Science, Education and Innovations in the Context of Modern Problems
Issue 11, Vol. 8, 2025

TITLE OF THE RESEARCH ARTICLE

The Legislative Equilibrium between Criminal Prosecution and the Right to Privacy under Algerian Law No. 18-07: A Legal and Technological Perspective

Gaffaf Fatma
Dr.
University Center Si Al-Hawas Barika
Algeria
E-mail: fatma.gaffaf@cu-barika.dz
ORCID: 0000-0001-9109-9402

Oumaima Boumehdaf
Doctor
University of Echahid Hamma Lakhdar – El Oued
Algeria
E-mail: oumaiama.boumehdaf@univ-elued.dz
ORCID: 0009-0000-1651-1268

Issue web link https://imcra-az.org/archive/385-science-education-and-innovations-in-the-context-of-modern-problems-issue-11-vol-8-2025.html

Keywords Right to Privacy; Criminal Prosecution; Algerian Law 18-07; Personal Data Protection; Cybercrime; Digital Rights

Abstract

This study explores the legal equilibrium established by Algerian Law No. 18-07 between the protection of the right to privacy and the necessity of criminal prosecution in the digital age. The legislation reflects a national effort to align domestic legal frameworks with international standards on data protection, individual freedoms, and cybersecurity. The research highlights the tension between the individual's right to confidentiality and the state's obligation to prevent and punish cybercrime, noting that technological development has reshaped the nature of both privacy violations and criminal investigations. Law 18-07 provides a comprehensive framework addressing the misuse of personal information, unlawful data disclosure, and the balance required to preserve justice while upholding fundamental human rights. The study concludes that the Algerian legislative system, while progressive, still faces interpretative and procedural challenges in applying privacy safeguards in criminal contexts, especially regarding data surveillance and electronic evidence gathering.

Citation. Gaffaf F; Oumaima B. (2025). The Legislative Equilibrium between Criminal Prosecution and the Right to Privacy under Algerian Law No. 18-07: A Legal and Technological Perspective. *Science, Education and Innovations in the Context of Modern Problems*, 8(11), 1339–1349. https://doi.org/10.56334/sei/8.11.10

Received: 21.04.2025 | Accepted: 15.09.2025 | Publishing time: 01.11.2025

Introduction:

The right to privacy is protected by a variety of laws, which means that people have the right to live their lives free from intrusion. discussions of their beliefs or culture, intrusions upon their family and personal privacy, or even threats to their physical and mental well-being, or assaults on their honor and reputation, the disclosure of

some humiliating but minor events in their private lives, the use of their personal information, or keeping an eye on all of their privacy and monitoring all of their correspondence through various media, regardless of whether it was sent or received. As it is a fundamental component of the human right to privacy, this is regarded as one of the most crucial pieces of data that must be protected. The major question raised by this research is: How much does Law really apply? Is 18-07 really effective at protecting private information?
To answer this question, we divide the study into two main sections as follows:
First section: Substantive rules for the protection of personal data.
Second section: Procedural rules established for crimes affecting personal data.

1/The Substantive Rules for the Protection of Personal Data

The right to privacy is closely linked to individual freedom, and there was a need for legal guarantees to protect it from various violations affecting one's private life and personal information. Therefore, most legislations hastened to define personal data in a way that ensures protection of this privacy from any infringement. In this axis, we will explore the concept of personal data and the procedural controls for its protection.

1/1/ TheConcept of Personal Data:

1/1/1/ TheJurisprudential Definition: Jurisprudence defined personal data as the data related to a person addressed by it, such as their name (Khalifa, 2007), which is considered one of the rights inherent to the human personality and constitutes it, as well as their social status, residence, and their criminal record (Haida, 2016, 2017).

In another definition, it is data related to a specific person and it is not necessary that it relates to the private life of individuals; it is sufficient that it concerns their professional life, or even their public life, or their known political or union affiliations (Khalifa, 2007).

It can be said that jurisprudence considers personal data not only as that which addresses the person, but includes everything related to the person's professional life, public life, political and union activities, which is the prevailing definition.

1/1/2/Legislative Definition of Personal Data

A/ Definition of international conventions on personal data:

-Definition of Personal Data in European Convention No. 108: The European Convention No. 108 issued by the Council of Europe defined personal data in Article 2, paragraph (a), which stated that "personal data means any information relating to an identified or identifiable natural person."

Definition of personal data in European Directive 46-95: Article 2(f) of European Directive No. 95-46 issued on October 24, 1995, defined "personal data" as any information relating to an identified or identifiable natural person, who can be identified directly or indirectly, particularly by reference to an identification number or to one or more factors specific to their physical, physiological, psychological, economic, cultural, or social identity.

Meanwhile, Article 02 of the European Directive on Electronic Signatures issued on December 13, 1999, referred to personal data and defined it as "any information relating to an identified or identifiable person." (Yahi, 2019)

Definition of personal data in the OECD Guidelines: The first version of the guidelines issued by the Organisation for Economic Co-operation and Development in 1980 defined personal data as follows: "Personal data means any information relating to an identified or identifiable natural person."

Accordingly, it is data that conveys information that can be linked to a specific person to determine their identity. This definition raised some issues as it excluded some data that could lead to identifying a person, such as means used by the person like a fixed or mobile phone number, vehicle registration number, or any information linked to any other means they carry, which facilitates violating individuals' privacy without deterrence, by processing data away from oversight bodies due to the impossibility of applying the legal text that indirectly excludes them. (Jbour and Haidar, 2018)

Definition of personal data in the General Data Protection Regulation in EU countries: Article 4 of the GDPR, concerning users in EU countries, defined personal data as information related to an identified or identifiable person, directly or indirectly, particularly by reference to an identifier such as a name, social security number, location data, online identifier (IP address or email address), or one or more factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity. (Technical Portal, 2021)

B/ Definition of national legislation on personal data:

The Algerian legislator, through Law 18-07, addressed several definitions including that in Article 03, paragraph 01 regarding personal data, as any information, regardless of its support, related to an identified or identifiable person as indicated below, the person concerned directly or indirectly, particularly by reference to an identification number or one or more elements specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity. (Law on the Protection of Natural Persons, 18/7/2018)

It is noted here that the text of the article refers to two characteristics: first, that personal data relate to a natural person and not a legal person. (Kardlas, 2021)

Although a legal person, like a natural person, has data and its own economic and commercial life, it should not be disclosed outside the confidentiality circle defined by that person. (Diab, 2013)

The second characteristic that can be deduced from this definition is that this data can be used to identify the person related to it.(Kardlas, 2021)This means that we should not skimp on data that directly indicate a person's identity, such as his name, surname, and nationality. Rather, we should take into consideration every means that makes him identifiable and contributes to determining his identity.(Jabour and Haider 2018)This is what was confirmed by European Convention No.108 in its definition of personal data as "any information relating to the identification of an individual, or a specific individual."(Mubarakiya, 2019)It is a brief, general definition that includes all information that identifies a person without mentioning this information.

1/2/ The Procedural Controls for the Protection of Personal Data:

The Algerian legislator has imposed many procedural aspects that must be observed, not only in the penal aspect but also what the data controller must adhere to, who plays a central role in the method of processing, and the necessity to consider many details covered by Law 18-07.

For personal data to be legally protected, the Algerian legislator pointed to a set of measures that must be observed by the data controller, which can be clarified as follows:

1/2/1/ Confidentiality:

Commitment to confidentiality in this field means determining who has the right and extent of sharing information and accessing it by others, as the data controller does not allow access to the information except to those concerned with the processing (Samet, 2020), as indicated in Article 39 of Law No. 18-07 related to the protection of natural persons in the field of processing personal data. (Law No. 18-07)

1/2/2/Commitment to Legitimacy and Integrity:

This means the data controller's commitment to act with legitimacy and integrity, as referred to by the legislator within the scope of Law 18-07 through Article 9, especially paragraph (a), which states: processing in a lawful

and fair manner, which also reflects the international dimension through the United Nations' concern with the issue of integrity and legitimacy according to Resolution 95-45 that includes guidelines for organizing files and data prepared by electronic computers. (Hamlel, 2020)

1/2/3/ Prior declaration with the competent authority:

In accordance with the provisions of Article 12 of Law 18-07, which states: «Unless otherwise provided by legal text, every operation involving the processing of personal data is subject to prior declaration with the national authority or authorization from it in accordance with the provisions stipulated in this law (Law No. 18-07)?" It is worth noting here the necessity of carrying out preliminary procedures before starting work within the scope of personal data processing, which entails the requirement to submit a declaration to the competent authority.

According to Article 13 of Law 18-07, the prior declaration including the commitment to carry out the processing must be submitted electronically to the competent national authority.

A receipt of submission is issued immediately or within 48 hours or via email, and after receiving the receipt, the data controller may, under their responsibility, commence the work required by their duties within the framework of the law.

2/Procedural rules established for crimes affecting personal data.

The right to privacy is universally recognized as intrinsic to both the individual and the community at large. Without a doubt, everyone has things in their life that are private and personal, that they value and would rather not share with others. Similarly, society as a whole also has its privacy, which it works to shield from other societies since it safeguards its security. security and the security of its members.

Maintaining a person's secrets and keeping them hidden from others is a basic principle to guarantee the right to privacy is protected from intrusion and violation by others. others. The following are the most significant types of these offenses:

2/1/ Instances of offenses involving personal data:

The particular clauses of Law 18-07, which includes the protection of natural persons in the processing of personal data, govern crimes involving the breach of personal data.

Crimes related to violating prior procedural rules for processing:

The processing of personal data cannot be carried out except after fulfilling certain preliminary conditions stipulated by Law 18-07.

Crimes of failing to meet preliminary conditions:

These occur when violating the provisions of Articles 7, 12, and 37 of Law 18-07. Article 7 mandates obtaining explicit consent from the concerned person to process their personal data, and Article 36 of the same law grants the right to object to this whenever legitimate reasons exist.

Article 12 of the same law also requires that every personal data processing operation be subject to a declaration or authorization procedure by the National Authority for the Protection of Personal Data, unless there is a legal provision exempting a particular processing operation from this. The commission of this crime requires the presence of certain elements, which are:

The material element consists of the automated processing of data without adhering to legally prescribed procedures, even if no criminal result ensues, as the crime is considered behavioral and does not require achieving a specific result (Shanin, 2018).

The crime has a moral element that can take the form of intent, which is established by the presence of general criminal intent, with the perpetrator being aware of the nominal or personal nature of the data or also knowing that the automated processing of the data was conducted without observing legally prescribed procedures (Awda, 2017).

Crimes of unlawful collection of personal data and the crime of deviation from purpose:

This type of crime occurs in the early stages of processing, encompassing various forms that violate the provisions related to the collection of personal data. The legislator included them in the legal texts, considering it a crime to collect any personal data by fraudulent, dishonest, or unlawful means, as well as any collection of personal data related to the criminal status of the concerned person. These are all crimes occurring at the beginning of processing, where the perpetrator unlawfully collects personal data.

The crime of using unlawful methods in collecting personal data:

Article 59 of Law 18-07 states: "Anyone who collects personal data by fraudulent, dishonest, or unlawful means shall be punished by imprisonment from one to three years and a fine ranging from 100,000 DZD to 3,000,000 DZD" (Law 18-07).

This crime occurs in the early stages of processing, where the perpetrator is able to obtain data about one or several individuals through the process of collecting and comprehensively gathering data in advance and organizing it for later use. This can be done either manually, by collecting it in files or paper records, or through electronic means, such as digital files. The data may also be collected from existing paper documents or through direct questioning in the form of a survey of the concerned person or by providing a questionnaire to be answered in writing. It can also be obtained from a survey of others, as if this other person is responsible for the concerned individual. (Ezzedine, 2018)

It is worth noting here that the law requires the use of unlawful, dishonest, and deceptive methods for the crime of unlawful collection of personal data to occur, which is the criminal behavior that must be present for the crime to take place. Among these methods are monitoring, intercepting, capturing, and extracting messages exchanged via email, secretly connecting wires to the computer storing the data to be seized, as well as capturing vibrations caused by sounds in the concrete walls of rooms and translating and processing them by a computer equipped with special software to convert them into words and phrases. (Al-Momani, 2010)

The French Court of Cassation considered in a criminal chamber decision dated November 3, 1987, that it is not sufficient for this crime to occur merely by collecting data in a deceptive, dishonest, or unlawful manner; it is also necessary that this data be recorded or stored in a file, whether automated or manual. In a recent decision by the same court dated March 14, 2006, the dishonest collection of personal data was considered established in:

- Any access to electronic addresses and their use, even without recording them in a file, for the purpose of sending electronic messages to the owners of these addresses.

- Any collection of personal electronic addresses of natural persons without their knowledge in the public space of the internet.

It is worth noting here that the crime of unlawful collection of personal data is a misdemeanor that only occurs if committed intentionally by the offender (an intentional crime), meaning the offender is aware of the illegality of the act they committed and wills to perform it. (Manar, 2016)

Crimes of deviation from the purpose:

This crime occurs with the presence of both the material and moral elements.

The Material element is fulfilled by the occurrence of the physical activity that constitutes deviation from the purpose or objective of the automated processing of personal data. The purpose or objective of the automated processing refers to the goal sought by the processor of the automated processing, which is the sole justification for processing electronic personal data. This crime presupposes the lawful acquisition of data, and the material activity constituting the material element of the crime is considered fulfilled if the offender exploits the personal data to disclose the sources of wealth of the data subject, or to know their financial status or matters related to their private life. (Awda, 2017)

As for the persons responsible for this crime, the legislator referred to anyone who carried out or used the processing, meaning all persons in possession of the data, i.e., those who participated in all stages of processing from collection to organization until those concerned receive the processing. (Qaid, 1994)

Here, it can be said that determining whether the perpetrator's act constitutes a deviation from the purpose of processing lies in referring back to the prior request, which specifies the purpose or objective of the automated processing of personal data, regardless of whether the person possesses this information for classification, transfer, or any other purposes.

In the crime of changing the purpose of automated processing of personal data, the form of criminal intent is general intent, which consists of knowledge and will. The perpetrator must know that their act is likely to constitute a deviation from the purpose of automated processing of personal data, and their will must be directed toward committing this crime or its objective, whether it is for the benefit of the perpetrator, to prevent harm to themselves, or to realize the interest of others.

Crimes Related to the Work of the National Authority:

Article 61 of Law 07-18 states the following: "Anyone who obstructs the work of the National Authority shall be punished by imprisonment from six months to two years and a fine of 200,000 DZD to 600,000 DZD, or by one of these penalties only, in the following cases:

- By objecting to the procedure of on-site verification.

- By refusing to provide its members or agents placed at its disposal with the necessary information and documents to carry out the mission entrusted to them by the National Authority, or by hiding or removing the aforementioned documents or information.

- By sending information that does not match the content of the recordings at the time of submitting the request or by not submitting it directly and clearly." (Law No. 07-18)

It is noted here that the crime of obstructing the work of the national authority is established whenever the national authority is obstructed by being prevented from performing its tasks or by refusing to cooperate with it, and this is done intentionally. The obstruction targets a set of monitoring tasks assigned to the national authority based on the provisions of Article 49 of Law 18-07, which grants it the right to carry out all necessary investigations and inspections to follow up on crimes and collect their traces and related evidence (conducting verification on site), as well as the authority to order the provision of necessary documents.

The criminal behavior in this crime includes the following:

- Obstructing the national authority from performing its monitoring tasks such as conducting the verification process.

- Refusing to receive inspectors and not allowing them to carry out their mandate.

- Refusing to send documents or information, which may take the form of sending incomplete documents or sending them after the specified deadlines (this refusal may be clear and direct). (Tabash, 2017)

It is evident from Article 61 of Law 18-07 that this crime is only established through intent, as shown by the nature of the punishable acts, which cannot be committed by mistake. Therefore, once general criminal intent is present, the crime occurs and is punishable.

Crimes related to the person responsible for the automated processing of personal data:

The Algerian legislator, similar to comparative legislations, has established a set of obligations for the person responsible for processing. Once these are violated, criminal liability arises, and several crimes punishable by law are created. Some of these relate to guaranteeing the rights of the data subjects, while others relate to ensuring the confidentiality and integrity of the processed personal data.

Article 64 of Law 07-18 shows us that the crime of violating the rights of the data subject is established as soon as the data controller refuses the rights of information, access, correction, or objection without a legitimate reason.

As for the case where the data controller refuses to grant the data subject the rights granted to them by the legislator in order to exercise a form of control over their personal data subject to processing, the refusal can be expressed in any form, whether verbally or in writing, implicitly or explicitly. The law does not criminalize refusal absolutely; rather, it follows the phrase "without legitimate reason."

Therefore, in the concept of the violation, there are cases that justify refusal to recognize those rights, such as when the data subject's request is abusive in the manner stipulated by Article 34 of the same law.

This crime is considered intentional, meaning that the data controller deliberately commits the offense despite knowing the illegitimacy of their act and directs their non-coerced will to commit it. Hence, the Algerian legislator considered it a misdemeanor punishable by imprisonment and a fine or by either of these two penalties only. Meanwhile, the Algerian legislator criminalized the breach of confidentiality and the integrity of processing by requiring the adoption of technical or organizational measures to prevent unauthorized access or loss of data.

Therefore, this crime assumes that the processing has been completed and thus requires the preservation and protection of the data from assault or destruction. In addition to the data controller not processing the data themselves, they must be keen to choose a subcontractor who provides sufficient guarantees to take appropriate measures to ensure the confidentiality of the processing.

These crimes are considered intentional crimes, where the perpetrator deliberately refuses one of the rights of knowledge and will, and this refusal is not supported by any legitimate reason. The perpetrator is also aware

of their lack of caution in choosing appropriate measures to protect the data, regardless of whether the damage to the data or to another person occurred accidentally, intentionally, or through negligence. (Tabash, 2017)

It is worth noting that Algerian legislation has referred to certain acts that it has criminalized, such as retaining data beyond the specified period, allowing unauthorized persons to access personal data, and transmitting it to unauthorized persons, which are the responsibility of the data controller. (Law No. 18-07)

2/2/ The Penalties prescribed for crimes affecting personal data.

In this section, we will address the penalties applied to each crime related to data as follows:

Penalty prescribed for crimes of failing to meet the preconditions:

The Algerian legislator penalized the crime of failing to meet the preconditions for processing in Articles 55 to 57, where Article 55 states: "Anyone who processes personal data in violation of the provisions of Article 07 of this law (Law No. 18-07) shall be punished by imprisonment from one to three years and a fine from 100,000 DZD to 300,000 DZD."

The same penalty applies to anyone who processes personal data despite the objection of the concerned person when this processing targets, in particular, commercial advertising or when the objection is based on legitimate reasons, as also stated in Article 56: "Anyone who carries out or orders the processing of personal data without respecting the conditions stipulated in Article 12 of this law shall be punished by imprisonment from two to five years and a fine from 200,000 DZD to 500,000 DZD. (Law No. 18-07)."

The same penalties apply to anyone who makes false declarations or continues data processing activities despite the withdrawal of the declaration receipt or the authorization granted to them." Referring to Article 57: "Anyone who processes sensitive data without the explicit consent of the concerned person, except in cases provided for in this law, shall be punished by imprisonment from two to five years and a fine from 200,000 DZD to 500,000 DZD."

Penalty prescribed for crimes of deviation from the purpose:

The perpetrator of the crime of deviation from the purpose, as stated in Article 58 of Law 18-07, is punished as follows: "Anyone who performs or uses data processing for purposes other than those declared or authorized shall be punished by imprisonment from six months to one year and a fine ranging from 600 DZD to 100,000 DZD, or by either of these two penalties only." (Law No. 18-07).

It is noted here that the legislator has been lenient in the penalty for this crime compared to other crimes, as discretionary power is given to the judge to impose either a fine or imprisonment.

Penalty prescribed for crimes related to the work of the national authority:

According to Article 61 of Law No. 18-07, it is clear that this crime is only established through intent, as evidenced by the nature of the punishable acts which cannot be committed by mistake. Therefore, once general criminal intent is present, the crime is established, and the offender is punished with a fine in addition to a custodial sentence (imprisonment) on the basis that it is a misdemeanor.

***Penalty prescribed for crimes related to the person responsible for the automated processing of personal data*:**

The Algerian legislator addressed the criminalization of such behaviors in Articles 61, which states: "Anyone who obstructs the work of the national authority shall be punished by imprisonment from six months to two years and a fine ranging from 6,000 DZD to 200,000 DZD, or by either of these two penalties only." ... (Law No. 18-07).

As for Article 64 of the same law, it states: "Anyone responsible who refuses, without legitimate reason, the rights of information, access, correction, or objection stipulated in Articles 32, 34, 35, and 36 of this law shall be punished by imprisonment from two months to two years and a fine ranging from 200 DZD to 200,000 DZD, or by either of these two penalties only. (Asadov, K. 2025) "

Article 65 of the same law states: "Without prejudice to the harsher penalties provided for in the applicable legislation, the data controller who violates the obligations stipulated in Articles 38 and 39 of this law shall be punished with a fine ranging from 200,000 DZD to 500,000 DZD."...

It is worth noting that the other provisions related to punishment apply to all offenses stipulated in Law 18-07, where the maximum penalties are reached in the case of transferring personal data to a foreign country in violation of the law according to Article 67, or for anyone who retains personal data concerning crimes, convictions, or security measures according to Article 68 (Law No. 18-07).

As for the legal entity responsible for the offenses stipulated in this law according to Article 70, Article 71 allows for the application of supplementary penalties provided for in the Penal Code, in addition to the possibility of ordering the deletion of part or all of the personal data and the confiscation of the crime scene, its reallocation, or destruction according to Article 72. Article 73 penalizes the attempt to commit the aforementioned misdemeanors with the penalty of the completed crime, and in the case of recurrence, the penalty is doubled according to Article 74.

Conclusion:

Given the aforementioned context, it is evident that offenses impacting personal information have emerged as a significant concern with extensive ramifications on a global and domestic scale. The existing legal framework in Algeria distinctly underscores the necessity of safeguarding individual privacy and upholding the confidentiality of their personal data. These statutes are designed to shield personal data and the broader community from illicit exploitation or infringement. The Algerian legislature has instituted substantial penalties to address offenses compromising personal information, encompassing punitive measures such as monetary levies and custodial sentences for offenders. Law No. 18-07 exemplifies the Algerian legislature's dedication to upholding the privacy of individuals' personal details and fostering confidence in the utilization of technology and digital communication. This is accomplished by criminalizing actions that undermine the integrity or confidentiality of such information and imposing differentiated sanctions on responsible parties. Furthermore, an autonomous body has been established with the responsibility of overseeing the execution and efficacy of these protections through its endowed powers and authority. Consequently, the primary proposals can be concisely articulated as follows:

1. Legislation pertaining to the protection of personal data should be updated frequently in order to stay current with technological advancements and the emergence of new risks.

2. Legislation must be unambiguous, all-encompassing, and able to deal with contemporary issues like big data analysis and artificial intelligence technology.

3. In order to stay ahead of the numerous dangers and damages that could jeopardize the security of personal data, the modernization of state equipment with contemporary technology must be expedited.

4. Police must have improved operational electronic skills in order to identify breaches and attacks aimed at personal data.

5. In order for judges to better comprehend the informational aspect of the text, they should be properly trained by having some words explained, since this helps them understand the text's applicability and accomplish the law's goals.

6. Enhance IT infrastructure, keep software up to date, and provide staff with the necessary training.

7. Strengthen international collaboration in the area of personal data protection, including the exchange of information and the signing of agreements with other nations to address cybercrime and share pertinent data.

8. Improve monitoring of organizations and institutions that process personal data, regardless of whether they are public or private.

9. Increase public understanding of the importance of safeguarding personal data and related rights by conducting awareness campaigns and citizen education. possible dangers, threats, and precautions.

Ethical Considerations

This study complies with international ethical research standards and involves no human or institutional data collection. All legal and analytical materials used are publicly available. The research focuses solely on legislative interpretation and theoretical analysis, without any personal or confidential information processing.

Methodology

The research adopts a qualitative legal-analytical approach that combines doctrinal interpretation with comparative analysis. Primary sources include Algerian Law No. 18-07, related legislative texts, and judicial precedents. Secondary sources encompass scholarly articles and international conventions on data protection and cyber law. This methodology enables a comprehensive understanding of how Algerian legal frameworks reconcile individual privacy with public interest in criminal prosecution.

Author Contributions

Gaffaf Fatma: Conceptualization, legal framework analysis, and interpretation of Law No. 18-07.
Oumaima Boumehdaf: Comparative legal research, literature review, and manuscript refinement.

Both authors reviewed and approved the final version of the manuscript.

Funding

The authors declare that they received no specific funding for this study.

Acknowledgement

The authors would like to express their gratitude to the faculties of law at University Center Si Al-Hawas Barika and University of Echahid Hamma Lakhdar – El Oued for their continuous academic support and encouragement throughout this research.

Conflict of Interest

The authors declare that there is no conflict of interest related to this research.

Bibliography

1. Algeria. (2018, July 10). Law No 18-07 concerning the protection of natural persons in the processing of personal data (Official Bulletin, Issue No. 34).
2. Osama, Q. A. (1994). Criminal protection of private life and information banks: A comparative study (3rd ed.). Cairo, Egypt: Dar Al Nahda Al Arabia.
3. Muhammad, K. (2007). Criminal protection of computer data in Algerian and comparative law. Egypt: Dar Al Jame'a Al Jadida.
4. Al-Ashqar, M., & Haidar, M. (2018). Personal data and Arab laws: Security concerns and individual rights (1st ed.). Beirut, Lebanon: Arab Center for Legal and Judicial Research & League of Arab States.

5. Al-Momani, A. Q. (2010). Cyber crimes (2nd ed.). Jordan: Dar Al Thaqafa for Publishing and Distribution.
6. Toumi, Y. (2019). Legal protection of personal data in light of Law No 07-18: An analytical study. Al Ustadh Al Baheth Journal for Legal and Political Studies, 40(02).
7. Jawhar, S. Q. (2020). Legal controls for electronic processing of personal data. Journal of Comparative Legal Studies, 6(02).
8. Hammadi, K. (2021). Protection of personal data. Electronic Law Journal. Retrieved September 15, 2021, from https://ganonak.blogspot.com
9. Ezzedine, T. (n.d.). Criminal protection of personal data in Algerian legislation: A study in light of Law 18-07 concerning the protection of natural persons in the processing of personal data. Academic Journal of Legal Research, (02).
10. Aidani, M., & Rizk, Y. (2018). The protection of personal data in Algeria in light of Law No 18-07. Ma'alam Journal of Legal and Political Studies, 5, 127-140.
11. Alawi, A., & Ben Zitah, A. (2022). The independent administrative authority for the protection of personal data: A study in French and Algerian law. Algerian Journal of Legal and Political Sciences, 125-144.
12. Asadov K. (2025). Socio-Political Transformations and Ethno-Historical Dynamics in Zangazur during the Second Half of the 19th and Early 20th Century (until 1918): Ethno-Political Identity, Historical Geography, and Imperial Strategies in a Contested Borderland of Azerbaijan. Science, Education and Innovations in the Context of Modern Problems, 8(9), 1345–1358. https://doi.org/10.56334/sei/8.9.10
13. Nem Ghazal, N. (2019). The protection of natural persons in the field of personal data. Algerian Journal of Legal and Political Sciences, 125-142.
14. Bouke, M. A., Abdullah, A., Alshatebi, S. H., El Atigh, H., & Cengiz, K. (2023). African Union Convention on Cyber Security and Personal Data Protection: Challenges and future directions. ArXiv. https://doi.org/10.48550/arXiv.2307.01966
15. Law Gratis. (n.d.). Privacy law in Algeria. Retrieved from https://www.lawgratis.com/blog-detail/privacy-law-at-algeria
16. Signzy. (n.d.). Law 18-07 personal data protection. Retrieved from https://www.signzy.com/regulation-glossary/law-18-07-personal-data
17. Hogan Lovells. (2022). Recent developments in African data protection laws: Outlook for 2023. Retrieved from https://www.hoganlovells.com/en/publications/recent-developments-in-african-data-protection-laws-outlook-for-2023