Volume: 9 Issue: 2 Month: 6, Year: 2026
P.P 362 - 380
مجلـة البحوث القانونية والاقتصادية
JOURNAL OF LEGAL AND ECONOMIC RESEARCH

THE ROLE OF E-GOVERNMENT IN PROTECTING INDIVIDUALS' PERSONAL DATA

Maamar BENALI*
University of Blida2 Lounici Ali- Algeria
m.benali@univ-blida2.dz
Law and PropertyLaboratory

Send Article Date: 10-03-2026	Date of acceptance of the article: 08-05-2026

Abstract:

E-government is concerned to bring administration closer to citizens, wherever they are. Therefore, some countries have enacted laws related to these procedures in order to enable their citizens to obtain documents online. However, the sovereignty of these countries may be compromised through this space, putting individuals' privacy at risk of cyber violation. Due to the importance of the issue, countries have developed legislative policies related to cybersecurity. Therefore, the competent international and national authorities have intervened to track violators of individuals' privacy in order to prevent and deter them, and this is done through technical and legal mechanisms, whether internationally or nationally.

Keywords: E-government, Cybersecurity, Personal Details, prevention and protection procedures.

Introduction:

The government is at the heart of how a state is run. It forms a central pillar of the institutional system, and its role is reflected in the work it carries out. As the body that exercises sovereignty over the country's territory, it represents the state's political authority. People rely on it to manage their civil, administrative and financial affairs, as well as matters beyond the nation's borders. In that sense, the government acts as the key link through which citizens' concerns, both at home and abroad, are addressed.

In recent years, rapid technological developments have emerged that have affected many areas of life. Information and communication technologies, in particular, have taken centre stage, givingrise to a

* Maamar BENALI.

new face of government institutions. Citizens and public bodies, across their various sectors, have been connected through a distinctive electronic framework known in modern terminology as E-government. whichis the other side of traditional government, itperforms the same functions but operates within a digital environment and information systems. It ischaracterised by the electronic exchange of documents and the completion of transactions online, rather than the paper-heavy procedures, routine processes and bureaucratic complexities typical of traditional administration. This wide-ranging digital project has become a key pillar in enhancing accuracy and transparency in governance. In response to these technological advances, many countries moved swiftly to establish electronic governments, including the United States during President Bill Clinton's second term, the United Kingdom in 1999, and the Government of Dubai in 2000, among others.

Although the term '**E-government**' may sound straightforward and harmless, a range of offences can take place behind it, arising from electronic dealings - such as accessing people's personal data without their prior consent. That is why both comparative legal systems and Algerian law have introduced a number of measures covering cyber security and the protection of individuals, in line with constitutional guarantees, to safeguard privacy through clear legal frameworks and strong deterrents against breaches of personal information.

Given how vital personal data and privacy are, and with government increasingly managing citizens' information online to bring public services closer through modern technology, we're faced with a key question: **how effective are the legal safeguards used by e-government in protecting an individual's right to privacy from cyber breaches?**

To address this issue, we used a descriptive and analytical approach, examining the applicable national laws and comparing them with other jurisdictions where no domestic provisions exist.

We divided our paper into two main sections: the first covers E-government and its link to personal data security; the second looks at E-government mechanisms for preventing cybercrimes against individuals.

1-E-government and protecting personal data

E-government represents a major step forward in shaping how the state's institutions operate. It has also meant moving into the realm of cyberspace, with all the security challenges that come with it. To tackle cyber breaches, a number of advanced countries, including Algeria, have introduced legislation on cybersecurity and the protection of personal data. So, we'll begin by looking at what e-government is and how it relates to the security of individuals' information.

1.1- Electronic government:

We'll begin by looking at what E□government actually means and why it matters, both for public authorities and for individuals. We'll also explore how it links to people's personal data in the context of cyber security, and how that data is handled within a proper legal framework. All of this will be covered in the following points:

1.1.1- The meaning of E-government:

The existence and establishment of a state requires more than just a group of people living in a certain territory. The third pillar of the state, political authority or what is known as traditional government, must also be in place. This pillar is based on organising and supervising the affairs of the people, looking after their interests, protecting the state's territory against foreign aggression and protecting citizens from within. It also leads the state towards achieving its goals of security and stability. The government is considered an important element in the formation of the state, to the extent that some consider it the foundation upon which the definition of the state is based (Fouda, 2019, p. 29).

Traditional government is considered the foundation of the E-government model. Traditional government is defined as the organisational entity formed by states to manage the country's affairs and make strategic decisions related to its political, economic and social future. This administration covers areas such as strategic economic, military and security planning, national income development, citizen education and health care, improvement of living conditions, crisis management, development of the country's relations with the outside world, and many other tasks (Badran, 2004, p. 25).

As for E-government, opinions differ on how to define it. Some define it as advanced knowledge in the development of administrative knowledge, its applied techniques and professional skills. It enriches administrative thinking with concepts related to electronic knowledge, communications and information technology, as this relationship between the management of government activities and practices and electronic data reflects signs of progress in performance and rationality in various decisions and e-government tools, which are essentially represented by computers, which are a set of physical and intangible parts. These devices are integrated, and the device receives and processes data through a set of high-speed calculations and logical sequences, after which the required results appear and can be stored and used many times (Taha, 2017, p. 10).

E-government has also been defined as the use of information and communication technology to achieve reform by accelerating transparency, bridging distances, removing barriers, and giving citizens the opportunity to participate in all stages of the political process and related decisions that affect various aspects of their lives (Laargh & Touiti, June 2016, p. 206).

The comprehensive definition of this concept is that E-government is the virtual counterpart of real, or traditional, government, with the difference that the former exists in electronic networks and information systems, while the latter mimics the functions of the state apparatus that exists in physical form (Badran, 2004, p. 45).

Through these definitions, we can say that E-government provides its services in the same way as traditional government, but the difference is that all this is done through an electronic entity instead of paperwork and administrative complexities, which ultimately means that the former is not a substitute for the latter, but rather its other side within the digital system (Ben Aichaoui, June 2009, p. 288).

1.1.2-E-government objectives for administration &individuals:

One of the main aims of E-government is to deliver everything a traditional government does in the real world, whether for public services or for citizens, but through digital platforms and electronic systems

A-As for the government (Administration):

-Simplification and standardisation of procedures: conversion of paper-based processes to digital, saving time and reducing errors. -Improving operational efficiency: saving financial and human resources, and increasing the accuracy and speed of transactions. -Enhancing communication: Facilitating communication between different government departments and other institutions. -Transparency: Providing reliable information and tracking departmental performance. -Infrastructure development: building integrated information networks (Al-Salamy, 2002, pp. 253-255). -Service development: Introduction of new services such as electronic commercial registers, biometric ID cards, and online social security services (e.g., the Chifa card in Algeria) (Yahiaoui, December 2016, pp. 40-41).

B-As for individual citizens:

Instant access to services: Complete government transactions (renew documents, pay taxes, obtain information) from anywhere, anytime, without having to visit offices. -Saves time and effort: Shortens transaction waiting times and reduces the need for travel. -Increased transparency: Easy access to government information and insight into the progress of transactions. -Skill development: Increasing awareness and knowledge of digital technology (Laargh & Touiti, June 2016, pp. 210-211).

From the above, we can say that the objectives resulting from the use of E-government are specifically to increase data accuracy, optimize the use of material and human resources, reduce the volume of administrative procedures, and thus save effort, time, and costs, leading to higher performance levels in various government, economic, and other institutions. However, despite the advantages of E-government, it may face some challenges related to the security of individuals' data or its facilities for managing the affairs of its citizens. Therefore, we must find the relationship between E-government and the security of its users' data, whether individuals or facilities under its supervision.

1.2- E-government and protecting people's data:

At this point, we will address the definition of cybersecurity, which the E-government must maintain against cybercrime, as all of its activities are carried out in cyberspace through its electronic administrative facilities. Then we will highlight the most important personal data related to individuals in the field of cybersecurity and the relationship between an individual's personal data and E-government agencies. This study will cover the following points:

1.2.1-Cybersecurity:

Cybersecurity, as defined by experts, refers to the technical and organisational measures put in place to prevent unauthorised access to computer networks, stop misuse, and recover electronic data, ensuring information systems continue to operate smoothly while safeguarding the security, confidentiality and privacy of data within cyberspace (Bougara, September 2018, p. 106). The United States Department of Defense, for example, offers a clear definition of cybersecurity, describing it as all the organisational measures needed to protect information in every form, digital and physical, from crime, attacks, sabotage, espionage and other incidents. Meanwhile, the European declaration defines it as the ability of an information system to withstand hacking attempts or unexpected events that put data at risk (Ben Marzouq & Al-Kar, June 2018, p. 34). The Algerian legislator also defined cybersecurity in Law No. 18-04, paragraph (03) of Article (10), which states that "Cybersecurity is the sum of tools, policies, security concepts, security mechanisms, guidelines, risk management methods, operations, training, best practices, safeguards, and technologies that can be used to protect electronic communications against any event that could compromise the availability, integrity, and confidentiality of stored, processed, or transmitted data" (Law No. 18-04, dated 10 May 2018, p. 07).

Cybersecurity refers to technical mechanisms and programs, as well as human capabilities used by E-government to counter any infringement that may affect electronic information. Since we are talking about individuals' personal data, we must address the definition of personal data that is related to individuals' personal information.

1.2.2-Personal data of individuals:

It is a statement relating to a specific or identifiable natural person (Mansour, 2009, p. 311). Dr. Abdel Fattah Bayoumi Al-Hajazi believes that nominal data includes matters relating to a person's right to protect their reputation or their right to honor, reputation, and respect, i.e., individuals retaining their status in society, which confers a degree of appreciation and respect (Hajazi, 2007, p. 216). As for Professor Rachida Bouker, she sees it as information in a dormant state, consisting of numerical or non-numerical facts, realistic rather

than imaginary observations, or measurements taken in a systematic manner that can be read and understood in their simple meaning, and used to draw conclusions and inferences about their complex meaning by linking more than one piece of data and drawing any resulting conclusions (Bouker, 2012, p. 65); Moroccan legislation stipulates in Article (01), paragraph (01) of Law No. 08 of 2009 dated 18 February 2009, relating to the protection of individuals with regard to the processing of personal data, that "personal data: any information of any kind, regardless of its medium, including sound and image, relating to an identified or identifiable natural person, hereinafter referred to as “the data subject”. A person is identifiable if they can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity" (Law No. 09-08, dated 18 February 2009, p. 552). The Algerian legislator adopted the same definition as the Moroccan legislator in Article 3(1) of Law No. 18-07 of 10 June 2018 on the protection of natural persons with regard to the processing of personal data. In the second paragraph of the same article, the definition of the data subject is added as ‘any natural person whose personal data is being processed’ (Law No. 18-07, dated 10 June 2018, p. 12).

Legislation unanimously stipulates that the establishment and use of personal data processing systems are subject to state control, whether in terms of their establishment, activity or objectives, in addition to continuous supervision. Whoever is responsible for storing and processing information is obliged to take all appropriate measures to protect it and prevent its dissemination, access, use for purposes other than those intended, or disclosure contrary to the law. The importance of this obligation becomes apparent when the processing involves the transfer of data over the Internet (Mansour, 2009, p. 312); E-government today is obliged to protect individuals' personal data from any unlawful processing. This is the role of E-government, which is essentially based on the idea of managing information security through its legally authorised bodies. These bodies represent the general internal operations provided in the E-government project through managing relations between citizens and institutions and strengthening the interconnection between public administration

through information systems. Performing tasks electronically through E-government is the embodiment of the idea of electronic administration (Badran, 2004, p. 60). Whichever body is legally authorised to store and process information shall be obliged to take all appropriate measures to protect it and prevent its dissemination, access, use for purposes other than those for which it was intended, or disclosure contrary to the provisions of the law. The importance of this obligation is evident when the processing involves the transfer of data in cyberspace (Mansour, 2009, p. 312); Whatever its functions, the E-government is the entity legally responsible for protecting individuals' personal data.

2- Legislative mechanisms for E-government in protecting individuals' personal data:

The legal mechanisms relied upon by the government are means of protecting individuals' personal information from any infringement they may face in cyberspace. The government has authorised certain competent bodies to carry out their supervisory and oversight activities in order to protect individuals' personal data, whether they are civilians or engage in commercial activities. We cannot understand these mechanisms without knowing the meaning of processing an individual's personal data within a legal framework, in addition to the entities legally authorised to monitor and supervise, and how these entities respond to any breach of individuals' personal information.

2.1- The entity legally authorised to process personal data:

Before addressing the entity legally authorised to process personal data, we must understand the meaning of personal data processing through its jurisprudential and legal definition. We then define the entity responsible for processing this data. The state may only process personal data through legal texts that permit it to do so:

2.1.1- Processing of personal data:

Respect for private life is one of the established constitutional principles, with the Algerian Constitution of 2020 stipulating that citizens' private lives are protected by law (Constitution of 2020, Dated 30 December 2020, p. 13 Article 47); Everyone has the right to keep the secrets of their private life hidden from the public, protected from the interference and prying of others. This includes all aspects of a person's private life, such as their lifestyle, livelihood, family, health

and emotional matters (Ben Saleh, 2016, p. 311); The right to privacy has not been specifically defined, and there is near unanimity on the difficulty of arriving at a comprehensive definition of privacy. Jurisprudence and jurisprudence have established different and divergent definitions, but what they have in common is the mixing of the concept of privacy with the concept of data protection, which places privacy within the framework of the right to protection of private data. The British CALCUTT Committee defined the right to privacy as the right of individuals to protection against interference in their lives and affairs and those of their families, either by direct physical means or by the dissemination of information about them (Qaid, 2016, pp. 441-442). From this view, we find that an individual's personal data is related to their privacy, so an individual's personal data can only be processed with their consent. So what is the definition of processing an individual's personal data?

So the definition of processing personal data refers to any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, erasure or destruction (Hazam, June 2019, p. 284). Moroccan legislation defines it in the second paragraph of Article 1 of Law No. 08 of 2009 on the protection of individuals with regard to the processing of personal data, which states: ‘Any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, erasure or destruction"

(Law No. 09-08, dated 18 February 2009, p. 552). As for Algerian legislation was consistent with this definition, according to the text of Article (03), paragraph 3, of Law No. 18-07, which states: "The processing of personal data is any operation or set of operations performed by automated or non-automated means on personal data, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, encryption, erasure or destruction" (Law No. 18-07, dated 10 June 2018, p. 12). Moreover The information system is also the fundamental factor in building and structuring information online, through data processing, which is systematic in nature in the virtual world. Therefore, it is defined as: 'Organised and logically structured data that is processed automatically to provide the specific information required when it is called up.' This enables a person to use the data as needed, entering, exiting and sending it (Ben Younes, 2004, pp. 361-362). Furthermore, data processing can only be achieved through an information system, and the only justification for processing electronic personal data is to obtain data in a lawful manner (Salman, 2018, p. 15). The entity legally authorised to process this information or data we shall be explained in the following point.

2.1.2-The responsible of the treatment personal data:

In order to process any personal data relating to a person, whether they are natural or legal persons or persons governed by public or private law, there must be a body responsible for this task; before this, the person responsible for data processing must be identified.

A-Definition of the data controller:

The controller is the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. If the purposes and means of processing are determined by legislative or regulatory provisions, the controller must be specified in the law governing the organisation and management or in the statutes of the competent body, law or statutes governing the processing of the personal data concerned. The controller may take the form of a

ministry, bank, company, university, hospital, etc. All these bodies fall under the term 'E-government,' which is responsible for electronic processing (Hazam, June 2019, p. 289); As The Moroccan legislation in Law No. 08 of 2009 defines the data controller as "the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. If the purposes and means of processing are specified by legislative or regulatory provisions, the controller must be indicated in the regulatory and management law or in the statutes of the body responsible under the law or statutes for processing the personal data concerned" (Law No. 09-08, dated 18 February 2009, p. 553), The Algerian legislator agreed with the Moroccan legislator in his definition and added legal entities such as companies, associations, public or private institutions, and others. His definition states: 'Any natural or legal person, public or private, or any other entity acting alone or in conjunction with others to determine the purposes and means of data processing (Law No. 18-07, dated 10 June 2018, p. 12 Article 03 Paragraph 12). The processing may relate to human resources management, electoral rolls, driving licences, magnetic bank cards, health files, biometric cards, etc. Article 3 of Law 25-11, amending and supplementing Law No. 18-07, defines biometric data as: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm their unique identification" (Law No. 25-11, dated 24 July 2025, p. 15 Text 03 Paragraph 22).

B- Definition of an internal treatmenter:

The Algerian legislator defines it as 'any natural or legal person, public or private, or any other entity that processes personal data on behalf of the data treatmenter' (Law No. 18-07, dated 10 June 2018, p. 12 Article 03 Paragraph 13);

That is, any treatmenter who acts as the original treatmenter of information by agency, delegation, contract, etc (El-Eidani & Zarrouk, December 2018, p. 121); The meaning of the Algerian legislation is consistent with the meaning of Article 01 Paragraph (6) of Law No. 8 of 2009 with regard to Moroccan legislation, whereby the sub-

treatmenter processes information on behalf of the data treatmenter (Law No. 09-08, dated 18 February 2009, p. 553).

He can other person who is not responsible for the treatment or the subcontractor who treatments the data may be referred to by Algerian law as 'the third party'. This is any natural or legal person, public or private, or any other entity other than the person concerned and responsible for the treatment, the sub-treatmenter and the persons authorised to treatment the data who are under the direct authority of the person responsible for the treatment or the sub-treatmenter (Law No. 18-07, dated 10 June 2018, p. 12 Article 03 Paragraph 14).

Therefore, the government treatments data with the authorisation of the national authority for the protection of personal data; however, this data may be violated by persons who are not legally authorised to treatment it. This brings us to the term 'personal data breach,' which refers to any security breach that accidentally or illegally leads to the destruction, loss, alteration, disclosure, or unauthorised access to personal data that is transmitted, stored, or otherwise treatmented (Law No. 25-11, dated 24 July 2025, p. 15 Article 03 Paragraph 26).

Since processing is carried out automatically by the E-government, it has the right to pursue and prevent this crime through the competent government authority. Who is the competent government authority and what procedures are followed in the event of a breach of information security?

2.2- Measures taken by the government in the event of a breach of data:

The challenges of controlling data flowing through the internet are significant, as the latter allows for a huge flow of information, making it difficult to control. Therefore, Algerian legislation and comparative legislation have established measures to facilitate the protection of cyberspace from any violations that may occur, especially for individuals who use the internet for the purpose of protecting their financial or commercial interests.

2.2.1- General principles of state obligations towards digital users:

Article 4 of Law No. 18-04, which sets out the general rules governing postal and electronic communications, states that "the State shall, within the framework of its powers, ensure, in particular, that:

- Defining and applying standards for the creation and use of various services;
- Security and safety of electronic communications networks;
- Continuity and regularity of services provided to the public;
- Respecting the rules of fair competition between dealers, participants, contractors and customers;
- Providing services that comply with the legal and regulatory requirements for comprehensive service;
- Compliance with national defence and public security regulations;
- Respecting moral values and common decency;
- Ensuring clients meet their legal and regulatory responsibilities (Law No. 18-04, dated 10 May 2018, p. 05).

And the same Law the article 96 states that electronic communications networks may be established or operated under the conditions set by law, excluding facilities for national defence or public security. And Article 97 of the same law also states that setting up and running public electronic communications networks, as well as providing services to the public, must comply with the following requirements:

- Terms of service, quality of services, availability, security and safety of networks and services, as well as all other essential requirements as specified in the terms and conditions;
- Conditions of confidentiality of data and information transmitted via electronic communications networks;
- Conditions for protecting subscribers' privacy and personal data;
- Requirements necessitated by the need to maintain public order, national defence and national security (Law No. 18-04, dated 10 May 2018, p. 27).

All of this is aimed at safeguarding online users' privacy when dealing with digital government services. A clear example is online banking apps, which are designed to protect customers from hacking and fraud.

2.2.2- Electronic banking and security measures:

The electronic bank is considered an extension of E-government administration, as it contributes to banking services for citizens through electronic platforms operating on the Internet. It contains all

the software necessary to deal fully with customers regarding banking and other marketing services, and is licensed by law to conduct its activities in an electronic environment (Al-Tamimi, 2012, pp. 45-48). The electronic bank offers a comprehensive range of banking services via its website and guarantees instant and fast digital transfers. The electronic bank also offers other services in addition to those listed above, such as easy-to-use electronic currencies, known as E-money (Al-Ginihi & Al-Ginihi, 2005, p. 35).

Since electronic money is handled by banks that provide electronic services, the bank may be exposed to legal risks such as violating individuals' privacy by imitating the bank's website, thereby misleading the bank's customers into believing that this platform is genuine. This is where the violation of individual privacy begins, whether it be accessing their financial balance or stealing it, etc. What legal measures should the bank take?

By legal measures that the bank must take, we mean swift legal means aimed at immediately stopping the attack on the bank. In fact, there is no specific provision in the Arab legal system, such as Egyptian law, regarding the measures that must be taken to stop such an attack. This shortcoming is particularly significant given the extreme importance of these procedures, as they are immediate means by which to stop this abuse, which drains customers' funds by exploiting their passwords and account numbers. It also damages the bank's commercial reputation (Al-Tamimi, 2012, pp. 554-555).

As for Algerian legislation, according to Regulation No. 24-04 dated 13 October 2024 on the specific conditions for licensing, establishing, accrediting and operating digital banks, Article 12 states that: « Digital banks are subject to the same rules and prudential conditions applicable to traditional banks » (Regulation No.: 24-04, Dated: 13 October 2024, p. 31). When considering legal proceedings relating to breaches of customer privacy, we find that Algerian lawmakers have required all financial institutions, including electronic banks, to have monitoring systems in place to monitor transactions and implement appropriate and effective internal procedures that allow all accounts to be screened for unusual or suspicious transactions. In such cases, financial institutions must inquire about the source and destination of the funds, as well as the location of the

transaction and the identity of those involved. A confidential report must be drawn up and kept on file (Regulation No.: 24-03, Dated: 24 July 2024, p. 28 Article 24). However, these methods are characterised by their slowness, especially when it comes to violations of customer privacy.

Conclusion

Cyberspace is one of the most important challenges that countries face in protecting their sovereignty from intrusion. Therefore, comparative legislation and Algerian legislation have issued several laws related to mechanisms for preventing and deterring any crime that occurs in cyberspace. Not to mention the technologies and policies that require E-government to avoid certain suspicious websites where cyber crimes are prevalent. E-government is an effective means of monitoring and supervising all its electronic entities. The best evidence of this is Law No. 18-04, which sets out the general rules relating to postal and electronic communications. Despite this law, there are still some shortcomings with regard to the crime of violating individuals' privacy.

Therefore, in 2020, the Algerian Constitution guaranteed the right to privacy of individuals, and the Algerian legislature also issued Law No. 18-07 on the protection of natural persons in the field of personal data processing. This law prohibits access, modification, or even viewing without the consent of the person concerned or the authorisation of the national authority for the protection of personal data. Despite the Algerian legislature's efforts to protect individuals' personal data through these laws, there are still shortcomings that the Algerian legislature must address, namely by:

- Establishment of an E-government to supervise and monitor E-administration activities; this shall be achieved by issuing clear laws regulating this body;
- Establish technical and legal mechanisms to regulate the privacy of E-government in its operations;
- Introducing swift, flexible laws to tackle privacy breaches;
- Imposing strict penalties on those who violate individuals' privacy, especially social media accounts, which have become widespread today;

- Imposing strict penalties on those who violate the privacy of influential individuals in the state, as this affects the reputation and prestige of the state;
- Algerian lawmakers should establish a technical committee to monitor identity theft, particularly on electronic banking platforms and in the activities of e-commerce merchants, using artificial intelligence technologies.

FootNotes:

1. Al-Ginihi, M., & Al-Ginihi , M. (2005). *Electronic Banking.* Egypt: Dar Al-Fikr Al-Jami'i, Alexandria.
2. Al-Salamy, A. (2002). *Excellence Management: Management Models and Techniques in the Knowledge Age.* Cairo: Dar Gharib Publishing.
3. Al-Tamimi, A. (2012). *Regulation of Electronic Banking on the Internet.* Egypt: Dar Al-Jami'ah Al-Jadidah Alexandria.
4. Badran, A. (2004). *E-Government: From Strategy to Implementation*. Beirut: Arab Institute for Studies and Publishing.
5. Ben Aichaoui, A. (June 2009). The impact of e-government implementation on business institutions. *El-Bahith Review, 07*(07).
6. Ben Marzouq, A., & Al-Kar, M. (June 2018). The Electronic dimension of the Algerian security policy in combating terrorism. *Social and Human Sciences Review , University of Batna 1, 19*(01).
7. Ben Saleh, M. (2016). *International Legal Protection of Personal Data Online.* Egypt: Arab Studies Centre for Publishing and Distribution.
8. Ben Younes, M. A. (2004). Crimes arising from the use of the Internet. Egypt: Doctoral thesis, Faculty of Law, Ain Shams University.
9. Bougara, Y. (September 2018). Cybersecurity: Algeria's Strategy for Security and Defence in Cyberspace. *Journal of African Studies and the Nile Basin, Arab Democracy Centre, 01*(03).
10. Bouker, R. (2012). *Crimes against automated processing systems in Algerian and comparative legislation.* Lebanon: Al-Halabi Legal Publications.
11. Constitution of 2020, C. (Dated 30 December 2020). Constitution of the People's Democratic Republic of Algeria. *(Official Gazette No. 82)*. People's Democratic Republic of Algeria.
12. El-Eidani, M., & Zarrouk, Y. (December 2018). Protection of personal data in Algeria in light of Law No. 18-07. *Maalem Magazine for Legal and Political Studies, 02*(03).
13. Fouda, M. A. (2019). *Constitutional Amendments in Contemporary Democratic Systems and Oversight.* Egypt: Dar Al-Nahda Al-Arabiya Publishing and Distribution.
14. Hajazi, A. B. (2007). *Combating computer and internet crimes in model Arab law.* Egypt: Dar Al-Kotob Al-Qanuniya.
15. Hazam, F. (June 2019). Legal guaranties Personalized data Treatment: a study in light of Law No. 18-07. *Idjtihad for legal and economic studies review, 08*(04).
16. Laargh, N. m., & Touiti, M. (june 2016). Electronic Government Strategy "The Algerian attempt". *Milav Journal of Research and Studies, 2*(1).

17. Law No. 09-08, L.-0. (dated 18 February 2009). the protection of individuals with regard to the processing of personal data. *(5711)*. Official Gazette of the Kingdom of Morocco.
18. Law No. 18-04, L.-0. (dated 10 May 2018). sets out the general rules governing postal services and electronic communications. *(Official Gazette No. 27)*. Algeria: People's Democratic Republic of Algeria.
19. Law No. 18-07, L.-0. (dated 10 June 2018). the protection of natural persons with regard to the processing of personal data. *(Official Gazette No. 34)*. Algeria: People's Democratic Republic of Algeria.
20. Law No. 25-11, L.-1. a.-0. (dated 24 July 2025). the protection of natural persons with regard to the processing of personal data. *(Official Gazette No. 48)*. Algeria: People's Democratic Republic of Algeria.
21. Mansour, M. H. (2009). *Electronic Responsibility.* Egypt: Dar Al-Jami'ah Al-Jadida, Alexandria.
22. Qaid, A. R. (2016). *Consumer Protection: A Study of Consumer Protection Laws and General Rules in Civil Law.* Egypt: Arab Studies Centre for Publishing and Distribution.
23. Regulation No.: 24-03, R.-0. (Dated: 24 July 2024). Concerning the prevention and combating of money laundering, terrorist financing and the financing of weapons of mass destruction. *(Official Gazette No.: 58)*. Algeria: People's Democratic Republic of Algeria.
24. Regulation No.: 24-04, R.-0. (Dated: 13 October 2024). Concerning the specific conditions for licensing, establishing, accrediting and practising digital banking activities. *(Official Gazette No.: 77)*. Algeria: People's Democratic Republic of Algeria.
25. Salman, Y. (2018). Crimes against privacy committed through modern information technology. *Journal of the Faculty of Law, Al-Nahrain University, 16*(29).
26. Taha, M. A. (2017). *Legislative response to computer and internet crimes: a comparative study. Mansoura.* Egypt: Dar Al-Fikr Wal-Qanun.
27. Yahiaoui, I. (December 2016). E-government in Algeria: between reality and challenges. *Journal of Economics and Management Sciences, 16*(16).

References :

1-Books:

-Al-Ginihi Munir & Al-Ginihi Mamdouh. (2005). *Electronic Banking*. Egypt: Dar Al-Fikr Al-Jami'i, Alexandria.
-Al-Salamy, Ali. (2002). *Excellence Management: Management Models and Techniques in the Knowledge Age*. Cairo: Dar Gharib Publishing.
-Al-Tamimi, Alaa. (2012). *Legal Regulation of Electronic Banking on the Internet*. Egypt: Dar Al-Jami'ah Al-Jadidah Alexandria.
-Badran Abbas. (2004). *E-Government: From Strategy to Implementation*. Beirut: Arab Institute for Studies and Publishing.
-Ben Saleh Marwa Zain Al-Abidin. (2016). *International Legal Protection of Personal Data Online*. Egypt: Arab Studies Centre for Publishing and Distribution.
-Bouker Rachida. (2012). *Crimes againstautomatedprocessingsystems in Algerian and comparative legislation*. Lebanon: Al-Halabi Legal Publications.

-Fouda, Mohamed Attia. (2019). *ConstitutionalAmendments in Contemporary Democratic Systems and Oversight*. Egypt: Dar Al-Nahda Al-ArabiyaPublishing and Distribution.
-Hajazi Abdel Fattah Bayoumi. (2007). *Combating computer and internet crimes in model Arab law*. Egypt: Dar Al-Kotob Al-Qanuniya.
-Mansour, Mohamed Hussein. (2009). *ElectronicResponsibility*. Egypt: Dar Al-Jami'ahAl-Jadida, Alexandria.
-Qaid Ashraf Muhammad Rizq. (2016). *Consumer Protection: A Study of Consumer Protection Laws and General Rules in Civil Law*. Egypt: Arab Studies Centre for Publishing and Distribution.
-Taha Mahmoud Ahmed. (2017). *Legislativeresponse to computer and internet crimes: a comparative study*, Egypt: Dar Al-Fikr Wal-Qanun.

2-Articles &Journals

-El-Eidani, Mohamed, and Youssef Zarrouk. (2018). *Protection of personal data in Algeria in light of Law No. 18-07*. Maalem Magazine for Legal and PoliticalStudies, Vol. 2, N°. 3.
-HAZAM Fatiha. (2019). *Legal guarantiesPersonalized data Treatment:astudy in light of Law No. 18-07*. Idjtihad for legal and economicstudiesreview, Tamenghest University Centre, Algeria, Vol8, N°. 04.
-Salman, Youssef. (2018). *Crimes againstprivacycommittedthrough modern information technology*. Vol 16, N°. 29 and 30. Journal of the Faculty of Law, Al-Nahrain University, Iraq.
-Ben Aichaoui, Ahmed. (June 2009). *The impact of e-governmentimplementation on business institutions*. El-Bahith Review by QasdiMerbahUniversity, Ouargla, Algeria, Vol7,N°. 7.
-Laargh Nassima Moudjahid &Touiti Mustapha. (June 2016). *ElectronicGovernmentStrategy "The Algerian attempt"* Milav Journal of Research and Studies, Algeria, Vol. 2, No. 1.
-Yahiaoui, Ilham. (december 2016). *E-government in Algeria:between reality and challenges*. Journal of Economics and Management Sciences, University of Setif 1, Algeria Vol. 16,N°. 16.
-Ben Marzouq Antara & Al-Kar Muhammad. (June 2018). *The Electronic dimension of the Algerian securitypolicy in combatingterrorism*. Social and Human Sciences Review ,University of Batna 1, Algeria, Vol19,N°. 01
-Bougara, Youssef. (September 2018). *Cybersecurity:Algeria'sStrategy for Security and Defence in Cyberspace*. Journal of AfricanStudies and the Nile Basin, Arab Democracy Centre, Germany, Vol1N°. 03

3-Acadimic Theses

-Ben Younes Mohamed Aboubakr. 2004. *Crimes arisingfrom the use of the Internet*. Doctoral thesis, Faculty of Law, Ain Shams University, Egypt.

4-Law & Official Documents

-Constitution of 2020. (Dated 30 December 2020). Constitution of the People's Democratic Republic of Algeria. (Official Gazette No. 82). People's Democratic Republic of Algeria
-Law No. 18-04 (dated 10 May 2018) sets out the generalrulesgoverning postal services and electronic communications. (Official Gazette No. 27). People's Democratic Republic of Algeria

-Law No. 18-07 (dated 10 June 2018) on the protection of naturalpersonswith regard to the processing of personal data (Official Gazette No. 34). People's Democratic Republic of Algeria
-Law No. 25-11 (dated 24 July 2025), amending and supplementing Law No. 18-07 dated 10 June 2018 on the protection of naturalpersonswith regard to the processing of personal data. (Official Gazette No. 48). People's Democratic Republic of Algeria
-Regulation No.: 24-03. Dated: 24 July 2024. Concerning the prevention and combating of money laundering, terroristfinancing and the financing of weapons of mass destruction. (Official Gazette No.: 58). People's Democratic Republic of Algeria
-Regulation No.: 24-04. (Dated: 13 October 2024). Concerning the specific conditions for licensing, establishing, accrediting and practising digital bankingactivities. (Official Gazette No.: 77). People's Democratic Republic of Algeria
-Law No. 09-08 (dated 18 February 2009) on the protection of individualswith regard to the processing of personal data (No. 5711). Official Gazette of the Kingdom of Morocco.