

Crimes Targeting Administrative Operations Across the Internet Space

Djenadi Abdelhaq

University of Saida Dr Moulay Tahar, Algeria

Email: abdelhak.janadi@univ-saida.dz

Abstract

The contemporary world is witnessing a radical transition toward digital administration, which has generated severe security and legal challenges manifested in the emergence of novel patterns of crimes targeting administrative operations across the internet space. These crimes threaten the pillars of the modern administrative state, foremost among which is the electronic signature—serving as the backbone of digital reliability and trust—as well as classified administrative information and documents inextricably linked to the security and stability of the State. Faced with this threat intersecting with digital transformation, the Algerian legislature intervened with a preventive and punitive legislative arsenal, most notably Law No. 15-04 relating to electronic signature and electronic certification, and Ordinance No. 21-09 relating to the protection of administrative information and documents. This research aims to shed light on these crimes by establishing their conceptual framework, identifying their legislative manifestations, and reviewing the punitive mechanisms capable of achieving general and special deterrence. To address this issue, the study adopted a descriptive-analytical methodology to examine legal provisions and interpret their content. The research concluded that the Algerian legislature has adopted a rigorous preventive and punitive approach to protect the digital administrative system, while recommending the necessity of keeping pace with continuous technological developments, and enhancing training and technical monitoring mechanisms to curb these novel risks and ensure the security of electronic administrative transactions.

Introduction

The contemporary world is witnessing a massive technological revolution in the fields of communication and information, which has led to the transition from traditional administration to an electronic administration relying on the internet space to manage and conduct its transactions. Despite the numerous benefits of this digital transformation, it has generated severe legal and security challenges and risks, represented by the emergence of novel patterns of criminality: namely, crimes targeting administrative operations across the internet space. These crimes target the pillars of digital administration, foremost among which is the electronic signature—serving as the authentication tool and evidentiary basis for transactions—as well as classified administrative information and documents that affect the security and public tranquility of the State.

Received: June 22, 2026; Accepted: September 17, 2026; Published: September 29, 2026

© 2026 The Author. Published by IMCRA. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, adaptation, and reproduction in any medium, provided that the original author and source are properly credited.

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



Faced with this perilous situation, the Algerian legislature found itself compelled to intervene to protect the digital administrative system from breaches and tampering. Consequently, it enacted a robust legal arsenal dedicated to this system, most notably Law No. 15-04 laying down the general rules relating to electronic signature and electronic certification, and Ordinance No. 21-09 relating to the protection of administrative information and documents. This research aims to shed light on these crimes by defining their concept, manifestations, and the punitive mechanisms capable of achieving general and special deterrence to curb their gravity. Accordingly, we have chosen to divide this study into two sections: the first section addresses the concept of crimes affecting the electronic signature, while the second section is dedicated to identifying the crimes targeting administrative information and documents.

Section I: The Conceptual Framework of Crimes Impairing Electronic Signatures

The electronic signature is considered the lifeblood of modern administrative and financial transactions within the internet space, serving as the digital alternative to the traditional handwritten signature that confers legal evidentiary value upon documents. Given the paramount importance of this mechanism, it has become a primary target for hackers and cybercriminals, prompting the Algerian legislature to surround it with rigorous protective guarantees to ensure its reliability. Consequently, this section is dedicated to deconstructing crimes impairing electronic signatures through the study of two complementary dimensions: the first dimension addresses the electronic signature and the manifestations of crimes impairing it, through its legal and doctrinal definition along with its substantive conditions, while reviewing the most prominent manifestations of these crimes—whether those targeting data or crimes committed by electronic certification service providers and auditing officers. The second dimension addresses the punitive policy and strict penalties enacted by the Algerian legislature to deter any infringement upon the security and confidentiality of this digital system.

First Division: The Electronic Signature and Manifestations of Crimes Impairing It

This division addresses the electronic signature as a modern method for identifying the signatory and its legal nature by allocating a subsection titled "Definition of the Electronic Signature," while a second subsection is dedicated to outlining the manifestations of crimes that may occur against electronic signatures and certification.

Subsection 1: Definition of the Electronic Signature

The electronic signature refers to data in electronic form incorporated into, attached to, or logically associated with a data message, which may be used to identify or authenticate the signatory in relation to the data message, and to indicate the signatory's approval of the information contained in the data message [1] .

It has also been defined as anything placed on an electronic document in the form of letters, numbers, symbols, signs, or others; meaning the procedure performed by the sender to link their identity to the signed document in order to enable the recipient to verify the validity of this signature. This constitutes a cryptographic communication method that works to authenticate transactions conducted via the internet [2] , through a set of mixed numbers interacting within specific and complex mathematical relations, thereby forming a secret code linked to the signatory's person [3] , via a restricted unit of data bearing mathematical relations with the data available in the content of the signed document [4] .

As for the Algerian legislature, it addressed the definition of the electronic signature pursuant to Executive Decree No. 07-162 relating to the exploitation regime applicable to each type of

network—including wireless electrical networks—and to various wire and wireless telecommunication services. The decree defined the "secure electronic signature" as a signature performed electronically, provided it meets specific requirements: being unique to the signatory, created by means that the signatory can keep under their exclusive control [5], and ensuring a link with the associated act such that any subsequent alteration of the act is detectable.

Furthermore, the Algerian legislature defined it under Law No. 15-04 laying down general rules relating to electronic signature and electronic certification as a set of data in electronic form, attached or logically linked to other electronic data, used as a means of authentication and executed by the signatory—defined as a natural person holding electronic signature creation data [6]—acting on their own behalf or on behalf of the natural or legal person they represent. This signature is executed through a creation mechanism consisting of a device or computer program designed to apply the electronic signature creation data, which is evidenced by an electronic certification certificate—an electronic document intended to prove the link between the electronic signature verification data and its signatory [7]. Based on this definition, the electronic signature is founded upon conditions represented by its association with the owner, enabling the identification of the signatory through their signature, in addition to the availability of a qualified electronic certification certificate; meaning it takes the form of a qualified electronic signature possessing the following attributes:

1. Created on the basis of a qualified electronic certification certificate.
2. Linked exclusively to the signatory.
3. Enabling the identification of the signatory.
4. Designed by means of a secure mechanism dedicated to electronic signature creation.
5. Created by means under the exclusive control of the signatory.
6. Linked to its specific data in such a way that subsequent changes to these data can be detected [8].

Subsection 2: Manifestations of Crimes Impairing Electronic Signatures and Certification

This subsection identifies the various acts constituting manifestations of crimes targeting electronic signatures and certification according to the following classification:

First: The Misdemeanor of Infringing upon Electronic Signature Data

This crime targets electronic signature creation data, which consist of unique data such as codes or private cryptographic keys used by the signatory to generate an electronic signature. The illegal acts constituting this crime include the possession, disclosure, or use of electronic signature creation data [9]. Possession denotes the factual authority vested in a person to exercise control over an item, portraying them as the rightful claimant; illegal possession is materialized through the wilful control of information and its exploitation by the possessor [10]. Disclosure refers to propagating, broadcasting, or divulging third-party electronic signature data—namely, the perpetrator making these data accessible to unauthorized individuals, which constitutes a violation of the confidentiality of the signatory's data [11].

As for use, it entails utilizing the electronic signature data or its creation data subsequent to possession. This usage undermines the security and confidentiality of the signature data or the signatory's particulars, thereby representing an unlawful infringement by the perpetrator upon the latter's privacy in utilizing their electronic signature.

Second: Misdemeanors Committed by Electronic Certification Service Providers

The commission of these crimes presupposes that the perpetrator holds the status of an electronic certification service provider. The latter is defined as any natural or legal person who issues qualified electronic certificates—defined as electronic documents proving the link between verification data and the signatory—and may provide other services in the field of electronic certification [12].

The crime committed by an electronic certification service provider materializes as the misdemeanor of breaching the obligation to notify the economic authority of the cessation of its activity within the statutory deadlines [13]. This crime is constituted by the provider's omission to inform the economic authority of the cessation of its operations as specified under the provisions governing the performance of certification services [14]. The criminal conduct of this offense is consummated merely by the abstention of the authorized body licensed to issue electronic certification certificates from continuing their issuance, without the condition of notifying the supervisory authority thereof [15]. Furthermore, any electronic certification service provider that resumes or continues its activity despite lacking a license or following its withdrawal is deemed to have committed the misdemeanor of issuing an electronic certification certificate without prior license or after its withdrawal. "License" refers to the regulatory regime for exploiting electronic certification services, embodied in the official document personally granted to the service provider, permitting the actual commencement of service provision [16].

Criminal liability also attaches to the electronic certification service provider upon committing the misdemeanor of breaching the duty to maintain the confidentiality of data and information related to issued certification certificates, whether resulting from non-compliance with regulatory and technical rules and procedures concerning electronic signatures [17]—such as the signature creation mechanism lacking security [18]—or the provider disclosing such data by granting access to unauthorized third parties. Additionally, the misdemeanor of assaulting the volition of the person concerned by the signature is established against the electronic signature provider when the latter collects the signatory's personal data without explicit consent [19]. The criminal conduct of this misdemeanor consists of the positive act performed by the perpetrator of utilizing electronic signature data for unallocated purposes, or collecting such data merely by inferring the concerned person's acceptance without regard to their explicit consent [20].

Third: Misdemeanors Committed by Auditing Officers

Auditing refers to the procedure of verifying the conformity between electronic signature data and the signatory in accordance with a specific frame of reference [21]. Auditing operations fall within the remit of electronic certification authorities, comprising both the National Electronic Certification Authority—an administrative authority established under the Prime Minister, tasked with promoting, developing, and ensuring the reliability of electronic signature and certification usage, possessing various missions including conducting audits at the governmental and economic electronic certification levels via the governmental auditing body [22]—and the Governmental Electronic Certification Authority.

The latter authority is established under the minister responsible for posts and information and communication technologies, and is tasked with monitoring and controlling the electronic certification activity of trusted third parties, as well as providing electronic certification services for stakeholders in the governmental sector [23]. In the performance of its duties, it undertakes auditing operations at the level of the trusted third party [24] in accordance with the adopted certification policy [25].

In addition to the aforementioned authorities, the Authority for Regulating Posts and Electronic Communications appoints the Economic Electronic Certification Authority, which is tasked with monitoring and controlling electronic certification service providers offering signature and certification services to the public [26], thereby exercising inspection and auditing functions [27]. The crime committed against any auditing officer belonging to any electronic certification authority consists of the act of disclosing confidential information acquired during the exercise of auditing procedures, whether through divulgence, broadcasting, or revelation.

Second Division: Penalties Prescribed for Crimes Related to Electronic Signatures and Certification

In accordance with statutory and judicial practice, every criminal offense entails a prescribed

penal sanction. This division is accordingly divided into three subsections: the first is dedicated to determining the penalty prescribed for the misdemeanor of infringing upon electronic signature data, the second addresses penalties for misdemeanors committed by electronic certification service providers, and the third establishes penalties for misdemeanors committed by auditing officers.

Subsection 1: Penalty Prescribed for the Misdemeanor of Infringing upon Electronic Signature Data

Any one or more of the acts constituting this crime—encompassing possession, disclosure, or use—is punishable by imprisonment ranging from three (03) months to three (03) years, and a financial fine ranging from 1,000,000 DZD to 5,000,000 DZD, or either of these penalties exclusively [28] .

Subsection 2: Penalties Prescribed for Misdemeanors Committed by Electronic Certification Service Providers

An electronic certification service provider who breaches the obligation to notify the economic authority of its activity cessation within statutory deadlines is punished by a custodial sentence ranging from two (02) months to one (01) year of imprisonment, and a financial fine ranging from 200,000 DZD to 1,000,000 DZD, or either of these penalties [29] . Furthermore, an electronic certification service provider targeting the public who resumes or continues its activity after the withdrawal of its license, or operates without a license, is punished by imprisonment ranging from one (01) year to three (03) years, alongside a financial fine ranging from 200,000 DZD to 2,000,000 DZD, or either penalty [30] .

Moreover, an electronic certification service provider committing the misdemeanor of violating confidentiality regarding granted certification certificates is punished by imprisonment ranging from three (03) months to two (02) years, plus a financial fine ranging from 200,000 DZD to 1,000,000 DZD, or either penalty alone [31] .

As for the electronic signature provider committing the misdemeanor of infringing upon the signatory's volition by collecting personal data without explicit consent, the prescribed custodial penalty is imprisonment from six (06) months to three (03) years, and a financial fine ranging from 200,000 DZD to 1,000,000 DZD, or either of these two penalties exclusively [32] .

Subsection 3: Penalty Prescribed for Misdemeanors Committed by Auditing Officers

Any auditing officer belonging to any electronic certification authority who commits unlawful disclosure—via divulgence, broadcasting, or revelation—of confidential information accessed during auditing procedures is subject to imprisonment ranging from three (03) months to two (02) years, and a financial fine ranging from 20,000 DZD to 200,000 DZD, or either penalty exclusively [33]

Section II: Crimes Targeting Administrative Information and Documents

The concept of the "public servant" first appeared explicitly in Article 04 of Ordinance No. 06-03 embodying the General Statute of the Public Service. A public servant is considered to be any agent appointed to a permanent public office and established in an administrative rank in accordance with the administrative hierarchy. Specific conditions must be met for a person to acquire the status of a public servant, namely: appointment to the position by public authority [34] —meaning that the appointment decision must be issued by a competent authority in a lawful manner—service in a public utility, and establishment (tenure) in a rank of the administrative hierarchy [35] .

Law No. 06-01 on Preventing and Combating Corruption added a broader definition of the public servant, considering it to be any person holding an administrative, executive, or judicial office, or serving in elected popular councils by virtue of appointment or election, whether on a permanent or temporary basis and whether remunerated or unremunerated. The status of public servant also attaches to any person holding a legislative, executive, administrative, or judicial office in a foreign country, or exercising a public function for a public body or enterprise on behalf of a foreign country, whether such employment is by appointment or election [36].

As for Ordinance No. 21-09 under study—concerning the protection of administrative information and documents—the Algerian legislature defined the public servant as any person holding a legislative, executive, administrative, or judicial office, or serving in local elected popular councils, whether appointed or elected, on a permanent or temporary basis, remunerated or unremunerated, regardless of their rank or seniority.

Furthermore, the category of public servants encompasses any other person who undertakes, even temporarily, an office or agency—remunerated or unremunerated—and contributes in this capacity to the service of a public body, public enterprise, any other enterprise in which the State owns all or part of the capital, or any other institution providing a public service, in addition to any other person defined as a public servant or assimilated person pursuant to laws and regulations in force [37].

First Division: The Conceptual Framework of Administrative Information and Documents and Manifestations of Crimes Impairing Them

Administrative information and documents are traditionally physical in nature; however, having been influenced by digital developments across various fields, they have assumed electronic forms capable of being traded within a digital environment. Given that crime is a phenomenon as old as humanity and evolves alongside it, administrative information and documents can become the subject matter of a crime, either inherently or through various transactions related or linked to them. Accordingly, this division is divided into two subsections: the first is dedicated to defining administrative information and documents in their traditional and modern forms, while the second addresses the various manifestations of crimes targeting administrative information and documents via the internet.

Subsection 1: Definition of Administrative Information and Documents

Doctrinally, a document is defined as a written instrument certified by an official body or signed by the person issuing it, containing what is termed a legal act or a legal event, with legal acts predominantly comprising administrative documents [38]. A "legal act" refers to administrative action that establishes, revokes, or modifies a specific obligation [39]. Information is defined as everything a person knows about an issue or incident, a collection of news and investigations, or anything leading to the discovery of truths and the clarification of matters—namely, truths about any subject, collections of ideas and facts about persons and places, or knowledge acquired through communication or research [40].

As for the Algerian legislature, it defined a document as correspondence, writings, and records created or obtained by any given authority [41] during the exercise of its activity. It also defined information as any event or news regardless of source—whether a document, photograph, audio recording, visual recording, audiovisual recording, conversation, or telephone call—the disclosure of which would prejudice the concerned authorities.

It is noteworthy that administrative information and documents assume an electronic form. The Algerian legislature addressed this in its definition of classified documents, considering them to be any

paper or electronic writing, drawing, plan, map, photograph, audio or audiovisual recording, or any other physical or electronic medium subjected to measures aimed at preventing their publication or restricting access to them [42]. Consequently, an electronic document is an instrument composed of various characters, numbers, or digital signs—including those exchanged via communication وسائل—possessing an understandable content, maintained on an electronic medium enabling reading or retrieval when necessary [43].

Subsection 2: Manifestations of Crimes Targeting Administrative Information and Documents via the Internet

Certain crimes addressed by the Algerian legislature under Ordinance No. 21-09 concerning the protection of administrative information and documents fall within cybercrimes involving the illicit use of the internet. Some of these require the fulfillment of a presumptive element for criminal liability to attach—specifically, crimes committed by a public servant—while others can be committed by either a public servant or a third party. These crimes assume the following manifestations:

First: The Misdemeanor of Unlawful Electronic Access to Classified Information or Documents

Access in this crime does not differ from access regarding automated data processing systems as stipulated under Law No. 04-15 [Note: referring to Law 09-04 / 04-15 contextually], assuming an illicit character—meaning the perpetrator lacks the requisite legal authority or license to access electronically stored data. This crime targets classified electronic information and documents, encompassing electronically written correspondence, records, or any electronic document whose publication is prohibited or subject to access restrictions. Furthermore, the Algerian legislature broadened the means through which this crime can be committed and defined its subject matter by criminalizing unauthorized access to any information system, website, or electronic network belonging to the concerned authorities, committed by employing any information and communication technology means with the illicit objective of acquiring classified electronic information or documents [44].

Second: The Misdemeanor of Electronic Publication of Classified Administrative Information or Documents

Publication refers to disclosure, the essence of which consists of imparting specific information to third parties. Disclosure materializes in written or oral form, directly or indirectly, wholly or partially, directed at an individual, groups, or the public, whether addressed to domestic or foreign entities [45]. Pursuant to the Algerian legislature's stipulations, this crime involves divulging classified information and documents—whether obtained as a result of committing the misdemeanor of unlawful electronic access to electronic media storing classified information and documents, or those utilized for publishing them wholly or partially via websites, electronic accounts, or software programs. Criminal liability attaches to anyone committing the criminal conduct of unlawful electronic publication, as well as anyone who establishes, manages, or supervises the websites, electronic accounts, or software programs utilized in perpetrating the crime [46].

Third: Misdemeanors of Electronic Publication of Classified Information or Documents Impairing Public Order and Public Tranquility

Public order comprises various constituent elements such as public security, public morals [47], public health [48], public tranquility [49], in addition to the general economic and social order [50]. Consequently, this crime is founded upon the act of intentionally publishing or broadcasting classified electronic information or documents via electronic communications or an information system, resulting in the impairment of one or more elements constituting public order or public tranquility [51].

Fourth: The Misdemeanor of Failing to Produce Electronically Stored Classified Information and Documents

When necessary, the competent judicial authority investigating one of the crimes concerning assaults on administrative information and documents prescribed in Law No. 21-09 may request any person to produce information or data stored through the use of information and communication technologies. Accordingly, this crime is consummated merely by the refusal or abstention of the latter to surrender such electronically stored information or data to the investigating judicial authority [52].

Second Division: Penalties Prescribed for Crimes Impairing Administrative Information and Documents via the Internet

Having examined the various manifestations that crimes impairing administrative information and documents via the internet may assume, the Algerian legislature has sanctioned each type of crime with an appropriate penalty to achieve general and specific deterrence. This is addressed by dividing this division into two subsections: the first determines the principal penalties prescribed for these crimes, while the second addresses supplementary penalties applicable to this category of offenses.

Subsection 1: Principal Penalties

First: Penalty Prescribed for the Misdemeanor of Unlawful Electronic Access to Classified Information or Documents

An unauthorized perpetrator who commits unlawful electronic access to any information system, website, electronic network, or any other information and communication technology means belonging to the concerned authorities, aiming to obtain classified information or documents, is punished by imprisonment ranging from five (05) to ten (10) years, and a financial fine ranging from 500,000 DZD to 1,000,000 DZD [53].

Second: Penalty Prescribed for the Misdemeanor of Electronic Publication of Classified Administrative Information or Documents

The penalty prescribed for publishing classified information and documents obtained pursuant to the commission of the unlawful access misdemeanor is doubled, becoming imprisonment ranging from ten (10) to twenty (20) years, and a financial fine ranging from 1,000,000 DZD to 2,000,000 DZD [54]. This indicates that the Algerian legislature established an aggravated form of the unlawful access misdemeanor in the event that classified information or documents acquired through the crime are published. Furthermore, the legislature prescribed imprisonment from five (05) to ten (10) years, alongside a financial fine ranging from 500,000 DZD to 1,000,000 DZD, for anyone who establishes, manages, or supervises a website, electronic account, or software program utilized in publishing the whole or part of classified information and documents content. The same penalty applies to anyone publishing classified information or documents via an electronic network or using information and communication technologies [55].

Third: Penalty Prescribed for the Misdemeanor of Impairing Public Order and Public Tranquility Associated with the Electronic Publication of Classified Information or Documents

Anyone who impairs public order and public tranquility through the intentional publication or broadcasting of classified information or documents using electronic communications or an information system is subject to a custodial sentence ranging from ten (10) to fifteen (15) years of imprisonment, and a financial fine ranging from 1,000,000 DZD to 1,500,000 DZD [56].

Fourth: Penalty Prescribed for the Misdemeanor of Failing to Produce Electronically Stored Classified Information and Documents

The Algerian legislature prescribed imprisonment from three (03) to five (05) years, and a financial fine ranging from 300,000 DZD to 500,000 DZD, for anyone committing the misdemeanor of failing to surrender classified information and documents stored electronically via information and

communication technologies to the judicial authority investigating one of the offenses prescribed in Law No. 21-09 relating to the protection of administrative information and documents [57].

Fifth: Penalties Prescribed for Attempt and Incitement

The same penalty prescribed for the principal perpetrator in the aforementioned crimes applies to anyone who incites their commission or attempts to commit them—meaning without requiring the crime to take the form of a completed offense [58].

Subsection 2: Supplementary Penalties

In addition to principal penalties, the competent judicial authority may pronounce one or more supplementary penalties prescribed in the Algerian Penal Code. It may also sentence a public servant who has committed one of the aforementioned crimes to a permanent ban from exercising high public office, or for a duration ranging from a minimum of five (05) years to a maximum of ten (10) years. Despite the discretionary application of supplementary penalties in misdemeanor matters, the Algerian legislature mandatorily prescribed the application of supplementary penalties consisting of the confiscation of devices, programs, and means utilized in committing one or more of the studied crimes, alongside the closure of the website or electronic account utilized in the crime, or a ban on accessing it. It also pronounces the closure of the establishment or premises exploited in committing the crime, provided that the owner of such premises or establishment had knowledge of the crime being committed through it [59]. It is noteworthy that the application of these supplementary penalties must observe the rights of bona fide third parties [59].

Conclusion

In conclusion of this study concerning the subject of crimes targeting administrative operations via the internet, it can be stated that the transition towards administrative digitalization has become an inevitable necessity, yet it remains fraught with security and legal risks necessitating continuous legislative adaptation. Through the analysis of current Algerian legal texts, we find that the Algerian legislature demonstrated early awareness of the severity of cybercrime by adopting precise definitions of the electronic signature in Executive Decree No. 07-162 and Law No. 15-04, in addition to establishing rigorous technical conditions to ensure its security and association with the exclusive holder. It is also evident that crimes are no longer restricted to direct assault, but extend to misdemeanors involving the possession and disclosure of signature data, certification service providers' breaches of obligations and confidentiality, and breaches of secrecy by auditing officers. The Algerian legislature countered this with a rigorous criminal policy under Ordinance No. 21-09, imposing custodial sentences and aggravated financial fines to protect classified documents, with custodial sentences reaching up to 20 years in cases of intentional electronic publication of information derived from unlawful access, alongside mandatory supplementary penalties such as confiscation and website closure.

Footnotes

1. See Abdel-Fattah Bayoumi Hegazi, *Towards Formulating a General Theory in Criminology and the Cybercriminal*, op. cit., p. 71.
2. See Amir Farag Youssef, *Electronic Signature*, University Press House, Alexandria, Egypt, 2008, pp. 14, 17–18.
3. See Faisal Saeed Al-Gharib, *Electronic Signature and Its Evidentiary Value in Proof*, Publications of the Arab Organization for Administrative Development, Egypt, 2005, p. 216.
4. See Abdel-Fattah Bayoumi Hegazi, *Combating Computer and Internet Crimes in the Model Arab Law*, op. cit., p. 73.
5. See Article 03 of Executive Decree No. 07-162 of 13 Jumada Al-Ula 1428, corresponding to May 30, 2007, amending and supplementing Executive Decree No. 01-123 of 15 Safar 1422, corresponding to May 09, 2001, relating to the exploitation regime applicable to each type of

-
- network—including wireless electrical networks—and to various wire and wireless telecommunication services, Official Gazette No. 37, p. 13.
6. Electronic signature creation data means unique data such as codes and private cryptographic keys used by the signatory to create the electronic signature. See Article 03, Paragraph 03 of Law No. 15-04 of 11 Rabi Al-Thani 1436, corresponding to February 01, 2015, laying down general rules relating to electronic signature and electronic certification, Official Gazette No. 06, p. 07.
 7. See Article 03, Paragraphs 01, 02, 04, and 07 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 8. See Article 07 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 9. See Article 02, Paragraph 03 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 10. See Rachida Bouker, *Crimes of Assault on Automated Processing Systems in Algerian and Comparative Legislation*, op. cit., p. 286.
 11. See Essam Abdel-Fattah Matar, *E-Commerce in Arab and Foreign Legislations*, New University House, Alexandria, Egypt, 2009, p. 337.
 12. See Article 02, Paragraph 12 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 13. The economic authority for electronic certification refers to the authority tasked with regulating posts and electronic communications, responsible for monitoring and controlling electronic certification service providers offering signature and certification services to the public, in addition to assuming other missions. See Articles 29 and 30 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification, op. cit., pp. 10–11.
 14. See Section II of Chapter III of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 15. See Aziza Lerqet, "Criminal Protection of Electronic Signature and Certification in Algerian Legislation", *Al-Ijtihad Journal for Legal and Economic Studies*, Issue 11, University Center of Tamanrasset, Algeria, 2017, p. 124.
 16. See Article 02, Paragraph 10 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 17. See Article 42 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 18. See Article 10 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 19. See Article 43 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 20. See Aziza Lerqet, "Criminal Protection of Electronic Signature and Certification in Algerian Legislation", *same reference*, p. 122.
 21. See Article 02, Paragraph 16 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 22. See Section I of Chapter II of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 23. See Section II of Chapter II of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 24. A trusted third party refers to the legal entity that issues qualified electronic certification certificates, in addition to the possibility of providing other services related to electronic certification for stakeholders in the governmental sector. See Article 02, Paragraph 11 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 25. Electronic certification policy refers to the set of organizational and technical rules and procedures related to electronic signature and certification. See Article 02, Paragraph 15 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
 26. See Articles 29 and 30 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.

27. See Articles 51 and 52 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
28. See Article 68 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
29. See Article 67 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
30. See Article 72 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
31. See Article 70 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
32. See Article 71 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
33. See Article 73 of Law No. 15-04 laying down general rules relating to electronic signature and electronic certification.
34. See Article 04 of Law No. 06-03 of 19 Jumada Al-Thania 1427, corresponding to June 15, 2006, embodying the General Statute of the Public Service, Official Gazette No. 46, p. 04.
35. See Ahcene Belourna, *The Public Service in Algerian Legislation: Theory and Practice*, Dar Houma for Printing, Publishing and Distribution, Algeria, 2019, p. 67.
36. See Article 02, Paragraph (b) of Law No. 06-01 of 21 Muharram 1427, corresponding to February 20, 2006, relating to Preventing and Combating Corruption, Official Gazette No. 14, p. 05.
37. See Article 03, Paragraph 01 of Ordinance No. 21-09 of 27 Shawwal 1442, corresponding to June 08, 2021, relating to the Protection of Administrative Information and Documents, Official Gazette No. 45, p. 10.
38. See Hammouda Abbas Mahmoud, "The Scientific Concept of Documents and Documentation", *Annals of the Faculty of Humanities and Social Sciences*, Issue 01, University of Qatar, p. 221.
39. See Abdelhalim Ben Mechri, *Administrative Drafting: Theoretical Introduction and Practical Models*, 1st ed., Al-Rimal Press, El Oued, Algeria, 2019, p. 86.
40. See Ahmed Ali, "The Concept of Information and Knowledge Management", *Damascus University Journal*, Vol. 28, Issue 01, 2012, p. 478.
41. Appointed authority refers to all legislative, judicial, and executive state institutions and bodies, public administrations, local authorities, every institution in which the State owns all or part of the capital, and every institution providing a public service. See Article 02 of Law No. 21-09 relating to the Protection of Administrative Information and Documents, op. cit., p. 10.
42. See Article 03, Paragraphs 02, 03, and 04 of Law No. 21-09 relating to the Protection of Administrative Information and Documents, op. cit., p. 10.
43. See Amal Habat, "The Evidentiary Value of the Electronic Document in Algerian Legislation", *Critical Journal of Law and Political Sciences*, Faculty of Law and Political Sciences, Mouloud Mammeri University - Tizi Ouzou, Algeria, pp. 136–137.
44. See Article 37 and Article 03 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
45. See Ahmed Mesbah Al-Ketbi, "Criminal Liability Arising from the Disclosure of Professional Secrecy", *University of Sharjah Journal for Legal Sciences*, Vol. 16, Issue 02, 2019, p. 318.
46. See Article 37, Paragraph 02 and Article 38 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
47. Public security means everything that reassures a person regarding their wealth and self by preventing the occurrence or probability of accidents that could inflict harm upon persons and property. See Sami Gamal El-Din, *Principles of Administrative Law*, Toubji Commercial Presses, 1994, p. 156.
48. Public health refers to protecting citizens from hazards threatening their health life from epidemics and communicable diseases, and preserving public health contributes to maintaining public security without breaching it. See Hosni Darwish Abdel-Hamid, "Administrative Police in Contemporary Positive Systems and Islamic Sharia", *Al-Mohama Journal*, Issue 02, Cairo, 1985, p. 142.

49. Public tranquility means the prevention of manifestations of disturbance and annoyances exceeding ordinary social life molestations. See Mahmoud Atef El-Bana, "Limits of Administrative Police Authority", *Journal of Law and Economics*, Issue 04, Cairo University Press, 1980, p. 358.
50. Examples of general economic order include the protection afforded to the citizen's purchasing power, intervention in curbing unemployment, price protection, and continuous supply of consumer goods. As for the protection of general social order, prominent examples include protections granted to vulnerable social segments such as child or maternal protection. See Bachir Belaid, *Summary Proceedings in Administrative Matters*, Amar Ghorfi Presses, Batna, Algeria, 1988, p. 85.
51. See Article 39 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
52. See Article 24 and Article 40 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
53. See Article 37 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
54. See Article 37, Paragraph 02 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
55. See Article 38 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
56. See Article 39 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
57. See Article 40 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
58. See Article 46 and Article 47 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.
59. See Article 44 and Article 45 of Law No. 21-09 relating to the Protection of Administrative Information and Documents.

Sources and References

First: Sources

- **Laws:**

1. Law No. 06-01 dated 21 Muharram 1427 corresponding to February 20, 2006, relating to Preventing and Combating Corruption, Official Gazette No. 14.
2. Law No. 06-03 dated 19 Jumada Al-Thania 1427 corresponding to June 15, 2006, embodying the General Statute of the Public Service, Official Gazette No. 46.
3. Law No. 15-04 dated 11 Rabi Al-Thani 1436 corresponding to February 01, 2015, laying down general rules relating to electronic signature and electronic certification, Official Gazette No. 06.

- **Decrees:**

1. Executive Decree No. 07-162 dated 13 Jumada Al-Ula 1428 corresponding to May 30, 2007, amending and supplementing Executive Decree No. 01-123 dated 15 Safar 1422 corresponding to May 09, 2001, relating to the exploitation regime applicable to each type of network—including wireless electrical networks—and to various wire and wireless telecommunication services, Official Gazette No. 37.

- **Ordinances:**

1. Ordinance No. 21-09 dated 27 Shawwal 1442 corresponding to June 08, 2021, relating to the protection of administrative information and documents, Official Gazette No. 45.

Second: References

• Books:

1. Amir Farag Youssef, *The Electronic Signature*, University Press House, Alexandria, Egypt, 2008.
2. Bachir Belaid, *Summary Proceedings in Administrative Matters*, Amar Ghorfi Presses, Batna, Algeria, 1988.
3. Belourna Ahcene, *The Public Service in Algerian Legislation: Theory and Practice*, Dar Houma for Printing, Publishing and Distribution, Algeria, 2019.
4. Ben Mechri Abdelhalim, *Administrative Drafting: Theoretical Introduction and Practical Models*, 1st ed., Al-Rimal Press, El Oued, Algeria, 2019.
5. Rachida Bouker, *Crimes of Assault on Automated Processing Systems in Algerian and Comparative Legislation*, Sbihi Juridical Publications, Beirut, Lebanon, 2012.
6. Sami Gamal El-Din, *Principles of Administrative Law*, Toubji Commercial Presses, 1994.
7. Abdel-Fattah Bayoumi Hegazi, *Combating Computer and Internet Crimes in the Model Arab Law*, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 2009.
8. Abdel-Fattah Bayoumi Hegazi, *Towards Formulating a General Theory in Criminology and the Cybercriminal*, Monshaat Al-Maaref, Alexandria, Egypt, 2009.
9. Essam Abdel-Fattah Matar, *E-Commerce in Arab and Foreign Legislations*, New University House, Alexandria, Arab Republic of Egypt, 2009.
10. Faisal Saeed Al-Gharib, *The Electronic Signature and its Evidentiary Value in Permanence*, Publications of the Arab Organization for Administrative Development, Egypt, 2005.
11. Mahmoud Atef El-Bana, *Limits of Administrative Police Authority*, Journal of Law and Economics, Issue 04, Cairo University Press, 1980.

• Scientific Articles:

1. Ahmed Ali, "The Concept of Information and Knowledge Management", *Damascus University Journal*, Syria, Vol. 28, Issue 1, 2012.
2. Ahmed Mesbah Al-Ketbi, "Criminal Liability Arising from the Disclosure of Professional Secrecy", *University of Sharjah Journal for Legal Sciences*, Vol. 16, Issue 2, 2019.
3. Habat Amal, "The Evidentiary Value of the Electronic Document in Algerian Legislation", *Critical Journal of Law and Political Sciences*, Faculty of Law and Political Sciences, Mouloud Mammeri University - Tizi Ouzou, Algeria, Issue 2, 2012.
4. Hosni Darwish Abdel-Hamid, "Administrative Police in Contemporary Positive Systems and Islamic Sharia", *Al-Mohama Journal*, Issue 2, Cairo, 1985.
5. Hammouda Abbas Mahmoud, "The Scientific Concept of Documents and Documentation", *Annals of the Faculty of Humanities and Social Sciences*, University of Qatar, Issue 1, 1979.
6. Aziza Lerqet, "Criminal Protection of Electronic Signature and Certification in Algerian Legislation", *Al-Ijtihad Journal for Legal and Economic Studies*, University Center of Tamanrasset, Issue 11, 2017.