain photographs, information or private conversations, which the perpetrator then uses as a means of blackmail.

To prevent this, Algeria has put in place an arsenal of laws and institutional mechanisms – which will be discussed in the second section – that go a long way towards protecting users of digital media.

On the other hand, cybersecurity has an impact on individuals' digital freedoms, namely: the freedom of peaceful assembly and trade union organisation; the freedom of access to information; and the freedom

¹ Abdullah Ja'fari, 'Cyber Threats and Their Impact on National Security in Algeria', *African Journal of Legal and Political Studies*, Ahmed Daraya University, Adrar, Algeria, Vol. 06, No. 02, 2022, p. 247.

of opinion and expression. These freedoms are restricted in the name of enhancing cybersecurity – such as through administrative measures – by blocking websites and platforms, deleting posts or accounts deemed to pose a security threat, restricting the use of encryption technologies, and disrupting communication platforms during protests.

Secondly: Electronic contracts

Electronic contracts are based on the principle of trust; weak or non-existent cybersecurity leads to companies being reluctant to accept digital signatures or transactions, for fear of a breach of their personal data or changes to the terms of the contract after signing; by adding new data or the forgery of electronic documents by cybercriminals, or so-called ‘hackers’.

Furthermore, the digital realm is a fertile ground for identity theft, forgery of signatures, and data loss resulting from cyber-attacks such as the transmission of viruses, digital sabotage, etc.

Section Two: Mechanisms for Achieving Cybersecurity and Strengthening Legal Security in Algeria.

Algeria’s shift towards a digital system poses a challenge for the country, given the imminent threat it represents to legal security, particularly in light of the escalating waves of cyber-attacks and threats.

In order to establish a secure digital society, Algeria has sought to put in place legal and institutional mechanisms aimed at countering these threats and thereby achieving cybersecurity, which in turn strengthens legal security in the digital environment.

Section 1: Legal mechanisms for achieving cyber security and strengthening legal security

The Algerian legislature has established an arsenal of legal provisions currently in force, and has also drawn up a national cyber security strategy as a forward-looking vision, in line with the direction set out in the National Digital Transformation Strategy. This is with a view to achieving cyber security and, consequently, strengthening legal security by protecting its foundations from various cyber threats that could undermine its structure and existence.

Section One: Legal mechanisms enacted from 2003 to 2016.

With a view to strengthening cyber security, Algeria has enacted a range of legal provisions, primarily comprising:

- Decree 03-05¹ : This decree, relating to copyright and neighbouring rights, dedicates Chapter One of Title Three to provisions on the protection of copyright, which enable the protection of intellectual works. The author is granted certain rights should their computer programme be altered or distorted; for instance, the right to withdraw it, provided they undertake to compensate the beneficiaries.
- Law No. 04-13:² The amended Code of Criminal Procedure includes an extension of the public prosecutor’s jurisdiction to cover offences relating to automated data processing systems.
- Law 04-15³ : Amending and supplementing Decree 66-156 containing the Penal Code, it provides in its Section 7 bis, entitled ‘Offences against automated data processing systems’.
- Law 16-02⁴ : containing the Penal Code, which criminalises the use of information and communication technologies to commit the acts referred to in Article 02 thereof and amends the provisions of Article 87 bis 11.
- Law No. 08-5 01: This law constitutes the legal basis for the introduction of the ‘Shifa’ card, which enables the assignment of a digital identity to the insured person, thereby facilitating the tracking of

¹- Article 25 of Decree No. 03-05 dated 19 Jumada al-Awwal 1424, corresponding to 19 July 2003, concerning copyright and related rights, Official Gazette, Issue 44, dated 23 July 2003.

²- Law No. 04-14, dated 27 Ramadan 1425, corresponding to 10 November 2004, amending and supplementing Decree No. 06-155 dated 18 Safar 1386, corresponding to 8 June 1966, containing the Code of Criminal Procedure, J.R.J.J., No. 71, dated 10 November 2004.

³- Law No. 04-15, dated 27 Ramadan 1425, corresponding to 10 November 2004, amends and supplements Decree No. 06-156 dated 18 Safar 1386, corresponding to 8 June 1966, containing the Penal Code, J.R.J.J., No. 71, dated 10 November 2004.

⁴- Law No. 16-02 dated 14 Ramadan 1437, corresponding to 19 June 2016, supplements Decree No. 66-156 dated 18 Safar 1386, corresponding to 8 June 1966, containing the Penal Code, J.R.J.J., No. 37, dated 22 June 2016.

⁵- Law No. 08-01 dated 15 Muharram 1429, corresponding to 23 January 2008, amending Law No. 83-11 dated 21 Ramadan 1403, corresponding to 2 July 1983, relating to social insurance, J.R.J.J., No. 04, dated 27 January 2008.

insurance transactions and ensuring that beneficiaries are indeed insured. This Act also provides for penalties for anyone who, through fraud, deletes or alters, in whole or in part, the technical and/or administrative data contained in the social insurance card or in the electronic key, thereby reinforcing the legislator's commitment to protecting the personal data of insured persons.

➤ Law No. 09-04:¹, which sets out specific rules for the prevention and combating of offences relating to information and communication technologies; it provides general protection against all breaches of personal data, regardless of the means involved in its transmission, whether via public or private networks.

Section II: Legal mechanisms in place from 2018 to 2025

The legal mechanisms established to achieve cybersecurity and ensure legal certainty are as follows:

➤ Law 18-07:² The Law on the Protection of Natural Persons with regard to the Processing of Personal Data has established a range of legal safeguards that constitute a new form of protection in the digital sphere.

➤ Law 20-3 05: This law concerns the prevention and combating of discrimination; it addresses the fight against online hate speech, the protection of individuals from digital psychological attacks, the imposition of legal liability on perpetrators of digital crimes, and thereby the strengthening of users' trust in the digital space.

➤ Law 20-4 05: This law amends Decree 66-156, which contains the Penal Code; Article 2 of the law criminalises any publication, promotion or dissemination of information that undermines public order and security by any means, including information and communication technologies.

➤ Presidential Decree 20-5 05: The issuance of this decree marks a qualitative leap forward in the consolidation of cyber security, as it aims to establish a national information systems security framework through the creation of two bodies under the Ministry of National Defence: the National Council for Information Systems Security and the Agency for Information Systems Security, whilst defining the composition, remit, organisation and functioning of each body.

➤ Law 25-11: This law amends Law 18-07 and introduces new concepts and terminology such as biometric data, a profile and anonymisation; this allows for the precise definition of the various forms of digital data and how they should be handled legally. The National Authority for the Protection of Personal Data was also established.

The same Act also provides for the appointment of a data protection officer or data protection representative, whose role is to liaise between the organisation and the National Data Protection Authority.

In addition, a specific chapter has been included on data processing by the judiciary and the police, whilst the role of the National Data Protection Authority has been strengthened by expanding its powers of oversight and inspection.

Second: The National Cybersecurity Strategy

The National Information Systems Security Authority is the state's instrument for achieving cyber security; to this end, it has been entrusted with the task of drawing up the National Cyber Security Strategy and protecting information systems in line with the provisions of the National Digital Transformation Strategy, and to ensure legal certainty.

1- Law No. 09-04, dated 14 Sha'ban 1430, corresponding to 5 August 2009, setting out specific rules for the prevention of offences relating to information and communication technologies, J.R.J.J., No. 47, dated 16 August 2009.

2- Law No. 18-07, dated 25 Ramadan 1439, corresponding to 10 June 2018, concerning the protection of natural persons with regard to the processing of personal data, Official Journal of the Kingdom of Morocco, No. 34, dated 10 June 2018.

3- Article 5 of Law No. 20-05, dated 5 Ramadan 1441, corresponding to 28 April 2020, concerning the prevention and combating of discrimination and hate speech, Official Gazette, No. 25, dated 29 April 2020.

4- Law No. 20-06, dated 5 Ramadan 1441, corresponding to 28 April 2020, amending and supplementing Decree No. 66-156 dated 18 Safar 1386, corresponding to 8 June 1966, containing the Penal Code, J.R.J.J., No. 25, dated 29 April 2020.

5- Presidential Decree No. 20-05, dated 24 Jumada al-Awwal 1441, corresponding to 20 January 2020, concerning the establishment of a national information systems security framework, J.R.J.J., Issue No. 04, dated 26 January 2020.

In this context, on 28 April 2025, a workshop entitled 'The National Strategy for Information Systems Security', organised by the Information Systems Security Agency, took place at the National Preparatory School for Engineering Studies in Rouiba, in the First Military District. The workshop ran until 30 April 2025 and was attended by representatives from the Presidency of the Republic, the Prime Minister's Office and various ministerial departments, as well as academics and stakeholders from the public and private sectors in the field of cyber security. Presentations addressed key themes related to the National Information Systems Security Strategy, such as the protection of critical infrastructure and national capabilities for responding to cyber incidents, as well as the legal and regulatory framework, in addition to international cooperation, national partnership and the establishment of an environment conducive to cybersecurity.

A representative of the Information Systems Agency under the Ministry of National Defence also revealed to Al-Ayyam News the measures taken by the state in the field of cybersecurity, highlighting the key features of the National Strategy for Information Systems Security and the adopted legal, regulatory and standards framework¹.

His remarks came during a parliamentary session organised by the Committee on Legal, Administrative and Civil Liberties of the National People's Assembly, entitled 'Legal Liability for Cybercrimes and Artificial Intelligence: Legislative Gaps and Future Challenges'.

He highlighted the sophistication of current cyber-attacks, which target states' critical infrastructure, including legal security, necessitating the development of a national information security plan in line with the decisions taken by the President of the Republic to safeguard the country's digital transformation.

As part of efforts to strengthen the legal framework and improve the legislative system relating to data protection and information systems, particularly those concerning personal data, a representative of the Ministry of National Defence announced the preparation of a draft bill addressing the technical, legal and regulatory aspects of cyber security. A working group has also been established to draft this bill and develop an appropriate framework to counter growing digital threats.

Second requirement: Institutional mechanisms for achieving cybersecurity and strengthening legal security

With a view to strengthening legal security in the context of digital transformation, Algeria has established an institutional framework to ensure cybersecurity. This consists of a group of bodies, most of which are sector-specific regulatory bodies active in the field of protecting the rights and freedoms of individuals in particular, in addition to other bodies specialising in the cyber domain, established by Presidential Decree 20-05.

Section One: Institutional mechanisms established to protect individuals from the risks of digital transformation

These mechanisms consist of various administrative authorities across different sectors that have been entrusted with the task of safeguarding individuals and their personal data from any cyber-attacks. These include:

Firstly: Electronic Certification Authorities

Law No. 15-04², in Articles 29, 26 and 16, sets out the authorities active in the field of electronic authentication, namely:

- The National Authority for Electronic Certification: This is provided for in Article 16 of Law No. 15-04; it is defined as an administrative authority established under the Prime Minister, tasked with promoting and developing the use of electronic signatures and certification and ensuring the reliability of their use.

¹- Al-Tayeb Saadallah, 'New draft law under preparation to strengthen cyber security in Algeria', newspaper article published on the Al-Ayyam NEWS website, 1 July 2025, accessed on 17 November 2025 at 22:20.

<https://elayem.news/01-07-25-58-36100-mchrwa-qanwn-jdyd-qyd-althdyr-ltazyz-almn-alsybrany-fy-aljzair.html>

²- Law No. 15-04 dated 11 Rabi' al-Thani 1436, corresponding to 1 February 2025, laying down the general rules governing electronic signatures and authentication, Official Gazette, Issue No. 06, dated 10 February 2015.

To this end, it carries out a number of tasks specified in Article 18 of the same Act.¹

- The Governmental Authority for Electronic Certification: Pursuant to Article 26 of the same Act, this is another governmental authority for electronic certification attached to the Minister responsible for Post, Information Technology and Communications, tasked with monitoring and supervising the electronic certification of trusted third parties, as well as providing electronic certification services to stakeholders in the government sector, in accordance with Article 28.²

- The Economic Authority for Electronic Certification: This is the authority responsible for regulating postal services and wired and wireless telecommunications, in accordance with Article 29 of the same Act.

Secondly: The National Authority for the Prevention of Crimes Related to Information and Communication Technologies

Presidential Decree No. 15-261³ established the National Authority pursuant to Article 2 thereof, entrusting it with a range of tasks set out in Law No. 09-04⁴, specifically in Article 14 thereof.

In particular:

- Ensuring the preventive monitoring of electronic communications with a view to detecting offences relating to acts of terrorism, sabotage and threats to state security, under the authority of the competent judge, to the exclusion of any other national bodies.

- Contributing to the training of investigators specialising in technical investigations relating to information and communication technologies.

- Developing cooperation with national institutions and bodies concerned with offences relating to information and communication technologies; and other tasks.⁵

Third: The National Authority for the Protection of Personal Data.

This Authority was established pursuant to Article 22 of Law No. 18-07⁶, which states: “An independent administrative authority for the protection of personal data, hereinafter referred to as the National Authority, shall be established under the President of the Republic, with its headquarters in Algiers...”.

This Authority is responsible for ensuring that the processing of personal data complies with the provisions of this Act and for guaranteeing that the use of information and communication technologies does not pose any risks to individual rights, public freedoms or private life.⁷

It should be noted in this regard that this Authority was established to protect the rights of individuals, public freedoms and private life – which are considered elements of legal security – from cyber-attacks and threats.

To this end, the National Authority for the Protection of Personal Data has launched a portal designed to enable public and private bodies, as well as natural persons involved in the processing of personal data, by creating a dedicated account to access the portal and completing an online form for prior authorisation of processing and licence applications, whilst being able to track the status of their applications.

Fourth: Bodies affiliated with the National Security and Gendarmerie

1. The National Gendarmerie’s Centre for the Prevention of Computer-Related Crimes:

This body, established in 2008, analyses data and information and identifies the perpetrators of cybercrime, whether they be individuals, a state, an organisation or other entity. It works to prevent and

¹- See Article 18, Law No. 15-04, op. cit.

²- For further details, see Article 28, ibid.

³- Law No. 15-261, dated Dhu al-Hijjah 1436, corresponding to 8 October 2015, sets out the composition, organisation and operating procedures of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, Official Gazette, Issue No. 35, dated 18 October 2015.

⁴- See Article 2 of Law 09-04, op. cit.

⁵- For further details, see Article 2 of Presidential Decree 15-261, op. cit., and Article 14 of Law 09-04.

⁶- See Article 22 of Law No. 18-07, op. cit.

⁷ - See paragraph 01 of Article 25, ibid.

combat cybercrime; 'prevention' refers to launching awareness campaigns to highlight and publicise cybercrime, whilst 'combating' refers to raising awareness of the negative uses of the internet¹.

2. The National Institute of Forensic Science and Criminology of the National Gendarmerie:

This is a public institution under the direct supervision of the Minister of National Defence. Its remit includes the design and development of databases, and the conduct of research relating to these activities through the use of precision technologies, in addition to other tasks.

It comprises several departments, such as the Fingerprints Department, the Documentation Department, and the Computer Forensics Department, which is responsible for monitoring, controlling and tracking cyber-attacks, computer piracy, and the reverse engineering of software, etc.²

3. The Central Department for Combating Cybercrime, attached to the National Security Directorate:

This is the core unit for combating cybercrime within the National Security Directorate. It was established in 2011, following which the Central Unit for Combating Crimes Related to Information and Communication Technologies was set up by a decision of the Director-General of National Security and attached to the Judicial Police Directorate in January 2015.

Section Two: Institutional Mechanisms under Presidential Decree 20-05

Given that the aforementioned bodies were not sufficiently effective in protecting individuals and their freedoms—including safeguarding legal certainty against cyber risks and threats—the President of the Republic, Mr Abdelmadjid Tebboune, established, by Presidential Decree 20-05, two bodies specialising in cyber security to be placed under the Ministry of National Defence, namely: the National Council for Information Systems Security and the Information Systems Security Agency.

First: The National Council for Information Systems Security

This is considered one of the most important bodies in the field of cyber security; it is an agency under the supervision of the Ministry of National Defence, responsible for drawing up the national strategy for information systems security, and in particular:

- Deciding on and defining the elements of the national strategy for information systems security proposed by the Agency;
- Examining and endorsing the Agency's work plan and activities.
- Examining and approving reports relating to the implementation of the national strategy for information systems security.
- Approving the classification of information systems.
- Approving the national authority's electronic certification policy.
- The Council shall issue a concurring opinion on any draft legislative or regulatory text relating to information systems security.

II: The Information Systems Security Agency

This is provided for in Article 17 of Presidential Decree 20-05³; the Agency is a public administrative body responsible in particular for:

- Conducting digital investigations in the event of cyber-attacks or incidents targeting national institutions.
- Preparing elements of the national strategy in the field of information systems and other tasks.
- Proposing draft legislative or regulatory texts in the field of information systems security, following the Council's approval.
- Monitoring information system security audits and other tasks.⁴

¹- Wajoot Souad, 'Combating Cybercrime at the National Level', Scientific **Research Journals**, Vol. 12, No. 04, 2024, p. 421.

²- Nabila Adan, 'Legal Mechanisms for Addressing the Challenges of Cyberspace – Algeria as a Case Study', **Algerian Journal of Political Science and International Relations**, Vol. 05, No. 01, June 2012, p. 19.

³ See Article 17 of Decree 20-05, op. cit.

⁴ For further details, see Article 18, ibid.

Conclusion

From the foregoing, we conclude that there is a direct correlation between cyber security and digital legal security: if cyber security is enshrined, digital legal security is achieved; and the reverse is true; if cyber security is not enshrined, digital legal security will be vulnerable to cyber threats and attacks.

We also conclude, through an examination of legal mechanisms, that the Algerian legislature has provided for deterrent measures, such as stipulating various penalties for the commission of a digital crime or a breach of personal privacy – that is, intervention after damage has occurred – within the digital environment.

Furthermore, by examining institutional mechanisms, we observe that these are regulatory bodies for specific sectors, specialising in the digital sphere and the protection of digital legal security.

Recommendations:

Based on the findings, the following recommendations can be made:

- The need to expedite the establishment of a legal framework specific to cyber security.
- The need to establish cybersecurity controls.
- There is a need to establish an infrastructure capable of enhancing the protection of individuals operating within the digital environment from any violations.
- Both cybersecurity and digital legal security should be enshrined in the Constitution, just as legal security is, given that digital legal security is a modern manifestation of legal security.
- Concluding international cooperation agreements, particularly in the field of cross-border breaches, and drawing on the experiences of leading nations in the field of cybersecurity in order to benefit from their expertise.
- Technical and judicial capacity-building by increasing the number of specialists in digital investigation in line with emerging threats.

List of Sources and References

First: Sources

- Legislation

- 1- Law No. 04-14, dated 27 Ramadan 1425 (corresponding to 10 November 2004), amending and supplementing Decree No. 06-155 dated 18 Safar 1386 (corresponding to 8 June 1966), containing the Code of Criminal Procedure, J.R.J.J., No. 71, dated 10 November 2004.
- 2- Law No. 04-15, dated 27 Ramadan 1425, corresponding to 10 November 2004, amends and supplements Decree No. 06-156 dated 18 Safar 1386, corresponding to 8 June 1966, containing the Penal Code, J.R.J.J., No. 71, dated 10 November 2004.
- 3- Law No. 08-01 dated 15 Muharram 1429, corresponding to 23 January 2008, supplements Law No. 83-11 dated 21 Ramadan 1403, corresponding to 2 July 1983, relating to social insurance, J.R.J.J., No. 04, dated 27 January 2008.
- 4- Law No. 09-04, dated 14 Sha'ban 1430, corresponding to 5 August 2009, sets out the specific rules for the prevention of offences relating to information and communication technologies, J.R.J.J., No. 47, dated 16 August 2009.
- 5- Law No. 15-04, dated 11 Rabi' al-Thani 1436, corresponding to 1 February 2015, lays down the general rules governing electronic signatures and authentication, Official Gazette, No. 06, dated 10 February 2015.

6- Law No. 15-261, dated Dhu al-Hijjah 1436, corresponding to 8 October 2015, defining the composition, organisation and operating procedures of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, Official Gazette, No. 35, dated 18 October 2015.

7- Law No. 16-02, dated 14 Ramadan 1437, corresponding to 19 June 2016, amending Decree No. 66-156, dated 18 Safar 1386, corresponding to 8 June 1966, containing the Penal Code, J.R.J.J., No. 37, dated 22 June 2016.

8- Law No. 18-07, dated 25 Ramadan 1439, corresponding to 10 June 2018, concerning the protection of natural persons with regard to the processing of personal data, J.R.J.J., No. 34, dated 10 June 2018.

9- Law No. 20-05, dated 5 Ramadan 1441, corresponding to 28 April 2020, concerning the prevention and combating of discrimination and hate speech, Official Gazette, No. 25, dated 29 April 2020.

10- Law No. 20-06, dated 5 Ramadan 1441, corresponding to 28 April 2020, amending and supplementing Decree No. 66-156 dated 18 Safar 1386, corresponding to 8 June 1966, containing the Penal Code, Official Gazette, No. 25, dated 29 April 2020.

- Decrees:

1. Decree No. 66-156 dated 18 Safar 1386, corresponding to 8 June 1966, containing the Penal Code, J.R.J.J., No. 25, dated 29 April 2020.

2- Decree No. 03-05 dated 19 Jumada al-Awwal 1424, corresponding to 19 July 2003, concerning copyright and related rights, J.R.J.J., Issue No. 44, dated 23 July 2003.

- Decrees:

1. Presidential Decree No. 20-05, dated 24 Jumada al-Awwal 1441, corresponding to 20 January 2020, concerning the establishment of a national information systems security framework, Official Gazette, Issue No. 04, dated 26 January 2020.

Second: List of References

- Academic books:

1. Belkhir, Mohamed Aït Oudieh, **Legal Security and its Foundations in Administrative Law**, Dar al-Khaliduniya, 2018.

2. Fatih Khaloufi, **The Powers of the Administrative Judge in Interpretation**, Dar Houma for Printing, Publishing and Distribution, Algiers, 2017.

- Doctoral theses:

1- Abdelhay Yahya, **'The Principle of Legal Certainty and its Applications in the Jurisprudence of the Council of State'**, thesis submitted for a Doctor of Science degree, specialising in Public Law, Faculty of Law and Political Science, Martyr Hama Lakhdar University, El Oued, academic year 2022–2023.

- Academic articles:

1- Dalal Louchane and Fatiha Bouaqal, 'Legal Certainty: Between Legislative Guarantees and the Risks of Judicial Discretion', **Al-Bahith Journal of Academic Studies**, University of Batna, Vol. 05, No. 12, January 2018.

2- Mohamed bin Daima and Samir Shaaban, 'Upholding the Principle of Legal Certainty in Light of the Specific Nature of Business Criminal Law in Algerian Legislation', **Al-Bahith Journal of Academic Studies**, Vol. 10, No. 02, June 2023.

3- Nabila Adan, 'Legal Mechanisms for Addressing the Challenges of Cyberspace – Algeria as a Case Study', **Algerian Journal of Political Science and International Relations**, Vol. 5, No. 1, June 2012.

4- Souad Wajout, 'Combating Cybercrime at the National Level', **Scientific Research Notebooks**, Vol. 12, No. 04, 2024.

5- Abdullah Ja'fari, 'Cyber Threats and Their Impact on National Security in Algeria', **African Journal of Legal and Political Studies**, Ahmed Daraya University, Adrar, Algeria, Vol. 06, No. 02, 2022.

- Academic presentations:

1- Husam Bouhajar, 'The Concept and Foundations of the Principle of Legal Security', presentation delivered at the local symposium on legal security, 15 October 2024, University of Guelma, p. 04.

- Online newspaper articles:

- Al-Tayyib Saadallah, 'New draft law under preparation to strengthen cyber security in Algeria', newspaper article published on the Al-Ayyam NEWS website, 1 July 2025, accessed 17 November 2025 at 22:20.

<https://elayem.news/01-07-25-58-36100-mchrwa-qanwn-jdyd-qyd-althdyr-ltazyz-almn-alsybrany-fy-aljzair.html>

- Websites:

1- Strategic Action in the Field of Cybersecurity, **Guide to Preparing the National Cybersecurity Strategy**, Issue 02, 2021, p. 12, accessed on 17 November 2025 at 19:00, published on the website: <https://ncsguide.org/wp-content/uploads/2024/05/508938A.pdf>

2- Presentation on cyber security, Enterprises, General Authority for Small and Medium-sized Enterprises, 2022, p. 3, published on the General Authority for Small and Medium-sized Enterprises website, accessed on 4 November 2025 at 20:55.

[https://www.monshaat.gov.sa/sites/default/files/2023-](https://www.monshaat.gov.sa/sites/default/files/2023-03/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%20.pdf)

[03/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%20.pdf](https://www.monshaat.gov.sa/sites/default/files/2023-03/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%20.pdf)

3- Basic Cybersecurity Controls, Saudi National Cybersecurity Authority, 2024, ECC02, accessed on 4 November 2025 at 22:00, published on the Authority's website

https://cdn.nca.gov.sa/api/files/public/upload/29a9e86a-595f-4af9-8db5-88715a458a14_ECC-2-2024--NCA.pdf

Recibido: 31/07/2026 · Aceptado: 12/09/2026 · Publicado: 10/10/2026

Declaraciones

Conflictos de interés: La autora declara no tener conflictos de interés relacionados con este estudio.

Financiación: La autora declara que este estudio no recibió financiación específica.

Responsabilidad autoral: La autora asume la responsabilidad del contenido del artículo.

Licencia

Este artículo se publica bajo la licencia Creative Commons Atribución 4.0 Internacional (CC BY 4.0), que permite su uso, distribución, reproducción y adaptación en cualquier medio, siempre que se cite adecuadamente a la autora y la fuente, se incluya un enlace a la licencia y se indiquen los cambios realizados.

<https://creativecommons.org/licenses/by/4.0/>

