The legal system of information security and its role in the protection of information within institutions

Faiza Khireddine[1]*,

[1] University of Algiers 1 Faculty of Law Said Hamdine, (Algeria)

Khireddine.faiza@yahoo.com

Submission date: 18/02/2023 Acceptance date: 21/05/2023 Publication date: 04/06/2023

Abstract:*The developments in information and communication technology and the advent of the Internet have witnessed a qualitative leap in the lives of individuals and societies, and all different sectors have become dependent on the use of digitization and information systems in accomplishing their tasks. By strengthening the security of its institutions and ensuring their information security and protecting them from various criminal operations that take place through the Internet.*

key words*: Digitization, cybercrime, information security, cybercrime, information protection system.*

ملخص:

عرفت التطورات الحاصلة في تكنولوجيا المعلومات والاتصالات وظهور شبكة الانترنت قفزة نوعية حضارية في معيشة الأفراد والمجتمعات، وأصبحت جميع القطاعات المختلفة تعتمد على استخدام الرقمنة والأنظمة المعلوماتية في انجاز مهامها، فأصبحت تهدد بخطر الاعتداء عليها مما دفع بالدولة إلى تدعيم جهاز المحافظة عليها عن طريق ترسانة قانونية تضمها من خلال تقوية أمن مؤسساتها وضمان أمنها المعلوماتي وحمايتها من مختلف العمليات الإجرامية التي تتم عن طريق شبكة الانترنت.

الكلمات المفتاحية: الرقمنة، الجرائم الالكترونية، الأمن المعلوماتي، الخطر الالكتروني، نظام حماية المعلومات.

Introduction:

Information systems within organizations become an important resource for them, since they provide them with the different information that help them make the right decisions. In order that these systems can accomplish the tasks expected of them in the best way, the organization must protect this resource from the various risks that can hinder its functioning. (Seffari, 2022)

The need to educate Algerian institutions to the need to adopt standards for information security because of their direct positive impacts on reducing the risks of interruption of the functioning of economic systems and keeping the confidentiality of information, ensuring the integrity and reliability of information sources and ensuring availability of information sources and online operations without interruption. Also the need to improve Algerian laws and legislation that are related to information security and especially in light of an environment with interconnected and fast-paced business, which increases the volume of threats and risks. It is necessary to strive to confront these dangers and to develop the necessary technical methods and means for this confrontation. To this we see to ask the following problem: **what is the legality system of information security? How does data protection and information are used?**

Defining information security

Information security meaning:

Several definitions have been provided to information security, some of which will be listed below:

- The US National Security Systems Committee defines information security as: The protection of information and its important elements, including the systems and devices that use, store and transmit this information (Kraybit Hk Hadid N, 2017).
- From an academic point of view, Information security is the science that deals with theories and strategies which provide protection for information from the risks that threaten it and from their activities. From a technical point of view, it is the means, tools and procedures (Seffari, Information Security And The Need To Move Towards The Application Of Standard , 2022).

From a legal angle, information security is the subject of studies and measures to protect confidentiality, the integrity of the content and availability of information, and the fight against activities of abuse or exploitation of its systems in the commission of crimes (N Abdelatif Abdelkarim, KH Alrubaie , 2013).

-It means also all policies, procedures and technical tools that are used to protect the system from all forms of illegal use of resources such as theft, alteration and modification, damage to information or databases or intentional physical damage to devices in addition to the presence of other threats such as human errors, natural accidents and disasters (Sharif, 2018).

The previous definitions all indicate that information security is nothing but a set of procedures and measures taken by the institution in order to protect its information assets, by relying on technical means and tools to ensure its protection.

The objectives of information security:

It is to develop, implement and maintain information which constitutes a large and increasing part of business cost; it also helps to ensure that organizations perform their operations effectively; therefore, the main objectives of information security can be summarized as follows (Al-Tayeb, 2018):

- Reducing the risks of interruption of the functioning of economic systems and institutions.
- Keeping the confidentiality of information.
-Ensuring the integrity and reliability of information sources.
- Ensuring availability of information sources and online operations without interruption.
- Guarantee comply to policies and laws related to security and privacy.

Security information basis:

In order to protect information security, it is necessary to provide a set of elements that must be taken into consideration. These elements are represented in what is known as the information security triangle (Seffari, Information Security And The Need To Move Towards The Application Of Standard , 2022):

Source: Prepared by the researcher. These elements are (N Hadid, Hk Kraybit , 2017):

- Confidentiality: it is protecting information from spreading in an unauthorized way, by preventing not allowed users from entering and accessing information sources. In order to ensure this, you must monitor access to information and encrypt it in order to increase its security and protection during the storage or transmission process, while providing authorized persons to view this information with decryption keys.
-Integrity: it focuses on keeping data clean and untainted, both when it's uploaded and when it's stored. This means making sure only those who are allowed to modify it, modify it.
- Availability: it means keeping data accessible, essentially when an authorized user needs to access data or information, they can. It can be sometimes confused with or even seem to contradict confidentiality.

Electronic attacks and Cybercrimes

The risks that threaten information security are numerous and have developed year after year as they keep pace with every innovative modern technology in the world of information and communication technology.

Types of electronic attacks:

Electronic attacks are those attacks that may occur to information within the electronic scope, such as information stored in a personal computer, the network or the server, and include various methods such as impersonation, unauthorized use, service obstruction, eavesdropping and malicious programs. The forms of attacks varied and took many ways and names Confidentiality Availability Information Security Integrity (Filali, 2019).

- **Malware attack**: They are malicious programs that run away without the help of the computer user such as (Alhassan, Mohammed Mahfouz, Alexander Adjei-Quaye, 2017):

-Viruses: A malicious program that includes destructive targets for the contents of infected computers, characterized by its ability to copy itself.

- The Ver worm: A malicious program capable of multiplication and moving from one computer to another. Its goal is overcrowding the infected computer and slow network speed.

-Macro program: It is designed to work on a single application such as word or Excel.

- Logic Bombs: A program that infects the system and waits for an event (such as date, verbs, private data, etc.).
-Trojan horse: It is a program hidden in another program that performs malicious operations without the user's knowledge and takes control of the device. It works to steal passwords and sensitive information.
- Spyware attack: These are hidden programs that leak information and send it abroad via Internet.
- Sniffing: This technique relies on eavesdropping on transmitted data in the organization's network.
- Service Denial: physical damage to the server to prevent service provision.
- Spamming: This is to harm the system of electronic messages and to send them randomly.
- The IP address spoofing method: that is, replacing the sender's IP address with another address and thus breaking into the organization's network.

Effects of Cybercrimes

The definition of information crime has evolved as it was linked to the development of information technologies. Therefore, we find that its definitions have developed moving from "computer misuse", to "computer fraud", "information crime", then "computer crimes", and "computer-related crime". Then "high-tech crimes'', "hackers crimes", "internet crimes", and finally "cybercrime".
Many business owners get so busy that they forget about other important factors like cybercrime. If you haven't considered your company's cyber security needs, your business and customers could already be at risk (Seffari, Information Security And The Need To Move Towards The Application Of Standard , 2022).
In reality, there are many things you can do to stop cybercriminals from harming your company. By learning more about cybercrime's effects on business, you can also determine ways to prevent your company from becoming a victim. In 2017, the newsworthy Equifax data breach affected 147.9 million consumers. Mobile game producer Zynga was targeted by hackers in 2019, and the hack led to data breaches for 218 million users. These hacks gave cybercriminals access to Facebook IDs, emails, phone numbers, and other personal information. (Desmet, 2021)

Cyber-attacks like these can damage more than a company's brand image. Medical information, personal banking details, and much more can also be lost. With the Quest Diagnostics data breach in 2019, 11.9 million records were hacked. Today, cybercrime costs companies and individuals across the world more than 445 billion$ per year. Cybercrime effects on businesses play a big part in these numbers and continue to grow (Karra, 2021).

Local data protection laws and scope

The law N° **18-07** dated on 10 June 2018 related to the protection of private persons in the processing of personal data (hereafter the "Law") has set out the conditions of the collection, recording, organization, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, as well as locking, encryption, erasure or destruction of any information, whatever its support, concerning an identified or identifiable person, directly or indirectly, in particular by reference to an identification number or to one or more elements specific to their physical, physiological, genetic, biometric, psychic, economic, cultural or social identity.

Despite its publication on 2018, the entry in force of this Law is subject to the actual installation of the authority in charge of protection of personal data which is until now (February 2021) not installed yet.

Main obligations and processing requirements

Any personal data processing is subject to a prior declaration to the national Authority or its authorization.

The controller must implement the appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorized dissemination or access, in particular when the processing involves data transmission in a network, as well as against any other form of unlawful processing (El Abeidi, Fatma Nadji, 2012).

The controller as well as the persons who, in the performance of their duties, have knowledge of personal data, are required to respect professional secrecy even after having ceased to exercise their functions, under criminal sanctions.

Any person acting under the authority of the controller or that of the subcontractor who has access to personal data may only process them on the instruction of the controller, except in the case of execution of a legal obligation (S Bediaf, A Hamrani, 2020).

When the controller is not established on Algerian territory, he or she must notify the national authority of the identity of his or her representative installed in Algeria who, without prejudice to his personal responsibility, replaces him in all his rights and obligations resulting from the provisions of the law.

Interconnection of files containing personal data must obtain prior authorization of the Authority.

The processing of personal data with a purpose of public interest research, study or evaluation in the field of health is authorized by the national authority, in compliance with principles defined by this law and according to the public interest that the research, study or evaluation presents.

There is no age limit regarding the data subject. The law has mentioned however that a "child" needs the prior consent of his or her legal guardian or the judge (Al-Tayeb I. B., 2018).

Processing of personal data that reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of the data subject or which relates to his health including his genetic data is forbidden except when:

-the processing is necessary for the safeguard of vital interests of the data subject or of another person and if the data subject is physically or legally unable to give consent.

-The processing is carried out, with the consent of the data subject, by a foundation, association or non-profit organization of a political, philosophical, religious or trade union nature, within the framework of its legitimate activities, provided that the processing concerns only the members of this body or the persons who maintain regular contact with it related to its purpose that the data are not communicated to third parties without the consent of the persons concerned (El Abeidi, Fatma Nadji , 2012).

-The processing relates to data clearly made public by the data subject, as long as his or her consent to the processing of the data can be inferred from his or her statements.
-The processing is necessary for the recognition, exercise or defense of legal claims and is carried out exclusively for this purpose.
-The processing of genetic data, excluding those carried out by doctors or biologists and which are necessary for the practice of preventive medicine, medical diagnostics and the administration of care or treatment.
Personal data relating to offences, penalties and security measures can only be processed by the judicial authority, public authorities, legal persons who manage a public service and court officials within the framework of their legal powers.

Sanctions and non-compliance

There are several types of sanctions for each kind of infringement to the rules related to protection of personal data.

Administrative sanctions:

In case of non-respect of the rules related to data protection, the abovementioned authority can decide the following administrative sanctions:
-the warning.
-the notice.
-provisional withdrawal for a period that may not exceed one year, or the definitive withdrawal of the declaration receipt or authorization.
-an administrative fine up to(DZD 500,000).

Criminal sanctions:

There are various criminal offences under the law among others:
-unlawful obtaining of personal data.
-misuse of the collected personal data.
-transfer of personal data without authorization.
-destroying or falsifying information and documents.
-making false statements in response to an information notice or obstruction to the work of the authority; and altering personal data to prevent disclosure to the data subject. (Al Otaibi, G Ghanem , 2013)
Sanctions may vary between two months to five years' imprisonment and from (DZD 20,000 to DZD 500,000).

In addition to the organization, individual company directors can face criminal liability (fines and custodial sentences).
The above-mentioned Authority has the following enforcement powers:
-to impose information notices and publish them.
-to impose the destruction of the data and/or its removal or closing.
-to impose encryption of the data.
-entry and inspection.
A data subject may (in addition to making a complaint to the Authority) also make a claim to the courts for compensation for material or non-material damage (which may include distress).

Application

Criminal law provides for the prohibition of any fraudulent access to any system, or the collection, processing, storage, transfer of personal data for criminal reasons and considers as an offender:
- Anyone who fraudulently introduces data into an automated processing system or fraudulently deletes or modifies the data it contains.

- Anyone who willfully and fraudulently: designs, researches, collects, makes available, disseminates or markets data that is stored, processed or transmitted by a computer system.

- Anyone who holds, reveals, discloses, or makes any use whatsoever of the data obtained by the above mentioned means.
-The Law n° 09-04 provides for the measures and rules for offences related to technology and communication, the obligation for service providers to cooperate with judicial police and authorities for this purpose. The principle of access and its details will be described in the request or order of access. It might be the order to provide readable data or more information such as access to a computer system including its encryption codes.

-The above-mentioned surveillance operations may only be carried out with the written authorization of the competent judicial authority. It may, in some circumstances, be issued to judicial police officers by the General Attorney at the Court of Algiers, for a period of six months renewable, on the basis of a report indicating the nature of the technical

process used and its objectives. In the latter case, the technical devices put in place must focus, exclusively, on the collection and the recording of data relating to the prevention and combating of terrorist acts and attacks on the security of the State.

-The Law 18-04 consecrates the principle of protection of the privacy and personal data of subscribers and users of internet networks, defines among other provisions the "cyber security" and measures to implement in this regard, and also provides for the obligations of electronic communications operators.

-The Law 18-04 defines cyber security as the set of tools, policies, security concepts, security mechanisms, guidelines, risk management methods, actions, training, good practices, guarantees and technologies that can be used to protect electronic communications against any event that could compromise availability, integrity or confidentiality of data stored, processed or transmitted. The authority in charge of the regulation of electronic communications scrutinizes and verifies that electronic communications operators respect their commitments to cybersecurity. It is worth mentioning that there are no more details regarding cybersecurity conditions nor sanction in case of infringement.

-The Decrees related to licenses to operate public telecommunication networks provide for some provisions applicable to the contractor holding the telecom license on the confidentiality of information and protection of users and personal information, as well as provisions required for national defense and cooperation with governmental authorities, including the applicable sanctions.

-Decision N° 48/SP/PC/ARPT/17, provides for some rules in connection with data protection and security such as the commitment to:
-Establish infrastructure on the national territory and ensure that this uses equipment integrating the most recent and proven technologies.
-Guarantee that customer data is hosted and stored on national territory.
-Ensure the integrity and confidentiality of customer data except in the cases provided for by the texts in force.
-Guarantee a backup solution for hosted or stored data.

-Establish a customer identification file.
-Do not disclose or use customer data.
-Put in place the necessary mechanisms to ensure the security of data, applications and infrastructure associated with cloud computing, in particular regarding the integrity and confidentiality of data, through the implementation of information security mechanisms against various threats and intrusions;
-The physical and environmental security of the premises housing the infrastructure, particularly against fires and water damage.
-The Decree n° 02-156 states the obligation for operators and service providers to take all necessary measures to ensure compliance, including: network security; maintenance of network integrity; data protection, including personal, protection of privacy and confidentiality of information processed, transmitted and stored.

Conclusion:

Through this study, we tried to sensitize Algerian institutions to the need to adopt standards for information security because of their direct positive impacts on reducing the risks of interruption of the functioning of economic systems and keeping the confidentiality of information, ensuring the integrity and reliability of information sources and ensuring availability of information sources and online operations without interruption. Also the need to improve Algerian laws and legislation that are related to information security and especially in light of an environment with interconnected and fast-paced business, which increases the volume of threats and risks. It is necessary to strive to confront these dangers and to develop the necessary technical methods and means for this confrontation.

We came up with a set of recommendations that we can summarize as follows:
- Enacting a stand-alone law on cybercrime with an emphasis on its implementation on the ground;
- We have been implementing information systems in organizations and attracting support staff specialized internally and externally in information security to supervise this aspect.

- Awareness of the dangers of cybercrime through media campaigns and the inclusion of specialties in the field of information security in Algerian universities;
- Establishing mechanisms to deal with accidents and emergencies in the field of information security by forming centers and teams for immediate response that work seriously.

References

Alhassan, Mahfouz M. Adjei-Quaye A. (2017). ‘’*Information Security In An Organization’’.* International Journal of Computer (Ijc,2017, Vol 24, (N° 01).

Abdel-Latif Abdel-Karim, N. Al-Rubaie, K H. (2013). ‘*’Information Security and Confidentiality and Its Impact On Competitive Performance, An Applied Study in The Iraqi General Insurance Companies And Al-Hamra National Insurance’’.* Journal of Accounting And Financial Studies. Volume 8, No. 23. University of Baghdad, Iraq.

Al Otaibi, Ghanem G. (2013). ‘’*Information Systems Security And Its Relationship To The Levels Of Creativity Of Workers In The Stc*’’. Magister Thesis. Saudia Arabia: Naif University.

Ben Karra A. (2021). ‘*’A Strategy To Achieve Information Security For E-Government In Algeria*”. Comprehensive International Conference On Theoretical Issues and Their Operational Solution Methods. Dar Arafid for Production

Bin Al-Tayeb (2018). ‘*’The Importance of Information Systems Security for Modern Economic Institutions*’’. Journal of Development and Applied Economics. Al-Masila University. Issue 3.

El Abeidi, Fatma Nadji. (2012). ‘’*The Risk of Using Computerized Accounting Information Systems And Its Impact On The Efficiency Of Auditing Process In Jordan’’.* Magister Thesis Middle East University. Jordan.

Bediaf S. Hamrani, A. (2020). ‘*’Information Security in Algeria. Algerian Journal for Security and Development’’*. Issue16.

Filali, A. (2019). ‘*’The Level of Information Security in The Algerian Organization and The Extent to Which It Is Affected by The Nature of Threats and The Nature of the Protection Applied*.’’ Phd Thesis. University of Tlemcen, Algeria.

Desmet, N. (2022). ‘*’Cybercrime Effects On Business: Why You Should Care*”. Https://Www.Linkedin.Com/Pulse/Cybercrime-Effects-Business-Why-You-Should-

El Hamami. Alaa Hocine, Alaani. Saad Abdelaziz (2022). ‘’*Technology of Information Security and Protection Systems”*. Dar Wael. Volume 09 Number02. Jordan

Mokrani K. Cherbi M L. (2019). "*An Analytical Study of the Reality of Information Security in Algeria Telecom*." Ouargla. Journal of Financial Accounting and Managerial Studies. Vol 06. Number 03.

Seffari A. (2022). "*Information Security and The Need to Move Towards the Application of Standard*". Journal of Human Sciences- Oum El Bouaghi University.

14-Yahya Sharif, H. (2018). "*The Impact Of The Information System On Strategic Vigilance In Small And Medium Enterprise".* A Field Study On Some Algerian Enterprises. Phd Thesis in Economic Sciences. Algeria: Farhat Abbas Setif.