Article history (leave this part):
Submission date: 2024-08-29
Acceptance date: 2024-12-10
Available online: 2024-12-28
Keywords:
Public rights; E-Administrative Control; Right to Privacy; Comparative Law; A.I.
Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Competing interest:
The author(s) have declared that no competing interestsexist.
Cite as (leave this part):
Remaznia , R. (2024). title. Journal of Science and Knowledge Horizons, 4(01), 82-99. https://doi.org/10.34118/jskp.v4i01.3853

Journal of Science and Knowledge Horizons
ISSN 2800-1273-EISSN 2830-8379

Legal Safeguarding of Digital Rights and Liberties Under The E-Administrative authorities (Comparative study)

Belarouci Amine *, Serbah khaled

1-Comprative Law Laboratory, Hassiba benbouali University chlef (Algeria), Phd researcher, a.belarouci@univ-chlef.dz,
https://orcid.org/0009-0005-7367-2283

2-Lecturer A, Hassiba ben bouali University chlef, k.serbah@univ-chlef.dz,
https://orcid.org/0009-0005-1899-7966

Abstract:

The tremendous development we are experiencing is due to the world of digital technology. the authorities were forced to develop their administrative control methods to become digital and instantaneous as well, In order to keep pace with the terrible daily developments in this field and the technologies associated with it, especially A.I Systems, which has developed the technologies used electronically so that criminal thought has also developed with it in the field of software and artificial intelligence. The state cannot achieve full protection for this digital environment, personal data and the privacy of individuals without resorting to administrative control methods that are in line with this field. Thus, traditional administrative control turns into electronic administrative control that aims to monitor the exercise of public rights and freedoms in the digital environment, which has also evolved into digital public freedoms such as social media, electronic data exchange platforms and digital platforms for public administrations and bodies. These entities are exposed every minute to coordinated attacks from internal and external sources, which requires the authorities in France and American United States to protect the right to privacy of individuals on the one hand, and to protect public order on the other hand. This is the goal of our study by analyzing the legal texts issued in the both countries comparative law.

***Belarouci Amine**

I- Introduction :

The world is experiencing a successive transformation in the way individuals participate in political life, due to Digital Platforms such as Facebook, LinkedIn, WeChat, Twitter, AirTask, Uber... and others, Which are no longer less important than traditional institutions in how we organize our professional and social lives. This Digital environment have also become one of the most important topics that we participate in public debate and attract the attention of political action, in advanced industrial societies, whether in authoritarian states or even emerging democracies in the developed world.

Since the distinction of the authorities and their enjoyment of the powers of electronic administrative control is based on restricting or preventing the rights and freedoms of individuals in exceptional cases specified in the constitution, the legislator had to issue restrictions that limit the arbitrariness of these authorities, the most important of which is adherence to the principle of legality. and adherence to the constitutional and legal texts and regulations regulating these authorities, without neglecting the most important guarantee of rights and freedoms, which is the constitution, the protector of these freedoms. Administrative oversight is considered one of the most important functions of the public authority that distinguishes the state through the administrative authorities that enjoy the privileges of the public authority by imposing the preservation of public order in its three meanings: public health, public tranquility, and public security.

In order to maintain the stability of the state. however, the actions and behaviors of the state may have a negative impact; on public liberties called for by international and national treaties at the same time, and this is what the modern state aspires to, as it controls them according to legal rules and regulations. It imposes restrictions on the activities of the administrative police, whether in normal or exceptional circumstances, and in the latter, liberties become threatened and more affected than in normal circumstances, due to the broad powers of the administrative police by virtue of exceptional legitimacy. In this regard, the question arises about the extent of the ability of administrative police agencies to achieve a balance between achieving public order and restricting individuals in exercising their rights and liberties.

Therefore, Protecting public rights and liberties in the smart digital environment as well as the right of Privacy in this digital environment , of that

relies on A.I systems is the primary concern of all countries, regardless of the nature of the prevailing system in them, whether they are developing or developed countries.

With the expansion of the use of digital and electronic media, it has become imperative for these countries to develop their traditional methods of administrative control, and this is what we have seen through our analysis of the texts of American and French laws in this field, given that the latter often leads to restricting individual freedoms due to justifications imposed by the public interest, and although the individual has the right to enjoy some rights in the digital environment, this enjoyment is not absolute, and without any controls that limit the enjoyment of these rights so that this does not affect the rights and freedoms of others and the public security of the state, as well as commitment to the general frameworks and commitment to the controls specific to the use of artificial intelligence systems through which they are practiced, these freedoms are what distinguish freedom from chaos and make this use a civilized behavior.

On the one hand, there are individuals and groups or companys who regard themselves as digital rights activists, practitioners, and researchers. Collectively, they have made highly significant, threshold contributions in drawing our attention to new locations, frameworks, and kinds of rights that are coalesced in relation to digital technologies. Key issues such advocates have emphasised include: Internet filtering; Internet shutdown; the so-called “net neutrality” debate; the threats to freedom of expression from copyright law reform and enforcement. Institutional recognition of, and support for, such digital rights has tended to come first from organizations focussing on digital technologies, What are digital rights and why do they matter now? How did the laws issued in France and Egypt protect public order on the one hand, and how did they allow individuals to enjoy their freedoms in the digital environment? Such as Internet governance organizations like the Internet Society and its various regional chapters. A criticism of such digital rights groups is that their work is not so well connected to conventional or “traditional” human rights issues.

To answer the question raised by the topic under our study, we will rely on description and analysis, Also to simplify concepts and analyze legal texts in this field, we relied on the analytical approach. We also used in our study the comparative approach between French and American (US) legislative texts. which includes the most important legal aspects of this topic within two main

topics:

1- **The E-Administrative Control authorities in the digital environment.**
2- **Public rights and liberties in the digital environment.**

II - The E-Administrative Control authorities in the digital environment.

The biggest challenge for the authorities responsible for administrative control in the digital environment is the equation of maintaining public order on the one hand, and maintaining a greater degree of individuals exercising their public rights and liberties in the digital environment. That is why the legislator worked to move administrative control to the information network itself, and was keen to impose and strengthen his powers in order to maintain public security, through the means available and regulated by an arsenal of laws developed for this purpose [1].

II -1 The concept of electronic administrative police control.

Imposing the development of the concept of public rights and liberties and the environment in which they are practiced, the administrative police must also develop its means and objectives in order to keep pace with this tremendous development in the digital environment in which these rights and liberties are exercised, so as not to violate one of the most important constitutional principles, which is not to infringe on the individual's right to communicate with others. Or publishing or even receiving information. Since administrative control is the essence of public authority in the state due to its close connection to the public rights and liberties of citizens directly, and its use of methods and procedures that prevent threats to public order, and in view of the terrible technological development that has paved the way for the existence of a digital environment in which many rights and liberties are exercised, all of this is imposed on the police authorities. The administrator must develop his concept and methods as well. What is electronic administrative control?

II -1-1 Definition of the E-Administrative police control.

Electronic surveillance is considered one of the most important sources of research and investigation that is often relied upon for investigation, such as social media crimes, especially cybercrimes that threaten public order, and various administrative websites on the electronic information network, and from it came the electronic administrative police as a new idea as a result of modern studies in administrative law. After being influenced by electronic development, where did

it become referred to in comparative legislation with this description? In order to define electronic administrative control, we discuss its definition among jurists, then its definition in comparative legislation[2].

To strengthen administrative control over public rights and freedoms in the digital environment, the European Union e-government law has identified three policy options, which we will briefly describe below[3] :

Option 1: Regulate and rationalize administrative procedures This option aims to update the 2016 proposal in the context of digitalization, reflecting the legal rules on digital technologies and data that have recently been adopted, as reflected in French legislation issued starting in 2016, and the use of digital tools by the public administration represented by electronic surveillance authorities. The option focuses on individual redress mechanisms in the context of administrative procedures that often lead to administrative action against individuals by restricting their freedoms in the digital environment.

Option 2: Regulate administrative activities in the field of administrative control. Rather than focusing on the redress stage, this option regulates the rights to information and procedures. A similar approach has been taken in France as part of the concept of digitally ready legislation.

Option 3: This option is summed up in a "EU Digital Governance Code". Soft legal instruments to restrict rights and freedoms could also be an alternative to legally binding regulation. This would take the form of a "Code to strengthen the EU's digital governance", similar to the proposal discussed in the 2016 Impact Assessment of Electronic Surveillance Mechanisms, where digital aspects would have to be taken into account. Examples of this approach can be found in the French or Spanish Charter of Digital Rights and the 2021 European Declaration of Digital Rights.

a- Jurisprudential definition.

In light of the modernity of the concept of electronic administrative police, jurists did not address a definition that prohibits and comprehensives this type of control, but most of them agreed that electronic administrative police is a mechanism that allows the authorities to try not to prevent the use or secure the right to access, publish, or use digital media via computers and devices. Other electronic and communication networks and using them in a way that does not expose the public order to danger[4].

Jurists currently agree that electronic administrative control, and in the era of comprehensive digitization of everything, requires the legislator to work to adapt laws to preserve basic rights and keep them in line with the terrible development taking place in the digital space, especially digital individual rights, which are closely linked to the right to demonstrate and express, and the right In privacy with the use of computers, phones, and smart devices on the one hand, and on the other hand, securing the digital space to maintain public order, and this is what is imposed by the race of individuals to use the terrible use of everything digital and electronic to the point of addiction, so to speak.

b- Legal definition.

The General Chamber for Legal Studies of the European Union has conducted legal studies, which are considered the legal basis, so to speak, in order to move towards a third generation of administrative police through digital management that aims to protect privacy in the digital field and media. European countries have advanced in advanced stages compared to other countries. In this field, it was helped in this by the legal arsenal in the field of public communications that the European Union countries successively initiated in the middle of the twentieth century.

Also the Law 78-12 was issued in France regarding computing, file processing, and liberties. It indicated that it is the responsibility of the state to protect the personal data of citizens entered into computers, which established the basis for exercising liberties using various technological means in accordance with specific legal frameworks prepared for that purpose[5].

Then, in the year 1981, the European Council issued Convention No. 108 regarding the protection of individuals during the automated processing of personal data, adopted within the framework of the European Council on January 28, 1981, and supplemented by the Additional Protocol of 2001, where it was agreed to expand the powers of the administrative police in this field and grant it broader powers in The field of processing cross-border data flows under ETS No. 181. Signed by member states on 11/08/2001, it is noteworthy that this agreement entered into force in all European countries on 07/01/2004.

"***The authority of the electronic administrative police is not new or parallel to the traditional authority of the administrative police, but rather constitutes a real extension of it in the digital space, and reflects the presence of the parties***

and the basic objectives of administrative control, but in a new and different guise, with an electronic suit and an artistic and programming character."[6]

II -2 - Means and mechanisms of the electronic administrative police.

The state uses specific means and mechanisms to maintain its electronic security, given that cybersecurity is at the forefront of concerns, whether through the activity of individuals by tracking and monitoring their activities, or by tightening electronic security measures to avoid cybercrimes that threaten its economic and social security.

II -2-1 E-Administrative police means.

Despite all the numerous important advantages of electronic administrative police over the activity of individuals and their means of communication on the Internet, whether through preventive monitoring of information or administrative blocking of it, a jurisprudential debate has been raised about its pros and cons or whether or not to accept such control. Especially since there are those who see the illegality of this system because it affects individual rights and liberties that are exercised digitally through electronic means and devices, while others see the necessity of the existence of this system due to its importance in combating organized and cross-border crime that is carried out electronically through social media and other networks. In order to curb its spread and limit its spread.

a- Preventive monitoring of information.

Electronic oversight is considered the most important challenge for the interests concerned with cybersecurity through research and investigation. Various administrative authorities also exercise their supervisory duties towards many electronic activities in the electronic reality, in order to preserve the security of the state by securing all commercial and economic operations that occur in the digital environment, because, by its electronic nature, it requires... This type of control is to maintain the security reality or information security, which is considered the backbone of cyberspace[7].

Electronic surveillance is also defined as the process of conducting an investigation that is conducted surreptitiously, in a manner that violates private conversations, ordered by the judicial authority in the form specified by law, with the aim of obtaining non-material evidence of a crime whose occurrence has been

verified. It includes, on the one hand, eavesdropping on the conversation, and on the other hand, preserving it using devices designated for that purpose[8].

Here we must differentiate between information security and cybersecurity. Information security is a science that is concerned with preserving the confidentiality of information and data that the Internet user connects with various communication networks, electronic platforms, or specific applications, from any attempt to breach, espionage, or seize them, which requires working with systems. Specific custom protection for data, applications and operating systems.

Cybersecurity aims to protect systems, networks, and various electronic devices from electronic and digital attacks. More simply, it is equivalent to creating a firewall that prevents any attempt at hacking or espionage.

From the above, we conclude that information security is broader in scope than cybersecurity, as the latter focuses on protecting systems and networks from electronic threats, while we consider information security to be broader in scope and includes protecting all information and data, regardless of their type, regardless of the media used.

b- Administrative withholding of information.

The administration resorts to several different means to ensure the security of sensitive information related to the security of the state in various political, economic and military fields in particular, in parallel with the spread of electronic governments and the requirements of digitalization, to facilitate citizen transactions in the first place and ensure access to real-time and confirmed numbers and statistics, to support various forward-looking studies for offices and agencies. Government, so it was necessary to think about the legal mechanisms that allow the state to withhold information that is of a sensitive nature, or that is pursued by parties hostile to the state in order to use it for purposes that affect the security of that state [9].

Until we began to see that advanced and current wars were reduced to the websites of vital areas of states. The latter are threatened all the time by cyber attacks from overseas and from various regions of the world that threaten the security of the state in the first place, especially if the websites of ports, banks, and various security sites are disabled. As well as the government, which works to facilitate the work of users, which requires each country to secure its sites and

ensure the periodic blocking of everything that is sensitive in various important electronic data.

c- Periodic preventive inspection:

The state services responsible for controlling electronic services and the digital space work to grant the competent police authorities, represented by the Administrative Police, to allow them to search the database of any website that uses a server identified with the international number of that country, according to a specific periodic schedule in order to prevent the occurrence of cyber attacks that would affect on that country.

The work of these departments is based on a specific encryption through which any post, communication, or audio or video message is recorded, in which a keyword is mentioned that is predetermined in the database of the programs used for electronic monitoring. In the event that any warning is recorded in this regard, these departments work. On periodic and continuous inspection in order to prevent any threat to public order, which was introduced by the European Parliament in Framework Resolution 2056 of 2002. It was then amended by issuing Regulatory Law No. 2065 of 2023 under the name of regulatory oversight of the technology giants in the world. It was implemented starting from the first of February 2024 on all digital services in all countries of the European Union[10]. Its aim is to create a safe digital environment in which all public rights and liberties are exercised for all individuals away from any threat to their personal data on the one hand, or danger threatening the public order of countries. On the other hand, concerned with implementing this law. All platforms are obligated to include the conditions for using electronic platforms in this law as a mechanism through which public order is adhered to.

In this regard, we see that accessing websites and forums on the electronic network for the sake of maintaining public order, does not allow the competent authorities to view the personal data of the users of these sites and forums, and to track the buttons that they press through the computer or smartphone, is similar to violating the privacy of others without permission. Judicial permission allows this.

II -3 Limits of the legal regulation of the E-Administrative Control.

Despite all the procedures in place in the digital environment through various electronic platforms, the authorities concerned with controlling the use of services provided by electronic windows on the one hand, and the great dependence of countries on digitization and their management of their facilities through electronic government on the other hand, which makes these countries provide a legal environment It is robust to ensure that the interests charged with securing these electronic networks exercise the protection of the information provided by this technology, especially since it affects the security of countries economically and even militarily. Even nuclear reactors are managed with high-tech electronic systems, which raises the ambitions of fighting everything that disturbs the security of these countries.

The American experience in this field is considered pioneering compared to other countries in the European Union and China, as the American legislator works on two parts: the first is technical standards for how to practice electronic administrative police, and the second is legislation and oversight.

a - Technical standards for electronic administrative control.

The National Institute for Technical Standards and Technological Measurements (NIST) was established in 1901 as the first measure to encourage innovation and industrial competitiveness, and to unify electronic surveillance systems and collect information based on what is available from the systems used in military computers, all of this to enhance and develop military and economic security, to be amended in 1988. Its tasks are by directing its programs to improving the quality of life for individuals, through planning to make technology available and use it in a purely civil manner[11].

After the September 2011 bombings in New York, the United States of America worked to strengthen its legislative arsenal, in order to facilitate the work of the competent authorities by granting them the necessary immunizations to access media users' accounts and programs related to chat and file sharing, and after fierce battles between the US Congress, represented by the Senate. The American Council and the House of Representatives on the one hand, and on the other hand the organizations and associations concerned with human rights

b- Legislation and oversight:

The package of legal texts is considered a legal shield through which state authorities work to enable administrative control to access the information network, in order to work to protect public order on the one hand, and to try to provide a safe environment for exercising digital rights. If we find that in the year 2023, the percentage of young people represented more Of 79% of Internet users, their average age is between 15 and 24 years[12], not to mention the fight against electronic crime, which has become widespread and spread like wildfire, especially if we know that most of the criminals in this space are from outside the countries where these crimes are committed and because of the advanced software used by them. They are called pirates, considering that they seize everything valuable through their intrusions and espionage into electronic and bank accounts...etc [13].

In the state of Philadelphia in the United States of America, the local government issued a law in 2009 that clarified the conditions for selling software related to artificial intelligence, where artificial intelligence was defined as: two types, the first is super-intelligent, which is used in sensitive sectors such as defense, space and medicine, and the second type is limited intelligence, which is commonly used in economic companies, various departments, universities and even the media. Only the sale of these sensitive software is subject to strict control, while manufacturing and innovation are among the basic freedoms of the American citizen. [14]

Compared to Algeria and the Arab countries, we see that the legislative package for electronic protection in this field in European countries and the United States of America is very advanced and keeps pace with criminal thinking in this field, especially in protecting the personal data of individuals on the electronic network, and securing government websites from cyber attacks. Not to mention the use of A.I systems in the field of monitoring publications and ideas that are marketed via the Internet, as these countries require major companies in the field of Internet servers, This is what the Algerian legislator addressed through the law N° 2018/07 relating to the protection of natural persons in the field of processing personal data [15].

III - Public rights and liberties in the digital environment.

The right to be left alone or the right to live in solitude signifies a desire to distance oneself from the noise and distractions of one's surroundings, including one's professional environment and even society, in order to enjoy some peace

and quiet and to do as one pleases away from the eyes of others, which is something that individuals often yearn for. Even for the most prominent figures in society who are constantly pursued by others seeking to know their activities, this fundamental right to privacy has been defined by the Canadian Supreme Court as follows: "a narrow scope that allows for personal benefit, within which private choices are decided according to their nature".[16] .

Human rights are now universal, indivisible and inalienable. In our digital age and artificial intelligence, websites provide opportunities to better exercise them but also create risks to their exercise and protection. For example, digital spaces provide enhanced means, speed and scope for people to exercise their freedom of expression, but they also exacerbate privacy risks by enabling unprecedented collection and storage of personal data and the risk of its being breached or surreptitiously accessed.

III -1 - The digital environment is a new space for exercising rights under the right to privacy.

With the successive eras of human rights, the process of human rights has witnessed a significant development in its concept and elements, reaching the multiplicity of its generations, as digital rights have become such as the right to publish or create digital content through the right to use a computer or any other similar device, or software and networks without any restriction on that activity. The right results from or is linked to many other rights, such as the right to freedom of opinion and expression, the right to privacy, the right to circulate information, the right to scientific knowledge, and other rights and liberties [17]. The concept of public liberties has developed with the development of the means used by individuals and those surrounding them in their environment, so that Social media has become an incubating environment for these liberties and their practice away from any friction or restrictions, especially political and religious liberties, where forums and meetings for multiple entities, parties, or sects are now being held in closed chat rooms on various applications in cyberspace.

The evolution of the right of privacy in the United States can be traced back to the First, Third, Fourth, Fifth, and Ninth Amendments to the US Constitution to protect freedom of expression and individual rights against unreasonable searches and seizures by the Government, Although the U.S Constitution does not explicitly focus on protecting personal information, safeguarding individuals

from unsolicited invasions was integrated into its jurisprudence by penumbras [18].

The rapid development of technological advancement in recent years has profoundly impacted the right to privacy in profound ways. The advent of the Internet, mobile phones, social media platforms, and sophisticated big data analytics has led to unprecedented volumes and granularity of individuals personal information being collected, analyzed, and even shared without their consent. This has redefined what is public and what is private in the digital realm. In addition, the proliferation of surveillance technologies, facial recognition systems, and the Internet of Things (IoT) has made maintaining individual privacy even more complicated [19].

The media and communication, in addition to the Internet, play a decisive role in embracing various human activities, as it is the easiest and best spatial context for exercising various public rights and liberties, so that messages are exchanged indicating the date and place of the intended meeting, such as websites, portals, forums, chat rooms, and the fast information road. [20], Also do not forget the role that the Internet media played in communications between individuals of peoples who carried out revolutions in order to change the regimes of government in their countries, such as Tunisia and Egypt...etc., and even in preserving the regime from the dominance of coup plotters, as happened in Turkey in the summer of 2016.

An example of a digital privacy violation is: "the 2022 case of **BETTERHELP**, an American mental health platform that provides online counseling and therapy services via web or text message, sharing its customers' personal data with **FACEBOOK**. On March 2, 2023, the Federal Trade Commission issued an order proposing to prohibit **BETTERHELP** from sharing consumer health data with third parties and to pay $7.8 million to consumers to settle allegations of exposing sensitive consumer data to **FACEBOOK**, **SNAPCHAT**, and others. The FTC alleged that **BETTERHELP** collected health status, history, IP addresses, and email addresses from consumers while making repeated promises to keep this information private, and that the platform received numerous complaints from 2013 to December 2020, yet continued to violate its privacy promises and exploit consumers' health information to target them and others with advertisements about the service. [21] "

III -1-1 Rights and freedoms in the digital environment are protected by international law.

The evolution of technology has outpaced the evolution of privacy laws, necessitating a fundamental reassessment of legal frameworks to effectively address emerging challenges. Traditional legal concepts and approaches, such as consent and prior notice, have proven inadequate in the context of current data systems and processing technologies. The need for a modern legal framework is evident in the current globalization of data flows, which transcend national borders. Based on all this, the European Union took an important step by enacting the General Data Protection Regulation (GDPR) in 2018. [22]

Generations of human rights have followed since the Universal Declaration of Human Rights. The first generation of human rights, represented by civil and political rights, is considered the founder of the consolidation and development of the concept of human rights. The second generation, represented by economic, social and cultural rights, appears, then the third generation, which concerns collective rights in the environment. And development, so that the fourth generation currently living will come, which is the generation of digital or electronic rights.

The notion of rights has a long, complex, and rich set of histories, based in politics, law, philosophy and ethics. As we celebrate the 77 th anniversary of the United Nations Universal Declaration of Human Rights (UNDHR), the idea of rights is still strongly contested from a wide range of perspectives. We take a broad, pluralistic approach to investigating digital rights that encompasses elements such as [23]:

• Rights explicitly set out or recognized in law, policy, and regulation; rights ideas and practices developed and asserted by a wide range of movements, organizations, and individuals.

• Rights that extend beyond traditional frameworks of states, national, regional, and international communities of countries. The recognition of certain rights is shaped by cultural, social, political, and linguistic dynamics, as well as particular contexts and events.

We can define the term digital rights and freedoms as: the right of individuals to facilitate access, use, create and publish digital content through the use of electronic means, computers and devices, or software and communication networks without condition or restriction. This right is linked to another group of rights and freedoms, which are: freedom of opinion, the right to expression, the right to privacy, the right to circulate all information and knowledge, and other

rights and freedoms. The trends that addressed the definition of a prohibitive definition of digital rights did not agree. Rather, they tried to define the specific meaning of these rights, such as clarifying the elements specific to these rights and the benefits they contain. This is due to their recent acquaintance with this type of rights, and this phenomenon has rarely been delved into in depth with contemporary studies, but most of them define digital rights as: "the right of every individual to access, use, create and publish digital content, and use computers or other devices, software or communication networks without any restrictions." [24] From here are generated many other rights and liberties, such as freedom of opinion and expression, freedom to exchange information, the right to privacy, the right to development, knowledge, and other rights and liberties.

Digital rights are also considered an extension of human rights in reality, and they are rights that have gained recognition and legal protection from international law in multiple conventions and treaties, which stipulate in their entirety: (Digital rights are the same as the rights enjoyed in real life, and must be protected along with the environment in which they are exercised). Among other things, digital rights are an extension of human rights in reality. We previously concluded that digital rights are based on four basic principles: availability of the medium and the right to privacy, freedom of expression, and freedom to develop and innovate.

III -1-2 Characteristics and advantages of digital rights.

Since the international resolution was issued by the Human Rights Council in 2013, which recognized digital rights and their use in the digital space, and that they are no less important than previous generations of rights and liberties, these rights and liberties have been characterized by the following:

-Firstly, rights are of recent origin and have immediate effect.

Digital rights are modern rights due to the modernity of the revolution taking place in information technology, and the use of data imposed by the digital space and the essential feature it has given to current contemporary life, where the individual has become indispensable with his personal computer, or smartphone device, which means that he is connected around the clock. In this digital virtual space. In particular, it has the benefit of shortening the time required to obtain information, or bringing it closer to the distances between individuals, no matter how far they are, through their visual communications. These are rights closely related to the international information network.

-Secondly, purely legal rights.

There are deep-rooted natural rights that are linked to human nature, and they are inherent rights, and there are legal rights recognized and recognized by the International law, which is their source. Therefore, digital rights are considered legal rights whose origins were recognized and given a legal basis for exercising, protecting, and preserving them from any interference by any party, and perhaps the successive legislations internationally and nationally for Protecting digital rights is the most prominent evidence of the law's recognition of their origin and protection, and how to codify their uses away from suspicion, and the attempt to distance their users from electronic crimes that also appeared simultaneously with the boom taking place in this field [25].

The right to digital privacy has been enshrined in various international and regional conventions, including:

- United Nations General Assembly Resolution 68/167 [26] on digital privacy, which was adopted by the Assembly without a vote in December 2013, through which the protection of rights in the digital space was enshrined.

- The report of the High Commissioner for Human Rights, which highlights the effects of A.I technologies on the exercise of the right to privacy and related rights and other human rights.

- European Regulation No. 679/201 6on the protection of natural persons with regard to the processing of personal data issued by the European Parliament on 27 April 2016 and the free movement of such data (GDPR) [27].

-Thirdly, rights of a universal nature.

The connection of digital rights with the International Information Network and the rapid global spread it produces has given it a global character, especially with the increasing desires of individuals to use and satisfy their needs for the right to communicate, browse, publish, correspond, and create blogs with various goals, which is shared by all individuals inhabiting this world, no matter how numerous and diverse they are. Their languages, religions and ethnicities, but the goal of the right to use the information network is the same [28].

-Fourth, digital rights are fundamental.

The Human Rights Council resolution on digital rights included a description

of them as fundamental human rights, and not secondary rights or entertainment...etc; This is a description that the nature of digital rights is consistent with due to the urgent need for them by individuals, until they have become intertwined in all aspects of life. The human being and his companionship, which is what international institutions and companies in this field have noticed in order to attract the interest of users of the network.

III - 2 Legal rules to protect public liberties in the digital environment.

In the past, defending freedom of the press was a cry indicating an inevitable development to defend the human right to information and exchange it quickly. However, with the development of time, the methods used in this regard have evolved. The legal texts used before the advent of the Internet, including the digital environment, require a fundamental modification in the concept. Even in the legal means available to protect the right to information and the right to communicate and exchange personal information, it is also protected from any theft or restriction, as it is a basic right, which is the right to privacy.

III–.2.1-Legal definition of public communications on the Internet.

The French legislator took the initiative in this regard, as Law 575/2004 related to trust in the digital economy was issued, stipulating in its first article the creation of a new category: "Public communications through various electronic means," which includes[29]:

-audio-visual communications.

-public communications on the Internet.

In Article Two of this law, the legislator defined public communications on the Internet as: everything that is placed at the disposal of the public or a specific category thereof, through electronic communications, including signs, signals, writings, images, sounds, and messages of any kind that do not acquire the character of private correspondence [30].

From the above, we see that the French legislator divided this digital content of public rights and liberties in the digital space into a general nature that includes posts on various blogs, and a purely private nature that includes emails and voice messages on various applications and even video ones, which are tools that can be accessed after entering with a password. Specifically, these messages are exchanged in a cyberspace protected by the highest levels of protection and

periodic encryption with an automatic update that is displayed to subscribers to this software on the digital space.

IV - Conclusion

Recent years have witnessed unprecedented growth and development in the use of the Internet, revealing emerging opportunities and threats. The coming years are likely to present many of the same risks and opportunities, as new complexities emerge regarding the regulation of the online sphere, both enabling and threatening freedom of expression and access to information. From all of the above, it is clear to us that the new generation of digital rights and liberties, and whatever the risks that arise from practicing them in the digital environment saturated with A.I Systems, do not allow states to spy on and use the data of information network users, and track their paths and areas of interests on it, because here we are faced with Negative use of A.I technology, which requires more efforts by the legislator to protect these digital rights and liberties as they are a new generation of human rights. We also found the following:

-Digital rights have developed and gained international recognition, starting with the United Nations through the World Council for Human Rights, and in return, national legislation, especially European legislation, for example in France, has become more in line with the recommendations of international organizations in this field.

-We found that in this two countries there is a lack of adequate national legislation or enforcement, weak procedural safeguards, and ineffective oversight, all of which contribute to a lack of accountability for arbitrary or unlawful interference in infringements on the right to privacy.

- It also becomes clear to us clearly the extent of the direct impact of administrative police authorities on public liberties, given the flexibility of the idea despite its constitutional and social importance, and the provision of the largest possible number of legal and political guarantees to protect this new generation of liberties.

- Any attack that on thos digital rights may occur by administrative police agencies must be confronted with judicial force, because it has been proven that there is a relationship of complementarily, agreement, and connection between them, as is evident through their exercise of their duties and powers within the limits set for them by law, so that administrative police agencies can not Tyranny,

violating the liberties of individuals, and not exercising liberties absolutely so as not to prevail in chaos and unrest that are difficult to control and lead to disruption of public order.

-New technologies are constantly emerging and creating new threats. Important steps must be taken every day by officials, digital rights activists, the international community, and the courts, to ensure that the Internet remains a source of knowledge and development, and that it becomes a safe space for all users to access their full rights.

-There is a clear and urgent need for vigilance in ensuring that any policy or practice in the field of surveillance complies with international human rights law, including the right to privacy, by establishing effective safeguards against abuses occurring in this area.

- The dialectic of maintaining public security in the digital environment and leaving a wide margin for individuals to enjoy their digital rights and freedoms has made the legislator's task difficult. States' laws and policies must reflect their own national practices to ensure full compliance with international human rights law. Where interferences and deficiencies exist, States should take steps to address them, including by adopting a clear, precise, accessible, comprehensive and non-discriminatory legislative framework. Steps should be taken to ensure effective and independent oversight systems and practices, paying attention to the right of victims to an effective remedy.
- The above recommendations provide a roadmap for defining the future of privacy law. International collaboration, exchange of legal and judicial texts and interpretations, and commitment to public awareness among individuals are fundamental principles in shaping a secure privacy landscape that may balance the benefits of technological media with the protection of rights and freedoms.

***[1] -Zainab Muhammad Jamil Al-Dannawi**, Legal Protection of Privacy on the Internet in Light of International and Internal Efforts, article published in the book of the Forum of Proceedings of the International Conference on Privacy in the Information Society, King Faisal University in the K.Saudi Arabia 2019, p. 23.*

***[2] - Mohammad Taher,** Digital Liberties (Basic Concepts),P58.*

***[3] - Lenka Jančová and Meenakshi Fernandes** , Digitalisation and administrative law European added value assessment, Published on the site of EU Parliement, European Added Value Unit PE 730.350 – November 2022.*

*[4]- **Ahmed Mohammad Fathi Al-Kholy,** Civil Liability for the Unlawful Use of Artificial Intelligence Applications, an article published in the Journal of Jurisprudence and Legal Research, Faculty of Sharia and Law in Damanhour, Arab Republic of Egypt, Issue 36, October 2021, p. 228.*
*[5] - **Nicolas Ochoa,** Personal data law, a special administrative policy. Law University Paris 1 Panthéon-Sorbonne, 2014, French. ffNNT: ff. fftel-01340600f.*
*[6]- **Convention No. 108/1981** of the Council of Europe on the protection of individuals during automated processing of personal data, adopted within the framework of the Council of Europe on January 28, 1981, and supplemented by the Additional Protocol of 2001.*
*[7]-**Eduard Lioe Kim,** Armed Forces in law enforcement operations, the German and European perspective, springer, Verlag, Berlin Heidelberg, 2010, p 52 – 57.*
*[8] - **KONOBEEVSKAYA, IM** (2019). "Digital rights as a new object of civil rights: Proceedings of Saratov University." New series. Series "Economics". Management. Right, 19(3), pp.330-334.*
*[9] - **https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/use-and-disclosure** Accessed on 24-04-2024 at 22 :40 pm.*
*[10] -**https://www.iberdrola.com/innovation/what-are-digital-rights** Accessed on 23-04-2024 at 02.pm*
*[11] -**https://www.nist.gov/director** National Institute for Technology Standards and Metrology, Accessed on : 03/25/2024 at 19:03*
*[12]- **Safety of children and youth on the Internet**, a study published on the United Nations website, **https://www.un.org/ar/global-issues/child-and-youth-safety-online**. Accessed on : 23/04/2024 at 19:05 .*
*[13]- **Mansour Aqeel and Ali Qasim,** The Internet and Security Dimensions, Center for Police Research and Studies, Dubai, United Arab Emirates, January 1996, p25.*
*[14]-**Hildebrandt Mireille**, « Legal Person hood for AI? », Law for Computer Scientists and Other Folk (Oxford, 2020; online edn, Oxford Academic, 23 July 2020).*
*[15]- **Law 18-07** of June 10, 2018, relating to the protection of natural persons in the field of processing personal data, Official Journal of Algerian Republic, No. 34 issued on June 10, 2018.*
*[16] - **Mohammad Taher**, Digital Liberties (Basic Concepts), Foundation for Freedom of Opinion and Expression, 1st Edition, Cairo Egypt, 2013, p. 5.*
*[17] - **https://www.ohchr.org/en/topic/digital-space-and-human-rights**. Accessed on 24/04/2024 At 22:07. pm*
*[18] - **G.Haywood, H Suvineetha, L.McKee, Privacy**, Harm and Non-Compliance from a Legal Perspective, Journal of Cybersecurity Education, Research and Practice Journal of Cybersecurity Education, Volume 2023 Number 2 Article3, Available at: **https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/3***
*[19] - **Oluwatosin Reis**, Privacy Law Challenges In The Digital Age: a Global Review Of Legislation And Enforcement, International Journal of Applied Research in Social Sciences, Volume 6, Issue 1, January 2024.P74.*
*[20]- **T. Vedel,** «Les politiques des autoroutes de l'information dans les pays industrialisés : une analyse comparative», Réseaux, 1996, n° 78, p. 11-28.*
*[21]- **N. Wetsman,** Mental Health App Privacy Language Opens Up Holes for User Data, The Verge (May 4, 2022, 11:30 PM), **https://www.theverge.com/2022/5/4/22985296/mental-health-app-privacy-policies-happify-cerebral-be:erhealth-7cups.***
*[22]- **R. Debbarma**, (2023). The changing landscape of privacy laws in the age of big data and*

surveillance. Rivista Italiana di Filosofia Analitica Junior, 14(2), 1740-1752.
***[23] - https://news.un.org/ar/story/2013/12/192412** Accessed on 22/04/2024 at 22:40 United Nations news website.*
***[24]- Fedorenko, NV & Hejgetova**, SE (2019). Digital Rights in Civil Legislation of Russia. In Institute of Scientific Communications Conference,Springer, Cham.*
***[25] -Mekamcha Ghaouti**, la reconnaissance constitutionnelle des libertés publiques et leur protection, revue Algérienne des sciences juridiques, université d'Alger, volume 36, N° 2, année 1998, p 56*
***[26] - Regulation (EU) N° 2016/679** of the European Parliament and of the Council of 27 April 2016, Official Journal of the European Union L 119/1, of 4 May 2016*
***[27] -General assembly of the United Nations**, Distr.: General 21 January 2014, Digital copy available on the website of **UN** https://documents.un.org.*
***[28] - https://www.nytimes.com/2015/04/10/opinion/global-threats-to-net-neutrality.html** Accessed on 22/04/2024 At 22:25*
***[29]- Law N°. 575/2004** of June 21, 2004, For confidence in the digital economy, J.O N°. 143 of June 22, 2004, p.1168.*
***[30] –Article N° 2 Law 575/2004** related to trust in the digital economy was issued of the named law The separation of these two regimes, namely audiovisual communication and communication to the public online, also results in their submission to a different supervisory authority. Thus, while the Regulatory Authority for Electronic Communications and Posts is responsible for activities relating to communications to the public online, it is the Audiovisual Council which will be responsible for the field of audiovisual communication.*

References/Bibliography:

A-Books :

***1- Mohammad Taher**, Digital Liberties (Basic Concepts), Foundation for Freedom of Opinion and Expression, 1st Edition, Cairo Egypt, 2013.*

***2- T. Vedel,** Les politiques des autoroutes de l'information dans les pays industrialisés une analyse comparative, Réseaux, 1996, n° 78.*

***3- Nicolas Ochoa,** Personal data law, a special administrative policy. Law University Paris 1 Panthéon-Sorbonne, 2014*

***4- Eduard Lioe Kim**, Armed Forces in law enforcement operations, the German and European perspective, springer, Verlag, Berlin Heidelberg, 2010.*

***5- Mansour Aqeel and Ali Qasim**, The Internet and Security Dimensions, Center for Police Research and Studies, Dubai, United Arab Emirates, January 1996.*

***6-Ghassan hadi abd karaghouli**. The electronic administrative control authority and its judicial guarantees in Iraq. PhD thesis .2020*

B-Journal article:

***7- N. Wetsman,** Mental Health App Privacy Language Opens Up Holes for User Data, THE VERGE (May 4, 2022, 11:30 PM),*

https://www.theverge.com/2022/5/4/22985296/mental-health-app-privacy-policies-happify-cerebral-be:erhealth-7cups

***8- FEDORENKO, NV & HEJGETOVA**, Digital Rights in Civil Legislation of Russia. In Institute of Scientific Communications Conference, Springer, Cham ,SE (2019).*

***9- Zainab Muhammad** Jamil Al-Dannawi, Legal Protection of Privacy on the Internet in Light of International and Internal Efforts, article published in the book of the Forum of Proceedings of the International Conference on Privacy in the Information Society, King Faisal University in the K.S. Arabia 2019*

***10-Mekamcha Ghaouti**, la reconnaissance constitutionnelle des libertés publiques et leur protection, revue Algérienne des sciences juridiques, université d'Alger, volume 36, n 2, année 1998.*

11-G.Haywood, H Suvineetha, L.McKee, Privacy**, Harm and Non-Compliance from a Legal Perspective, Journal of Cybersecurity Education, Research and Practice Journal of Cybersecurity Education, Volume 2023 Number 2 Article3, Available at: **https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/3

***12-Ahmed Mohammad Fathi Al-Kholy**, Civil Liability for the Unlawful Use of Artificial Intelligence Applications, an article published in the Journal of Jurisprudence and Legal Research, Faculty of Sharia and Law in Damanhour, Arab Republic of Egypt, Issue 36, October 2021.*

***13-KONOBEEVSKAYA, IM** (2019). "Digital rights as a new object of civil rights: Proceedings of Saratov University." New series. Series "Economics". Management. Right, 19(3).*

***14-Hildebrandt Mireille**, « Legal Person hood for AI? », Law for Computer Scientists and Other Folk (Oxford, 2020; online edn, Oxford Academic, 23 July 2020).*

***C–Internet websites**:*

15–https://news.un.org/ar/story/2013/12/192412 Date of visit 22/04/2024

16–https://www.ohchr.org/en/topic/digital–space–and–human–rights.

17–https://web.archive.org/web/20190901020624/

18–https://www.nytimes.com/2015/04/10/opinion/global–threats–to–net–neutrality.html

19–https://www.oic.qld.gov.au/guidelines/for–government/guidelines–privacy–principles/use–and–disclosure

20–https://www.iberdrola.com/innovation/what-are-digital-rights

D–Legal texts :

21- Law No 2518/F3/B of the US Code of Criminal Procedure.

22– Law No. 2004-575 of June 21, 2004, For confidence in the digital economy of france, J.O No. 143 of June 22, 2004.

23- Convention No. 108/1981 of the Council of Europe on the protection of individuals during automated processing of personal data, adopted within the framework of the Council of Europe on January 28, 1981, and supplemented by the Additional Protocol of 2001.

24– Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Official Journal of the European Union L 119/1, of 4 May 2016.

25– Resolution No. 168/167 on the right to privacy in the digital age, adopted by the United Nations General Assembly on 18 December 2013 during the 68th session on the basis of the report of the Third Committee.

26– Law 18-07 of June 10, 2018, relating to the protection of natural persons in the field of processing personal data, Official Journal of Algerian Republic, No. 34 issued on June 10, 2018.

27- Resolution of The European Parliament N° 2056 of 2002: the framework of a Transatlantic Partnership Agreement.