Breach of the confidentiality of personal data in the digital space.

Fadhila GUERNANE

University Mhamed Bougara of Boumerdes, (Algeria)
f.guernane@univ-boumerdes.dz

Submission date: 22/02/2022 Acceptancedate: 26/05/2022 Publication date: 05/06/2022

Abstract: *The right to privacy has received significant attention from legal and constitutional legislators as a personal right that guarantees human dignity. Personal data is crucial to the right to privacy. Therefore, protecting it is preserving this right. However, the great revolution the world has experienced in the field of information technology has become a threat to this right.*
The use of the Internet has proven its inability to provide sufficient security for data privacy. Access to this information has become very easy by creating new methods to invade the privacy of individuals by accessing this personal space.

key words*:persenal data; digital space; piracy; Right to privacy;Personal rights.*

ملخص: *حظي الحق في الخصوصية باهتمام بالغ من طرف المشرع القانوني والدستوري وحتى الدولي باعتباره من الحقوق اللصيقة بالشخصية ، وتعد البيانات الشخصية أحد التطبيقات الهامة للحق في الخصوصية ، ومن ثم فإن حمايتها هو سبيل للحفاظ على هذا الحق ، إلا أن الثورة الهائلة التي عرفها العالم في مجال تقنية المعلومات أصبحت تشكل خطرا على هذا الحق وتهدد بانتهاكه ، حيث أثبت استخدام الانترنت عجزه عن توفير أمان كاف لسرية ما ينقل عبرها من بيانات ، وأضحى الوصول إلى هذه المعلومات أمراسهلا من خلال استحداث أساليب جديدة للتعدي على خصوصية الأفراد عبر الولوج إلى هذه البيانات الشخصية .*

الكلمات المفتاحية: *البيانات الشخصية ، الحق في الخصوصية ، الفضاء الرقمي ، الحقوق اللصيقة بالشخصية ، التعدي .*

Introduction:

Ensuring the citizen's right to privacy is a fundamental requirement that all countries seek to achieve, preserving their private secrets and preventing them from being hacked by others and not exposed only through the protection of personal data. However, the technological evolution with regard to the facilitation of the life of the individuals is important and, in turn, it has become a real danger for the confidentiality of the personal data of individuals due to its unprecedented speed in collecting and integrating this information in digital space. This made it vulnerable to various attacks from individuals and even governments, such as wiretapping, extortion, information systems hacking, and access to personal and professional secrets.

This required highlighting the different forms of personal data breaches in this virtual environment in order to facilitate its response in various forms, be it legal or technical.

For this, the following problem was explored: **What are the forms of attacks created by the digital revolution on personal data and its impact on the violation of the right to private life?**

On this basis, the action plan has been divided into two sections:

Chapter (I):the notion of personal data as one of the applications of the right to privacy.

Chapter (II): methods of attacking personal data in the light of the digital.

CHAPTER (I):THE NOTION OF PERSONAL DATA AS ONE OF THE APPLICATIONS OF THE RIGHT TO PRIVACY.

Ensuring the protection of personal data is sufficient for the citizen to preserve his right to privacy, and also allows the State to consult and process this data within precise and clear legal and regulatory frameworks, to prevent the occurrence of any act that would disturb security and public order, or by prosecuting and punishing those who have committed these crimes, the protection of personal data is in fact the protection of private rights and freedoms, So we will deal The content of personal data by highlighting its concept and the extent of the interest it has aroused among the legislator.

1- The Notion Of Personal Data:

Achieving a true definition of personal data need to register this term in international and Arab legislation.

1-1- The concept of personal data in an international perspective:

The first version of the guidelines issued by the Organization for Economic Co-operation and Development in 1980 defined personal data as: any information pertaining to a specific or identifiable natural person, and therefore it is this data that conveys information that may be linked to a specific person to determine their identity.However, this definition posed some problems, as it excluded data that could help identify a person or find and prosecute them, even if they were not linked to their personal identity but linked to any method he uses.

The danger of excluding this category of data, or keeping it out of the legal field, lies in the possibility that it allows the privacy of individuals to be infringed without dissuasion by processing data out of sight of the public censorship due to the impossibility of applying the text which indirectly excludes it.

In this context, the French law of 1978 provided for the protection of personal information by precisely limiting the scope of its application to any information revealing without ambiguity the identity of a person, but this law was modified in 2004 to keep pace with technical changes(Mona Al-Ashkar & Mahmoud, 2018, p. 77),Where it defined personal data as follows: “A personal statement is any information relating to a natural person whose identity is known or whose identity can be identified, directly or indirectly. Or he can be identified by reference to his name, personal identification number and location data. "Data is considered personal as long as it relates to the persons who have been identified, directly or indirectly, and it is also possible to identify the person and determine his identity when his name appears, for example, in a file containing the registration number or telephone number, fingerprint or DNA, it means all information that can distinguish people from others(El-Madawy, 2020).So the French legislator has retained the term personal information, instead of the expression nominal information that it used previously.

The European directive also defines personal data through the text of article 2(European Directive, 2021); first paragraph, as any

information or data likely to identify a specific or identifiable natural person, and whose identity can be identified directly or indirectly by referring to the identification number or by reference to all the symbols related to its physical, physiological, genetic, psychological, social, economic or cultural characteristics.

Consequently, it can be said that through this definition, a set of elements related to personal data can be deduced, as follows:

A-Data or information allowing the identification of a person.

The concept of personal data includes all kinds of information relating to a person, as is the case for personal or subjective information such as the blood group of a particular person, and also includes in this information what the most private data is called(Article8, European directive), which is the data that an Internet user performs when accessing a certain site in order to complete accessing a website, and it is highly sensitive information such as sexual orientation, political opinions and religion. Therefore, the personal data protection act prevents it from being processed in specfic cases, and it is also subject to numerous restrictions.

According to the narrow interpretation, the term personal data includes information relating to the private and family life of a natural person as well as information relating to his company, his activities and even his social behavior.

B-The person concerned:

This is any natural person whose personal data is processed, such as the information contained in the employee's personal file at the Personnel Affairs Department, and the results of the medical examination patient in their medical record(El-Madawy, 2020).

1-2- The concept of personal data in Arab legislation:

Arab legislation agrees to adopt a broad definition of personal data, as the Algerian legislator has set a precise definition of personal data, similar to other Arab legislation.

A-The Algerian rewarded:

He used the term personal data and gave it constitutional protection, since the constitutional amendment of 2020 included in article 47 thereof that: The protection of persons when processing personal data is a fundamental right(Lawn°01-16, 2016).

By enacting Law 18-07 on the protection of individuals with regard to the processing of personal data(Lawn°07-18, 2018), the Algerian legislator has given a precise definition of personal data, and it did well to ensure that this data does not remain subject to interpretations, the rights of which are lost.It defined personal data in its Article 2 as follows: "It is any information, whatever the medium, relating to an identified or identifiable person referred to below directly or indirectly person concerned, in particular by reference to the identification number or to one or more elements relating to his physical, physiological, genetic, biometric, psychic, economic, cultural or social identity.

B- The Moroccan legislator:

He used the term personal data like the Algerian legislator, who defined it as: "Any information of any kind whatsoever, including sound and image, relating to an identified or identifiable person by name of the person concerned"(MoroccanLawn°08-09, 2009).

C- The Tunisian legislator:

It is one of the first legislators to define personal data, since it took the initiative in 2004, four years before the Moroccan legislator and the 14 year old Algerian legislator, where he introduced them. defined as follows: "It is all data, whatever their source or form, which makes a naturel person identifiable or identifiable, directly or indirectly, with the exception of information relating to public life or considered as such by law"(TunisianfundamentalLawn°63, 2004).

It appears through these definitions that the Algerian, Tunisian and Moroccan legislators participated in giving a definition of personal data as any information relating to an identifiable or identifiable natural person"directly or indirectly, with the exception of information related to public life or considered as such by law.

while the Tunisian legislator used the term "data ", just like the Algerian and Tunisian legislators shared the use of the term "physical person", unlike the Moroccan legislator who adopted the term "self "(Ghazal, 2019, p. 114).

What is noted on these definitions is that the definition that Algerian legislator proposed in law 18-07 is almost identical to the definition adopted by the European directive in its second article as explained

previously above, and therefore it was appropriate to the current technological situation.

But the issue with Algerian legislation is that it came late in relation to the opening of Algeria to information and communication technologies, since the Internet was connected to the World Wide Web in 1995, when the personal data of Algerians were accessible to foreign companies active in Algeria and in very sensitive areas such as mobile and landline telephone operators, Internet service providers, etc.This law came at least a decade later than its Tunisian's and Moroccan's (Al-Aidani & Zarrouk, 2018, p. 129).

2- Justifications for the protection of personal data:

With the increase of modern technologies, the risks for the right to privacy have increased and the individual has been restricted in his relations by the control, storage and processing of personal data by means of information such as techniques of surveillance or espionage and compromising the personal data of individuals, and on this basis, several justifications for protection have emerged, which are summarized as follows:

2-1- Expansion of the Internet:

Reality has proven that the most important technologies that control all electronic transactions depend on the Internet, which is no longer safe from the access of any intruder or attacker(Al-Sayed Rashid, 2016, p. 45).

The social network has become one of the best communication intermediaries, since it serves as a communication platform on the Internet that allows users(Al-Anzi, 2018, p. 20) with common interests to join it by creating an account on its site for free, in order to exchange dialogue and discussion.

But despite the role that these networks play in our social lives, given that they have become a benchmark in the digital world(Al-Sayed Rashid, 2016, p. 45), they raise certain concerns about the security and privacy of data contributed by users(Al-Anzi, 2018, p. 20).

The digital age has contributed to the erosion of information privacy due to the recording and dissemination of information and data through the platforms of this network. This information has become public and commonplace after being private, because the situation becomes more

dangerous if it is used for criminal purposes(El-Madawy, 2020, p. 1935).

2-2- The specificity of electronic trading channels:

A person who uses the Internet expects a higher degree of privacy than in the real world, but the situation is different because electronic transactions leave traces and indications in the form of digital records about the sites visited, the problems in question, documents uploaded and goods traded, making a person vulnerable to hacking and then illegal use(Abu Bakr, 2004, p. 398).

2-3- Loss of centralization and control mechanisms in electronic trading channels:

The right to privacy in the context of the digital world acquires a kind of distinction, because passing an effective law to protect against attacks outside the digital world is very easy for the state, but it is not easy in light of the information environment because it has a direct link with a vast virtual world connected to a network The Internet has endless borders, and here the struggle for control of the Internet rages at through the difficulty of controlling the centralization of domain names, website addresses, etc. , which widens the circle of penetration of a right and makes it difficult to protect against any invasion of privacy(Al-Dahbi, 2017, p. 145).

CHAPTER (II):METHODS OF COUNTERFEITING PERSONAL DATA IN THE LIGHT OF THE DIGITAL SPACE

Studies and research on security have shown a series of risks to which personal data is exposed in the virtual world, due to the many applications on the Internet used by individuals without knowing the resulting risks in terms of the disclosure of their personal data and making them vulnerable to violation. Therefore these apps need to be clarified and then abuse images need to be clarified.

1- Electronic Applications That Threaten Personal Data:

A large number of Internet users are unaware of the risks that threaten their personal data, in particular when they use applications for the purposes of communication, entertainment or even shopping.

1-1- The “Cookies” Technical Compass:

Most websites, when visited, place a small file on the hard drive of the user's computer which connects to the private server of the site that has been browsed on the Internet, and this server sends these files to the hard disk of the user's computer when the latter visits any site on the Internet, He keeps a copy of these letters with him.

Therefore, users may be exposed to invading their privacy and collecting information about them, since cookies may know the IP address as well as the mode of connection to the Internet, the sites visited and the type of device, and the most dangerous of all is the data that the user has to enter such as name, email, credit card number, address, etc. It is information(Othman Bakr, sans année, p. 14).

1-2- Social Networking Sites:

Social networking sites have grown tremendously, with its user count in America in 2004 reaching over one million users, and as soon as Facebook opened its doors to the world, that number jumped to 500 million in 2010.

However, many risks befall Facebook users on a daily basis when they submit registration requests through the social network, such as account hacking, dissemination of embarrassing images, difficulty in deleting or canceling the account and in the absence of adequate protection of personal information; it becomes available and can be used for illegal purposes (El-Madawy, 2020, p. 1967).

1-3- Malware On Computer Malware:

Malware takes so many forms that the user cannot identify it. Computer viruses are the most well-known type of malware, so called because they can spread by creating multiple copies of themselves, and worms have the same property. Other types of malware, such as spyware, are named for their effect: spyware transmits information like credit card numbers(https://me.kaspersky.com/resource-center, 2020 at 14:39).

It is called malware because it comes from the words Malicious meaning malicious and software meaning program, and these malicious programs are installed without the knowledge of the affected user in order to collect the most private information as well as gain unauthorized access to information systems.

There are several types of malware; The most dangerous of them is program ngkeyloggi, which monitors the user's keyboard without their

knowledge. It can also find the password and private messages and the most private information of the user and then send them to hackers or scammers in order to analyze them and extracting information of interest to the user(El-Madawy, 2020, p. 1968).

1-4- Email:

Email is a high-level way to send, receive, and forward mail. It also has many advantages that help organize work. Instead of sending paper letters through regular mail, email can be used to send messages. Messages may include certain summaries in the form of files, graphics, or fax pages(Awad & Salman, 1996, p. 1).

Email is prone to so-called phishing, where phishing uses email messages to fraudulently obtain money and collect confidential information for the purpose of attacking such as name,address, password, credit card number(El-Madawy, 2020, p. 1965).

2- The Forms Of Misuse Of Personal Data:

There are many forms of personal data abuse in the digital environment, and the most important of them can be summarized as follows:

2-1- First: Impersonation:

It is considered the crime of the new millennium, due to the prevalence of its perpetration, particularly in commercial circles, through the unlawful use of another personal identity unlawfully, in order to take advantage of the status of that identity or to conceal the identity of the criminal in order to facilitate his commission of other crimes(El-Fiqi, sans année, p. 103).

Plagiarism means that a person impersonates another person, pretending in front of people that they are the same person in order to get their money or do all the transactions in their name, and that may also be for the purpose of achieving various purposes such as applying for a loan or purchasing goods or merchandise on one's behalf, or benefiting from services enjoyed by the injured party, such as services. Health insurance using documents related to the latter, such as a passport or a health insurance card(Khaled Muhammad, 2013, p. 11). Therefore, security procedures must be activated in order to prevent the impersonation of others to enter the computer.

The forms of personal violation can be summarized as follows:

- By entering the exploit protection system, it is possible for the criminal to use a false identity to gain access to restricted areas or to enter the information center building. Use of the method of pretense, whereby the individual wears computer equipment and appears to belong to the place in order to be able to enter.
- Use of passwords, personal number or telephone code (voice for example).

2-2- Unlawful Processing Of Personal Data:

Personal data is the basis of the right to privacy, because it represents, as a whole, the information of the individual, which acquires the status of confidentiality, because the process of unlawful processing of the bulk of the data is the most significant form of violation of this confidentiality by the violation by data controllers of the legal terms and conditions stipulated internally (Abd al-Azim, 2016, p. 92).

Although some countries recognize the principle of freedom of communication and transfer of information, they may adopt the licensing system, as a prior license must be issued to establish or use facilities and devices that are used to broadcast, transfer or process personal information, and some calls this process enters into technology transfer agreements, i.e. the owner of the program has the right to dispose of, operate and use it

In most cases, the owner of the program waives his subordinate rights of ownership "of all or part thereof" to others by selling it or granting a license to exploit it(Abd AlZoghbi, 2006, p. 346), and he always has all copyright protected by law. If others are given ownership of this copy and the right to exploit it, they have the right.

Its use to operate a computer for the purpose of processing information and transferring it within or outside the countryThrough the communication networks, according to the conditions under which he received ownership of the program or the right to use it.

There are several illegal methods of collecting and storing information, including:

- Capture the vibrations caused by the sounds in the concrete walls of the rooms and process them with a computer equipped with a special program to translate them into words and sentences. Monitor, intercept and offload messages exchanged by e-mail.

- Connecting wires in a hidden way to the computer in which the data is stored and illegally accessing the data of others.

Any method to collect data in an illegal manner, such as fraud, scam, wiretapping or recording without legal authorization (Al-Shazly & Kamel Afifi, 2007, p. 296).

The idea of unlawful processing of personal data is based on the question of the violation of the right of individuals to monopolize the processing of personal data, which requires a distinction between data that can be processed by others and those that cannot be(Al-Dahbi, 2017, p. 147).

Despite the difficulty of distinguishing between what is considered personal data and what is not, some believe that the use of computers as data banks would somehow affect the fundamental characteristics that characterize the individual data holder, which poses an unprecedented threat to the personality of the individual Even if complete personal information about the person is not collected through him, the collection of partial information about the personality of the individual can lead to the formation of an approximate image of the person, such as information about his health, professional or financial situation.

2-3- Unlawful Disclosure Of Personal Data:

This issue originates in some professions that depend on data confidentiality, such as the legal profession, the work of banks, where it is assumed that the owner of the profession will maintain the confidentiality of the client's personal data under of the interaction between them(Hisham & Rostom, 1992, p. 195).

Despite the multiplicity of data banks and the large number of stored data, the data enjoy sanctity like other form of privacy, since they include their personal secrets and personal situations in various directions, since preserving them from public is a humanist and moral task.

The Algerian legislator has considered that the illegal use of data is a crime punishable by law, if unqualified persons are authorized to access personal data, or if these data are transferred to a foreign country without authorization from the national and foreign country authority does not adequately protect rights and freedoms(Lawn°07-18).

However, the preservation of personal life or privacy does not prevent official authorities from disclosing the data they store in their programs, but it must be specified here, whether the data concerns the intimate life of the individual as his emotional life or anything relating to his reputation, then the official authorities have no right to publish this information nor do any others, but if this information is closely related to the question raised, there is no objection to disclosing it in order to reveal the truth, because in such a case, the public interest must prevail over the private(Maggabeb, 2009, p. 30).

2-4- Electronic Espionage:

Realistic experience has proven that the danger of using the Internet lies mainly in the its weakness .The means used to protect the transmission of data on the network, as well as the difficulty of gaining access to the perpetrators of the attack.Thus, electronic espionage has emerged as the most dangerous form of attacks that occur within the framework electronic transactions, and this is directly related to the violation of the confidentiality of personal conversations and the essence of correspondence and transactions that take place on the Internet at all levels.

Electronic eavesdropping in the realm of personal conversations can be defined as follows: "The process of eavesdropping or capturing data that is transmitted between two remote devices over the Internet," or by translating electromagnetic emissions from a computer into data, using any of the technical means(Al-Dahbi, 2017, p. 148).

It should be noted that electronic espionage, which is practiced in an outlaw context and practiced by state authorities, is one of the internationally and domestically prohibited methods of violating the rights of individuals, and this in the case where the act of espionage is proven to have occurred without the prior authorization of the court, and this falls within the scope of the abuse of the state's right to the violation of the rights of individuals under the aegis of national or public security.

Moreover, the threat of electronic espionage is greater today than ever before.

Especially in light of globalization and modern technologies, so that they are no longer limited to authorities or intelligence services, but rather the means of espionage have become within reach of ordinary

individuals, especially in the developed countries, unlike Arab countries, where the circulation of marketing spy devices is still difficult and cannot be traded freely and easily(Abdo, 1991, p. 86).

2-5- Deviation from the Purpose of Electronic Processing of Personal Data:

One of the greatest dangers or harms that affect the individual in the privacy of their information, given that it is the most important aspect of personal life when connected to the Internet, is that information collected about an individual for a specific and purpose is initially used when it is stored in the computer.

Many exceed the purpose for which they were originally collected, the gap in the field of processing. Electronic means deviating from the main purpose or the purpose for which the act was performed towards a purpose which is not legally established.

This purpose is represented by the attack on the reputation and the control of the individual, or by the obliteration of the personality, or by the commercial exploitation, or for purposes of pressure or political blackmail, etc. Consequently, all these unexpected uses on all sides lead to harming the individual and reducing his chances of fully enjoying his rights.

On the contrary, it can become a limitation of his freedom in what he wants to do.

It is indisputable that the type and amount of information a person gives about himself varies from side to side, depending on the purpose that prompted that individual to give that information.

On the basis of the foregoing, the legislator has tried more than ever to intervene in order to organize this issue in order to preserve the rights and freedoms of individuals in the face of these threats, whether they emanate from government bodies, which are mostly private institutions and companies. There is no doubt that this legislative protection only takes into account an interest established by the constitution on the one hand and on the other hand allowing the administrative authority to dominate and control the activities which affect the rights and freedoms of people regardless of which party performs the activity(Abd AlZoghbi, 2006, p. 260).

2-6- Hacking:

Some researchers have defined the crime of hacking as "the process of gaining unauthorized access to another's computer through the use of advanced high-tech programs and expertise"(Abu Bakr, 2004, p. 331).

Others have also linked the idea of hacking to illegal data processing, defining it as unauthorized access to a data processing system using a computer(Ibrahim, 2004, p. 242).

Thus, we find that penetration operations are no less dangerous than previous models, since the personal computer has become the most important means available for modern communications between individuals and has become completely used as mechanism for correspondence and transactions issued in the context of electronic transactions.Thus, the idea of hacking a personal computer is based on the transgression of privacy and confidentiality of transactions, and their capture and exploitation for various illegal purposes that inflict many losses on the individual materially and morally. This is what has been expressed in recent years through the so-called black hacks or "black hat hackers".

It is a group of cyber criminals who have adopted the method of penetrating personal computers of individuals by breaking into information systems and databases.unlawfully, modify, distort and destroy data for the purpose of material benefit or moral harm to the victim. These behaviors can often be part of personal, political or religious hostilities, or accomplish such acts on behalf of competing or hostile parties(Al-Dahbi, 2017, p. 148).

Conclusion:

The individual is the backbone of society, and his identity is part of his personality, it is the basis for the acquisition of rights, the approval of duties and the stabilization of transactions. Thus, States have, since their creation, paid particular attention to personal files.

With the development of technology, countries must keep pace with this change and adapt to the characteristics of this digital environment, as the traditional methods of storing personal data have been abandoned and replaced by other new ones, which have become the backbone of the digital economy and development, as it fuels innovation in various sectors, and the processes to address it help to improve performance and

productivity in all sectors of the state, which helps to raise the various challenges faced by the individual or the state.

As a result, personal data in Algeria was, until recently, in imminent danger.

In Algeria and abroad, since 1995, due to the absence of an effective legal system, until the promulgation of Law 18/07, which, although it was a late stage compared to the rest of the Arab countries, but it has been effective in ensuring the protection of this data as it has given a definition similar to that of the European directive, and therefore, for this law to be effective, citizens must be alerted to the dangers that surround their data in light of the digital space, and to make them aware of the different methods of abuse to which they may be exposed when using any of the technological applications on the Internet.

Bibliography:

1- Books:

- Abd al-Azim, M. E. (2016). *Privacy Computing* (Vol. 1). Egypt: Arab Renaissance House.
- Abd AlZoghbi, A. A. (2006). *The Right to Privacy in Criminal Law, A Comparative Study* (Vol. 1). Lebanon: The Modern Book Foundation.
- Abdo, N. (1991). *Computer Security (Virus and Information Piracy and Their Implications for National Security)* (Vol. 1). Beirut: Dar Al-Fikr for Research and Studies.
- Abu Bakr, O. M. (2004). *Crimes résultant de l'utilisation d'Internet.* Egypt: Dar Al-Nahda Al-Arabiya.
- Al-Shazly, F., & Kamel Afifi, A. (2007). *Jaram Computer, Copyright, Artistic Works, The Role of the Police and the Law.* Lebanon
- Awad, M., & Salman, J. (1996). *E-Mail with Windows* (Vol. 1). Jordan: Dar Al-Bashir.
- El-Fiqi, A. I. (sans année). *Information Crimes, Computer and Internet Crimes in Egypt and the Arab Countries.* Modern University Office.
- Hisham, M., & Rostom, F. (1992). *Criminal Code and Information Technology Risks.* Egypt: Library of Modern Machines.
- Ibrahim, K. M. (2004). *Information Crimes.* Egypt: Dar Al-Fikr University.
- Maggabeb, N. (2009). *NaimMaggabeb, Protection of Computer Programs, "A Study in Comparative Law.* Lebanon: Al-Halabi Human Rights Publications.

2- Journals articles:

- Al-Aidani, M., & Zarrouk, Y. (2018). The protection of personal data in Algeria in the light of law 07/18. *the Maalem magazine for legal and political studies, University Center of Tindouf* (5), 129.

- Al-Anzi, Z. (2018). Legal Responsibility for Expelling a Group Member on Social Media, inJordanian Legislation. *Journal of Sharia and Law Sciences, 2* (45), 20.
- Al-Dahbi, K. (2017). The Right to Privacy in the Face of Electronic Attacks, an article published in Professor Al-Baith. *Professor Al-Baith Journal for Legal and Political Studie, 8* (1).
- Al-Sayed Rashid, T. J. (2016). The Extent of Authenticity of Social Communication Text Messages in Evidence, "A Comparative Study". *Journal of Legal and Economic Sciences, Ain Shams University, Faculty of Law* (2), 45.
- El-Madawy, M. (2020, 03 16). *protecting the privacy of user information through controls on social networking sites*. Récupéré sur https://mksq.journals.ekb.eg/article_30623.html: https://mksq.journals.ekb.eg/article_30623.html
- Ghazal, N. (2019). *Protection of individuals in the field of personal data* (Vol. 56). Algerian Journal of Legal and Political Sciences.
- Khaled Muhammad, M. (2013, March). the criminal liability of publishers and technical service providers for misuse of social networks The Social. *Strategic Insights Journal* , 11.
- Mona Al-Ashkar, J., & Mahmoud, J. (2018). *Personal Data and Arab Laws* (éd. 1st edition). Lebanon : Arab Center for Legal and Judicial Research.
- Othman Bakr, O. (sans année). *Liability for Assault on Personal Data via Social Media Networks.* Egypt: Faculty of Law, Tanta University.

3- Websites:

- *https://me.kaspersky.com/resource-center*. (2020 at 14:39, 02 27). Consulté le 07 51, 2021, sur https://me.kaspersky.com/resource-center: https://me.kaspersky.com/resource-center

4- Legal texts:

- Article8. (European directive).
- European Directive, 9. (2021, 06 23). Récupéré sur https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046
- Lawn°01-16. (2016 , March 06). amending the Constitution. *J. n° 14, of March 7, 2016* .
- Lawn°07-18. (2018, 2018 1). relating to the protection of natural persons in the field of personal data processing. *J. C. n° 34 of June 10, 2018* .
- MoroccanLawn°08-09. (2009, 02 23). relating to the protection of individuals with regard to the processing of personal data. *Moroccan law 08/09 relating to the protection of individual J. J. of the Kingdom of Morocco n° 5711* .
- TunisianfundamentalLawn°63. (2004, July 27). relating to the protection of personal data. *Official Journal of the Tunisian Republic, July 30, 2004, n° 61, chapter 4.*