Interdisciplinary Journal of Humanities, Media, and Political Science (IJHMPS)
Vol. 2, No. 1. June 2025

The Role of Privacy As An Ethical Guarantee in The Use of Artificial Intelligence in Public Utilities: A Comparative Analytical Study

https://www.doi.org/10.56830/IJHMPS06202505

Mohamed Ahmed Abdel Naeem
College of Law - University of Bahrain, Bahrain

mabdelmonem@uob.edu.bh

Received: 17 April 2025 Revised: 24 May 2025 Accepted: 28 May 2025 Published: 15 June 2025

Abstract

Accelerated scientific development has imposed itself on countries with different degrees of progress between them, and artificial intelligence is one of the most prominent manifestations of this development, and artificial intelligence is generally meant to simulate machines to the mental abilities of humans, and this technology emerged in the last stage of the last century, and led to a major transformation in various areas of life. It is important that this legal framework coincides with an ethical charter that addresses the ethical risks arising from the administration's use of artificial intelligence applications. This charter includes a set of principles and guarantees aimed at reducing those risks, such as: the right to privacy and protection of personal data, transparency and integrity, justice and equality, responsibility, and other ethical principles.

The study addresses this important dimension, and sheds more light on one of the principles that represent ethical guarantees in this field, which is the guarantee of the privacy of personal data, and this dimension has aroused our interest due to the lack of legal studies that dealt with it. The study has resulted in important results and recommendations worthy of implementation to move forward towards the establishment of integrated legislation regulating the administration's use of artificial intelligence systems, and to exert more effort towards the establishment of an ethical charter that includes a set of guarantees such as the guarantee of privacy and the protection of personal data, in order to achieve the desired balance between the escalating technical innovation of those systems on the one hand and the protection of rights and freedoms on the other hand, and to ensure a safer use of these systems in general and in the field of providing public utility services in particular.

Keywords: Ethical Guarantee, Artificial Intelligence**,** Public Utility Services, Right to Privacy- Ethical Safeguards.

1. Introduction

Imposing the same accelerated scientific development on countries according to the different degree of progress among them. Artificial intelligence is one of the clear manifestations of this development. Artificial intelligence in general means that the machine simulates the mental abilities of humans. It emerged as a promising technology in the last stage of the last century and it would have brought about a major transformation in all aspects of life in general, and in turn it reflected on the performance of countries and their authorities.

Artificial intelligence technology has imposed itself on the performance of the administrative authority like other authorities, which therefore relied on this

technology in developing the management of many ministries and public facilities of various types. In response to this, several scientific, legal and ethical challenges have arisen with which it was important for legal systems to develop an integrated framework that ensures the use of this technology while respecting the principle of legality or compromising ethical frameworks and principles.

In this context, it was not surprising that the legal systems at the international and Arab levels - including the Bahraini legislator - seek to launch legal frameworks to control the activities of the various state agencies, especially public utilities as vital devices that provide their services to different groups of society on an equal footing, if they rely on artificial intelligence technology in the conduct of their activity.

It is not lost on the target that this legal framework coincides with an ethical framework and charter that faces the ethical risks arising from the administration's use of artificial intelligence applications, and in turn includes a number of principles and guarantees to reduce those risks, such as the principles of the right to privacy and protection of personal data, transparency and integrity, justice and fairness, and the availability of responsibility.... etc. The study addresses this important dimension, and sheds more light on one of the principles that represents an ethical guarantee in this field, which is the guarantee of the privacy of personal data, and this dimension has aroused our interest due to the lack of legal studies that dealt with it. The administration's use of artificial intelligence systems in the management and development of the performance of public utilities raises several legal problems, perhaps the most prominent of which is what raises the legal nature of these systems, and the extent and basis of legal responsibility for the damages resulting from this use, on the one hand. On the other hand, the administration's use of these applications raises ethical problems because those in charge of these systems are expected to waste the individual rights of their beneficiaries or users, such as the right to privacy, confidentiality of personal data, transparency, equality and availability without discrimination, which in turn raises the following pivotal question:

What is the role of ethical safeguards in general and the right to privacy of personal data in particular in reducing the ethical risks arising from the administration's use of artificial intelligence applications, and is there a need to establish an ethical charter in this regard?

The study seeks to answer the following questions:

1. What is artificial intelligence in general and its legal nature, and the field of its applications in public utilities in particular?
2. What is the concept and dimension of the guarantee of the right to privacy of personal data as a constitutional and ethical control of the administration's uses of artificial intelligence applications?
3. What are the legal and ethical risks of the administration's use of artificial intelligence applications?

4. What are the implications of holding ethical responsibility arising from the administration's breach of the privacy guarantee?
5. Is there a need to launch an ethical code to reduce the risks of management using artificial intelligence?

The study attempts to achieve the following objectives:

Define the concept of artificial intelligence in general and its legal nature, and the field of its applications in public utilities in particular; a statement of the concept and dimensions of the right to privacy as a constitutional and ethical control of the administration's uses of artificial intelligence applications; highlighting the most important legal and ethical risks of the Department's use of artificial intelligence applications; discuss the implications of holding ethical responsibility arising from management's breach of the privacy guarantee, and finally highlight the importance of establishing an ethical code to reduce the risks of the Department's use of artificial intelligence.

In addressing its subject and the problems it raises, the study relies on the descriptive and comparative analytical approach to achieve the objectives of the study and provide results and recommendations by describing and analyzing the trends of legal systems regarding the ethical challenges of the administration's use of artificial intelligence applications in the field of public utilities by identifying the vision of the legal system in the Kingdom of Bahrain with the requirements of the study using some comparative models.

2. The Concept of Artificial Intelligence:

There have been many jurisprudential attempts to define artificial intelligence. One of the traditional concepts of artificial intelligence is the **view** that artificial intelligence is "the science and engineering of making intelligent machines. (McCarthy, Artificial Intelligence, Logic, and Formalizing Common Sense Philosophical Logic and Artificial Intelligence. , 1989)

It can be defined simply as a technology that enables machines to simulate human mental abilities based on the integration of computer science and data analysis to perform complex tasks and make decisions using advanced algorithms that work at high speed and accuracy.

Another view was that it is the process of developing computer systems to be able to carry out tasks that usually require the use of human intelligence, such as visual perception, speech recognition, decision-making and translation. (McCarthy, 1993)

In more detailed terms, artificial intelligence is seen as software systems and perhaps devices designed by humans with a complex goal and work in the real or digital world by perceiving the environment, by obtaining information, and by interpreting the collected structured or unstructured data, and applying the analysis of this to the knowledge or processing of the information derived from those data, and deciding the best action or actions to be taken in order to achieve a specific goal. (Commission euro penne, 8avr.2019, p. p143)

The draft Arab Charter on the Ethics of Artificial Intelligence went on to define artificial intelligence as systems capable of processing data through algorithms to a degree that simulates intelligent behaviors in learning, prediction, control and decision-making. It may be in a virtual environment that is software or embedded in devices, equipment and mechanisms such as robots, automated chat systems, smart cities, autonomous generation, display and discovery systems, drones, smart homes, cars and smart virtual assistance systems. (Draft Arab Charter for the Ethics of Artificial Intelligence)

The proposed law submitted to the Shura Council defined the concept of artificial intelligence as a set of characteristics that characterize computer programs and robots, and smart machines that make them simulate human mental abilities, and their working patterns. (Article 1,, 24 April 2024)

In light of the above, it can be said that artificial intelligence is the machine simulation of some human mental abilities through specific technologies intended for specific purposes. In other words, it is a field that aims to develop systems capable of performing complex cognitive tasks based on learning, thinking, and interacting with the environment, in a way that simulates or exceeds human intelligence.

With this understanding , artificial intelligence provides a technological revolution, as it has the great ability to understand and analyze inputs well in order to provide outputs that meet the required needs, as artificial intelligence programs have a range of characteristics, including the ability to accept and accept information, deal with incomplete information, infer and use the experimental method in solving problems. (Al-Dhuhoori & Mustafa Al-Nujaifi, 2024)

2.1 The Legal Nature of Artificial Intelligence:

After determining what artificial intelligence is, the research requirements impose on the legal nature of it, which means answering the following question: Is artificial intelligence just a smart machine or can it be considered a moral person? The importance of answering this question appears in the important legal consequences of the answer in terms of the nature of the actions and bearing the burden of responsibility and other consequences. In this regard, in French and Egyptian law, a basic idea is to distinguish between a legal person and things, and people are persons of the law, while things are legal things.

It should be noted that artificial intelligence is a system of software, while the robot is a device and artificial intelligence is an element in it , and it is then called the intelligent robot, and it is a legal entity ownedbecause it is man-made.

Since it is physical money, it is subject to **the provisions of civil law** on funds, and the programs intended for operating the robot or those used by the robot in carrying out its tasks can be protected as **intellectual works** under copyright and intellectual property provisions apply to it, which proves rights such as **patent** if the necessary legal conditions are met.

In French jurisprudence, a new idea appears that seeks to recognize the

legal personality of the robot as a model of artificial intelligence, with the aim of transferring the burden of responsibility to it similar to a legal person. However, this idea is **dangerous because** it may lead to the abolition of the basic division prevailing in law, which is the division between **persons** and **things** (Glaser, 2018) On the other hand, the recognition of the legal personality of the robot can also lead in the future to the recognition of fundamental rights similar to natural persons, as this recognition will raise more severe problems than those raised for legal persons. (Abdellatif, 2021)

In this context, it can be said that the opinion opposing the recognition of the legal personality of the robot as an advanced model of artificial intelligence is consistent with realistic logic and the nature of things. The robot is not an independent entity but is man-made. This opinion is also consistent with legal logic. The robot does not have legal personality as a legal person, so it does not have an independent financial liability, and therefore it will not be eligible to bear the burden of responsibility, because it remains just something that is subject to the control and supervision of its users and designers.

3. Areas of the Department's Use of Artificial Intelligence in Facilitating Public Utility Services:

Artificial intelligence has achieved rapid and remarkable development over the past decade, as technologies such as machine learning, natural language processing, and computer vision are increasingly permeating various fields and disciplines within different societies. Proceeding from this, artificial intelligence is increasingly assuming an aspect of human tasks, replacing human decision-making, and has been widely used in a variety of sectors including business, logistics, manufacturing, transportation, health, care, education, state administration, and others (Huang, 2023). Developed countries are keen to employ artificial intelligence tools in various areas of governance and management within the framework of what is known as "e-government", and what results in the field of public service under the name of "smart management", which has become a prerequisite for the improvement of public facilities management methods.

The value of artificial intelligence is more evident in the field of public facilities management, as it contributes to the transformation of traditional management into smart management through **digitization** and **electronic storage** of documents , which contributes to enhancing efficiency and effectiveness in the delivery of public services. (Bakheet, 2023).

In application of this, we see the multiplicity of areas of the use of artificial intelligence applications in the field of public administration.

The uses of artificial intelligence in the field of administrative work are endless, and include the process of issuing administrative decisions related to the

granting of various permits, licenses and administrative approvals. It is also used in the field of concluding electronic administrative contracts, especially with regard to prior administrative examinations related to the conditions for participation in public tenders.

Artificial intelligence techniques are also used in the field of providing public services, such as extracting some administrative documents and receiving and processing various administrative requests. Moreover, it is used in the field of imposing administrative penalties, especially in the field of security and those related to administrative control measures in its various fields. (Rabhi) It seems a serious attempt by the national legislator in the project presented by the Shura Council recently to provide several areas for the uses of artificial intelligence in the field of public administration, as well as in the field of providing services, concluding contracts and issuing the necessary regulatory decisions for good work. (Article Thirteen of the proposal attached to the report submitted by the Legislative and Legal Affairs Committee of Majlis Al-Shura, April 24, 2024) Thus, artificial intelligence is an essential tool to improve the efficiency of administrative services and make them more flexible and faster, enhancing the quality of work and meeting the changing needs of public utility service applicants and employees. Despite this clear contribution to the use of artificial intelligence applications in facilitating and developing public utility services for the public, this use would raise the possibility of compromising the privacy of their personal data by those who manage them, and **in this regard it requires exposure to what is the right to privacy and the extent to which the administration's use of these applications affects this right?**

4. What is the Right to Privacy?

Privacy according to language is the source of the action that belongs to you, and the privacy of the thing that belongs to you, or what belongs to you alone, and the private opposite of the public, and the private one that belongs to you. (Al-Mujam Al-Wasit, Al-Maani Al-Jamaa Complex) However, it seems difficult to reach a comprehensive definition of privacy, and the reason for this stems from the fact that the pursuit of this definition usually stems from different philosophies, each of which focuses on a specific aspect or a set of aspects that the definition aims to protect. In addition, the concept of privacy itself is a changing concept, as the constituent elements are characterized by their excessive sensitivity to the development of means that enable approach to privacy. As a result, it is noted that the elements constituting privacy are characterized by their continuous increase; it expands in each time period to include other elements that were not among its components in previous eras. For example, after the concept of privacy was linked to traditional paper correspondence, correspondence developed through the telegraph and then to electronic correspondence, and on this temporal basis, we find that there is a difference in understanding the exact meaning of the term "privacy". In this

context, there have been many attempts to define the concept of privacy, and we find an opinion that stems from the element of ability, that is, the ability of a person to decide on what is related to him and the conditions that allow others (Glenn, 2003) to access these things. Another view defines it as one's ability to keep one's own affairs and prevent their disclosure (Al-Homsani, 1979)

It can be said that privacy in its general sense is the right of a person not to interfere or declare in relation to matters of a personal nature (Merriam-Webster), privacy is the circle close to the human being, which includes his private affairs related to him, both in his individual and family life. In more detailed terms, it is the ability of an individual or persons to isolate themselves or information about them and thus express themselves in a selective and selective manner, thus preventing information about them from becoming unknown to others. With multiple definitions of privacy and although they vary in defining their components, they share the fact that they provide a space for individuals to ensure that others are prevented from accessing it except with their consent. This space is known as privacy. Guided by the foregoing, it can be said that the right to privacy combines being a right of a special nature. It is a constitutional right that finds its basis at the national level in the Constitution from the reality embodied in constitutional texts on the one hand, and that it is a human right at the international level from the reality embodied in the texts of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and others, as will be mentioned , and a third aspect is a right intrinsic to personality and therefore has criminal and civil protection in accordance with the special rules in this regard. (Sorour, 1978) As we have finished defining what the right to privacy is and highlighting its legal nature, the question that arises in this regard is: To what extent could the administration's uses of AI applications provoke a violation of the right to privacy? This is what we present in the following item.

5. Does the Administration's Use of AI Applications Raise a Violation of the Right to Privacy?

Artificial intelligence, as developed, has contributed to an unprecedented breakthrough in the development of the performance of the administrative authority in several fields, especially in the field of providing public utility services, for example, services related to health, security, financial and other aspects. This opens up prospects for facilitating these services at high speed and quality. However, this development is offset by raising several legal and ethical challenges that will affect the basic rights of individuals, including the right to privacy.

In this context, privacy has become threatened due to the increasing interaction of individuals with the digital world, and personal digital data and before it the aspects of private life have become a material that is used either commercially in the implementation of marketing propaganda, monitored by

government agencies or exposed to theft and exploitation for purposes that harm their owners. If the administration uses artificial intelligence techniques to keep pace with the developments of the times if it plays its primary role in the management of the public facility and the provision of services, this in turn requires the use of personal digital data of its customers, which raises the possibility of compromising this data, or exposure to some aspects of private life. In order to clarify this, it is necessary to define the concept of personal data on the one hand and to determine the extent of possible infringement or harm as a result of the use of these technologies by the administration on the other hand.

Personal data in general means those stored in computers and various information systems such as mobile phones, various websites, electronic mail, or in the form of information banks or databases, which relate to persons such as their family, health, financial, and social data.

The French legislator has been proactive in defining the concept of personal data in Article 2 of Law No. 801 of 2004 on the Protection of Personal Data. However, it "is considered a personal statement any information related to a natural person whose identity is known or whose identity can be identified, whether directly or indirectly, or whose identity can be identified by reference to the name, personal identification number and location data and the online identifier of one or more specific elements of personal , physiological , genetic, psychological, economic, cultural or social identity."

The Bahraini legislator has been keen to control the concept of personal data in Article 1 of Law No. 30 of 2018 regarding the protection of personal data as follows: "Any information in any form relating to an identified individual, or directly or indirectly identifiable, in particular through his personal identification number or one or more of his formal, physiological, mental , cultural, economic or social identities." It also singled out a distinct concept of what he called sensitive personal data in the same article as:“ Any personal information that directly or indirectly discloses an individual's racial or ethnic origin, political or philosophical opinions, religious beliefs, trade union affiliation, criminal record or any data relating to their health or sexual status.” The Egyptian legislator, in turn, defined it with an approach in Article 1 of Law No. 151 of 2020 on the Protection of Personal Data as:" Any data related to a specific natural person, or that can be identified directly or indirectly by linking these data with any other data such as name, voice, image, or an identification number, or an online identifier, or any data that identifies psychological, health, economic, cultural, or social identity."

The Egyptian legislator's identification of sensitive personal data came in a broader sense than its Bahraini counterpart, as it defined it as"data that discloses psychological, mental, physical and genetic health, biometric data, financial data, religious beliefs, political opinions or security situation. In all cases, children's data are considered sensitive personal data." In light of the previous legislative definition of personal data, it can be said that there is a convergence

of vision between the three legislators, and then it can be said that it is the information of the natural person or that is closely related to him that distinguishes him from others. As for sensitive personal data, it is distinct from the first, that is, the ordinary person, as it reveals more specific and dangerous aspects of his association with matters of affiliation, beliefs, health, family and financial aspects, as well as the criminal record. The privacy of digital data is the information that is done through a machine or an electronic medium. With the rapid technological development, most of our transactions, in daily life, are done digitally . The identity card is a digital data registered with government institutions, through which our personal identities are inferred. (Mahmoud, 2022) It is difficult to develop a unified perception of the extent to which the administration's uses of artificial intelligence technologies affect privacy, as the matter varies from one society to another and from one legal system to another according to cultural and social conditions, the level of morals and religious beliefs. What is allowed under a particular legal system may be rejected by another system according to these circumstances. It is relative and varied, on the one hand. On the other hand, the impact of this use does not raise problems of the same dimension in public life, as it is not accompanied by considerations of confidentiality or other requirements of the inviolability of private life or privacy.

It is possible to imagine a violation of the privacy of personal or sensitive data through the administrative authority through its competent administrative bodies to access these data available to it for the purpose of inspection, electronic monitoring, information collection , or in light of what is required from the filling of digital personal data by individuals as basic requirements to obtain the multiple services provided by public utilities,or those that are among the records kept by the administration such as criminal and health records, and then the latter is allowed to deal with these data or records, which raises the possibility of compromising their privacy if they are dealt with in a manner that lacks professional ethics. Risks to privacy have increased in light of the increasing use of artificial intelligence technologies and their continuous development in daily administrative transactions, as they are today restricting the individual in his movements, monitoring his business and movements, collecting personal data about him, storing and processing them by informational means such as video surveillance techniques, mail control, communications, databases, and others.The danger of the administration's use of artificial intelligence applications on the inviolability of private life arises when collecting, storing and operating personal data, and when this information is extracted from the system's memory and communicated to others, regardless of whether it is a governmental or non-governmental body or a natural person. (Saleh, 2000)

In this context, it seems that the violation of private life is most severe in the face of the state and its agencies, as the ease of transfer and exchange of data

between computers and information banks belonging to the executive authority and (Azzawi, 2000) its agencies. In light of these challenges posed by these technologies, which are no longer complementary or luxurious, it is necessary to identify the legislative role in providing legal protection for the right to privacy in light of the use of these technologies, which requires shedding more light in the following item.

6. Legal Protection of the Right to Privacy

The constitutional legislator in the Kingdom of Bahrain realized the importance of protecting rights and public duties, as he was keen to approve them and referred to the ordinary legislator the work of regulating their practice and establishing mechanisms for their protection. Chapter III of the Constitution, which is prepared to embody this trend, came. Articles 24 and 25 of this Constitution stipulate that the right to privacy is protected and that it is prohibited to attack it, as mentioned above. Article 25 of the amended Bahraini Constitution stipulates that homes are inviolable. They may not be entered or searched without the permission of their families, except in cases of extreme necessity specified by law and in the manner stipulated therein. Article 26 added that the freedom of postal, telegraphic, telephone, and electronic correspondence is safeguarded, and its confidentiality is guaranteed. It is not permissible to monitor correspondence or disclose its confidentiality except in the necessities specified by law, and in accordance with the procedures and guarantees stipulated therein. Based on this constitutional recognition, several legislations, regulations and decisions have been issued at the national level in the Kingdom of Bahrain in support of protecting the right to protection of personal data as a manifestation of the right to privacy, for example: (the website of the National Portal of the Kingdom of Bahrain)

(1) Law No. (60) of 2014 on information technology crimes, came to be a deterrent to anyone who exploits technology and the Internet to carry out his crimes, and this law is a criminal protection for information technology users, as it included the identification of information technology crimes and measures to combat them.

(2) Resolution No. (43) of 2022 specifying the requirements that must be met in the technical and organizational measures to protect personal data. The resolution regulates a set of technical and organizational measures to be applied in data processing in addition to evaluating the impact of data protection and the obligation to notify of a data breach or violation. The resolution also obligated the data manager to establish clear rules for internal investigation aimed at revealing the reasons that led to the data breach or violation.

(3) Resolution **No. (45) of 2022 on determining the rules and procedures for the processing of sensitive personal data,**
and this resolution regulates the mechanism and procedures for the processing

of sensitive personal data, to ensure that they are not compromised or violated. The decision clarifies how to obtain prior authorization from the Personal Data Protection Authority for the processing of this data, as well as the regulatory rules related to the processing process.

(4)Resolution No. (48) of 2022 on the rights of the personal data subject. This resolution specified the scope of application of its provisions to the data stipulated in Article (1) of the Personal Data Protection Law. The resolution clarified the obligations related to the decisions taken based on automated processing, the approval of the processing and the scope of its application, as well as the irrelevant consent. The resolution stated the conditions under which the data subject has the right to request the withdrawal of the consent. The resolution obligated the data manager to indicate the procedures for submitting the objection by the data subject.

This interest on the part of the Bahraini legislator continued in the proposal submitted by the members of the Shura Council recently in the context of a proposed law to regulate artificial intelligence technologies. Article 5 of this proposal stressed the requirement that these technologies do not include any prejudice to constitutional rights and freedoms, do not prejudice the legal rights of children, and do not prejudice public order and morals... Etc. (Council, April 24, 2024)

For his part, the Egyptian constitutional legislator has affirmed in many successive Egyptian constitutions the recognition of the right to privacy, including what is stipulated in Articles 44 and 45 of the Permanent Constitution of Egypt of 1971 (repealed), as well as what is stipulated in the current Constitution of 2014 amended in 2019 in Articles 57 and 58, including the protection of the inviolability of private life, housing and means of communication in their various forms and restricting their monitoring with the issuance of a judicial authorization.

Article 57 stipulates that private life is inviolable and inviolable . Postal, telegraphic, and electronic correspondence, telephone conversations, and other means of communication are inviolable, and their confidentiality is guaranteed. They may not be confiscated, accessed, or censored except by a reasoned judicial order, for a specific period, and in the cases specified by law.

Article 58 of this Constitution also added to the inviolability of homes, which may not be entered except in cases of danger or distress, nor are they searched, monitored or intercepted except by a reasoned judicial order specifying the place, time and purpose, all in the cases specified by law.

The Egyptian ordinary legislator was proactive in issuing many legislations to protect personal data by imposing the protection of their confidentiality. This emerged, for example, through the Civil Status Law No. 260 of 1960. In this regard, Article (9) of this law, amended by Law No. (11) of 1965 and Law 158of 1980, stipulates that the data contained in civil status records are considered confidential. Since these data are confidential, their disclosure by the employee

makes him subject to the law and accountability under the provisions of the Egyptian Penal Code.

In this context, the Central Bank and Banking System Law No. 194 of 2020 was issued as a special chapter under the title "Confidentiality of Accounts". Article (140) of this law requires that all customer data, accounts, deposits, trusts and treasuries in banks, as well as transactions related to them, are confidential, and it is not permissible to view them or give data about them directly or indirectly except with the written permission of the account holder,or with a power of attorney issued by him, or to implementa judicial ruling or an arbitral award...etc.

This protective role of the Egyptian legislator was crystallized by the issuance of Law No. 151of 2020 on the protection of personal data. (Published in the Egyptian Official Gazette, Issue 28bis(E), 15 July 2020)For example, Article 2 of this law highlighted this role in the following: “Personal data may not be collected, processed, disclosed or disclosed by any means except with the explicit consent of the person concerned with the data, or in the cases authorized by law.”

The law also includes many criminal and administrative penalties in Articles (35-48) in the event of a breach or infringement of personal data in violation of the provisions of the law.

The leading role of the French constitutional legislator in this regard was highlighted. The preamble to the current French Constitution, issued in 1958 and amended in 2008, affirmed the general principle of respect for all rights and fundamental freedoms as defined in the Declaration of the Rights of Man and of the Citizen in 1789. Articles 4 and 11 of this Declaration stated that the goal of every political society is to preserve the natural rights of man and the rights that are not subject to prescription. These rights are freedom, property, security and resistance to injustice. (political encyclopedia) In this context, the French ordinary legislator issued Law No. 17-78 of January 6, 1978 on the processing of personal information and data and freedoms, as amended by Law No. 493-2018 of June 20, 2018 on the protection of personal data, to allow the concerned party alone the right to access his personal data (Law No. 78-17 , on Information Technologies, Data Files and Individual Liberties, 1978) The importance of the right to privacy is also reflected in the recognition of this right contained in international charters, declarations and covenants and the measures imposed on the international community by States to take at the level of their national legislation to recognize and protect it. For example, the Universal Declaration of Human Rights recognized the right to privacy. No one shall be subjected to arbitrary interference with his private life, family, home or correspondence, nor to campaigns against his honour and reputation , and everyone has the right to the protection of the law against such interference or campaigns.” (Article 12 of the Universal Declaration of Human Rights, 1948)

Article 17 of the International Covenant on Civil and Political Rights states

that it is not permissible to "expose any person arbitrarily or unlawfully to interference with his privacy, family, home or correspondence . (International Covenant on Civil and Political Rights, 16 December 1966.) The constitutional judiciary was not far from recognizing the right to the inviolability of private life as a model for the right to privacy. In an important ruling, the Egyptian Supreme Constitutional Court clearly expressed this principle by saying: "There are areas of the private life of each individual that represent inaccessible depths, and should always – and to be considered legitimate – not to be stormed by anyone to ensure their confidentiality, and to preserve their sanctity, and to push to try to eavesdrop on them or embezzle some of their aspects, especially through modern scientific means, which have reached a staggering level, and the growing capabilities to penetrate has had a far-reaching impact on all people, even in the most delicate of their affairs, and what is related to the features of their lives, and even to their personal data, which have been viewed and collected looting their eyes and ears, and often critical access to them or harming their owners.

These areas of the characteristics and intrinsics of life preserve two interests that may seem separate, but they are complementary, as they generally relate to the scope of personal matters that should be kept secret, as well as the scope of each individual's independence with some of his important decisions that – given their characteristics and effects – are more related to his fate, and affect the conditions of life that he chose their patterns – and crystallize all these areas – in which the individual resorts, reassured of their sanctity to dwell away from the forms and tools of censorship – the right for private life to have its borders, taking care of the intimate ties within its scope. Although some constitutional documents do not explicitly stipulate this right, some consider it one of the most comprehensive and broad rights, and it is also the deepest in connection with the values advocated by civilized nations." (the Egyptian Supreme Constitutional Court, 1972)

The comparative judiciary has also contributed to the establishment of the protection of privacy in many situations, including the ruling of the European Court of Human Rights in the case of Barbulescu v. Romania, where the Court issued a ruling on 5 September 2017 that Romania violated Article 8 of the European Convention on Human Rights. The Court pointed out that the national authorities did not strike the appropriate balance between the right of the employee to respect for his private life and correspondence and the right of the employer to ensure compliance with internal regulations. (The European Court of Human Rights (ECHR), 5 September 2017) Despite this legislative role and judicial recognition, as mentioned above, in providing legal protection for the right to privacy at the national, regional and international levels, this protection is still insufficient to cover all the risks of the administration's uses of artificial intelligence systems on the right to privacy. The matter is surrounded by other ethical considerations that must be taken into account in order to seek the safe

use of these applications. To what extent can privacy as an ethical guarantee contribute to this?

7. The Role of Privacy as an Ethical Guarantee in fine-tuning management uses of AI systems

We presented that despite the efforts exerted by the national and comparative legislator at the constitutional and legislative levels to provide the right to privacy with a measure of legal protection as mentioned above, they in their entirety seem insufficient to cover all the risks resulting from the multiplicity of the administration's uses of artificial intelligence systems in light of the accelerating pace of them at all levels. (Mengchen Dong, 2024)

Despite the great benefits offered by artificial intelligence in terms of improving services, increasing efficiency, and reducing costs, the irresponsible use of this technology may lead to a violation of individuals' privacy, which raises many ethical concerns.

This, in turn, requires identifying the ethical risks raised by these systems and determining the extent to which the ethical guarantees, including the privacy guarantee, contribute to confronting these risks, and the extent to which it raises some kind of responsibility of a special nature in the face of the administrative authority in the event that it violates this guarantee.

7.1 Ethical Risks of Management's Use of Artificial Intelligence Applications:

There have been many attempts on the part of jurisprudence in various fields of science to define the concept of moral risks, and it can be said in general that they are behavioral deviations that may arise in society as a result of changes imposed on it and threaten its human and moral values, or that they are risks that may arise from the permanent development of societies in a way that is incompatible with basic human values. (Taylor, 2020) While some opinions have tended to define the moral risks of using artificial intelligence applications as the set of harmful results and effects that may be left by artificial intelligence techniques through what they do without ethical and legal controls that may threaten all humanity and cause major moral and social issues in all fields. (Karim, 2024) . For their part, some international organizations have contributed to trying to define this concept of the ethical risks of artificial intelligence systems, recognizing that it represents a risk that requires the establishment of ethical controls and standards to control the use of these systems. In this context, the United Nations Industrial Development Organization clarified its concept of the ethical risks of artificial intelligence as those that arise from the development and use of artificial intelligence systems in a way that violates human rights or social rights. (United Nations)

The steady rise in artificial intelligence has created many opportunities globally, ranging from facilitating diagnosis for health care purposes to enabling humans to communicate with each other through social media, as

well as enhancing the efficiency of the workforce through automated tasks . (Ramos) (Miller, 2024), in addition to its many uses in the field of public utility services.

In this context, artificial intelligence systems produce new types of ethical issues that include, but are not limited to, the consequences of these systems on decision-making, as well as on employment, employment and work, social interaction, health care, education, the means of science, access to information, the digital divide, consumer protection, personal data, the environment, democracy, the rule of law, ensuring security and maintaining order, dual use, and human rights and fundamental freedoms, including freedom of expression, privacy, and non-discrimination. These rapid changes, of course, as we have pointed out, raise deep legal and ethical concerns that stem from the potential inherent in artificial intelligence systems, including the inculcation of biases, the exacerbation of climate deterioration, and the threat to human rights, especially privacy and the protection of personal data, in light of the fact that artificial intelligence systems rely on huge amounts of data to operate efficiently. This may lead to the collection of sensitive personal data without the consent or knowledge of users , and therefore the analysis of that data can lead to the detection of personal patterns and behaviors that may lead to a violation of individuals' privacy, including tracking people's locations or the use of medical data without permission. Thus, artificial intelligence systems pose many risks to privacy. Artificial intelligence systems are not transparent, as it is difficult to control the personal data that is included in the areas of requesting digital administrative services. Some trends have even exaggerated by saying that it has become impossible for users and seekers of these services to escape systematic digital surveillance. In addition to the above, it can be said that these risks can include other aspects that will achieve the unsafe use of artificial intelligence applications by management and users, and we mention that artificial intelligence systems can inherit some biases from the data they are trained on, which leads to unfair treatment of certain groups. For example, biased recruitment algorithms may lead to prejudice against certain population groups. On the other hand, some AI models make it difficult for people to understand how decisions are made by administrative authorities, because this lack of transparency can impede trust and accountability, as users cannot see the rationale behind AI-driven outcomes. Undoubtedly, these ethical challenges impose themselves, which requires the establishment of ethical guarantees coupled with executive mechanisms to reduce the risks of unsafe use of artificial intelligence technologies by the administration, and reduce the negative effects of this use against users of public facilities.

7.2 the nature and necessity of ethical safeguards to control the uses of artificial intelligence systems:

Ethical risks for the uses of artificial intelligence as developed, as well as legal protections, impose a number of ethical standards and safeguards that

contribute to controlling the practice of these uses . Ethical frameworks and principles provide basic guidelines for the responsible development and deployment of artificial intelligence systems, in order to ensure compatibility with societal values and ethical standards. (Chest)AI ethics is concerned with how human developers and manufacturers can act to minimize the ethical harm that can arise from AI, including addressing issues such as data privacy, bias, and the impact of AI on society. (Fawzi, 2024)There have been many attempts in general jurisprudence to develop an approximate concept of artificial intelligence ethics or what can be considered a guarantee to reduce the negative effects of the use of artificial intelligence applications. (Karim, 2024), and it can be said from these attempts that the ethics of artificial intelligence means those controls derived from the moral values of the human community aimed at controlling potential abuses of the rights and freedoms of individuals resulting from the uses of artificial intelligence applications, in an integrated manner with the legal controls governing these uses. In other words, ethical guarantees for the uses of artificial intelligence mean controls stemming from ethical values and principles such as integrity, transparency, equality and respect for privacy, which are approved by States and stakeholders at various levels within the framework of charters and covenants to ensure the exercise of these uses without prejudice to the rights and freedoms of individuals. Legal and ethical challenges to the use of artificial intelligence applications require the establishment of a set of guarantees to meet these challenges, in order to ensure the use of these applications, especially by the administrative authority in a more disciplined manner and less prejudicial to the rights of those dealing with them. This is highlighted in light of the lack of completion of the legal system to face these challenges, and the resulting legal dangers, especially in light of the lack of determination of the legal nature of applications of artificial intelligence, and then the failure of traditional liability systems to deal with all possible hypotheses generated by its uses in light of the jurisprudential dispute over the legal nature of these applications. (Alan, March 2020)

It is understood from the above that there is an urgent need to establish and enforce a number of ethical controls to govern the administration's use of artificial intelligence applications in a way that prevents prejudice to the basic rights of individuals. In order to do this, some efforts at various levels have sought to establish ethical charters to confront these risks and to control the uses of authorities in general and administrative in particular for artificial intelligence applications and reduce the damage of this use. Perhaps the most prominent in this regard is what was launched by the United Nations Educational, Learning and Cultural Organization (UNESCO) in the context of the recommendation on the ethics of artificial intelligence. (United Nations Educational, Scientific and Cultural Organization (UNESCO), November 22, 2021) where a first-of-its-kind global normative document in the field of artificial intelligence ethics, the

"Recommendation on the Ethics of Artificial Intelligence", was prepared in November 2021, and adopted by all ninety-three Member States.

This recommendation pays particular attention to the ethical consequences that wider AI systems have for UNESCO's key areas of competence of education, science, culture, communication and information, which were examined by UNESCO's World Committee on the Ethics of Scientific and Technological Knowledge in the Preliminary Study on the Ethics of Artificial Intelligence. This recommendation has exceptional implementability due to its broad policy areas of work**,** which allow policymakers to translate core values and principles into action while respecting data governance, ecology and ecology, gender, education and research, health and social welfare, and many other aspects of life. The recommendation also included ten basic principles to lay the foundations for a human rights-based approach to AI ethics, the most prominent of which is the right to privacy and data protection, where privacy must be protected and consolidated through the life cycle of AI systems.

On this basis, and in order to implement this recommendation, Member States and business organizations should take appropriate measures to monitor all stages of the life cycle of any artificial intelligence system, as well as data andall actors concerned with artificial intelligence.

This includes the way algorithms used to make decisions andparticipate in the process, especially in public facilities and where direct communication with the end-user is required as part of the ethical consequence assessment process, and the ethical aspects of AI system assessments should include Member States' legal human rights obligations. In this context, the Saudi Authority for Data and Artificial Intelligence has also achieved in the context of the principles of artificial intelligence ethics, including the establishment of a number of guarantees such as integrity, fairness, privacy, security, reliability, safety, transparency, responsibility and accountability. (Saudi Authority for Data and Artificial Intelligence (sdaia, September 2023) On the other hand, the Smart Dubai Foundation has established a document entitled "Principles and Guidelines for the Ethics of Artificial Intelligence", which included a set of ethical guidelines to control the uses of artificial intelligence, which included among them striving to achieve the fair use of artificial intelligence systems, making them accountable, as well as the importance of transparency and the need for their explainability and interpretation, among others. (Smart Dubai, 2021) Despite the issuance of some ethical charters - on the advanced detail - to contribute to controlling the uses of artificial intelligence, whether attributed to private entities, or attributed to the official authorities of the state, especially the administrative authority, if they manage public facilities, they remain only of literary and philosophical value unless accompanied by specific mechanisms that make them subject to implementation. There is no doubt that this represents a fundamental challenge to the activation of these charters and the ethical principles they contain, and this may be what prompted some European

organizations such as the Artificial Intelligence Organization for Society (AI4people) to formulate some mechanisms to activate these ethical guarantees to reduce the risks of using artificial intelligence, and the resulting waste or prejudice to the privacy of personal data available to the concerned administrative authorities if they manage public facilities. (others, 2018) This challenge also prompted the European Parliament to pass the first draft law to regulate the uses of artificial intelligence, as the draft law seeks to ensure that artificial intelligence technology products adhere to basic principles, including non-discrimination, curbing bias, protecting the right to privacy, and avoiding unfairness.

In order to achieve this, the law contains procedures related to data governance, transparency, and reducing bias, within the obligations of high-risk artificial intelligence systems. The law also includes a ban on a number of uses of artificial intelligence systems to ensure that these systems are not misused for the purposes of discrimination or manipulation of users' decisions, as we will detail later. (The European Commission, 2021)

This is the same thing that prompted the Bahraini legislator to proceed in this direction by submitting a proposal for a law to regulate artificial intelligence in the manner mentioned above.

7.3 Does privacy play a role as an ethical safeguard in curbing the excesses of AI systems?

Artificial intelligence techniques have great benefits in many fields, but in the absence of ethical controls, it is feared that they will lead to the emergence of bias and discrimination on the ground, fuel divisions and threaten fundamental rights andfreedoms. The importance of establishing ethical guarantees governing the use of artificial intelligence systems lies in the fact that they are designed to carry out work for the benefit of humanity in general and those dealing with the administration in particular. These systems in part are employed by the administration to provide certain services in various fields such as health care services, the issuance of identity cards and the completion of financial transactions, as well as the conclusion of some electronic administrative contracts. This allows the employees of public facilities responsible for their use and operation to view the most accurate personal data of dealers and those wishing to receive these services, and then the ethical officer has a complementary role not to misuse or manipulate this personal data in areas that may not be covered by the regulating legislation, in order to ensure respect for the right to privacy. As we have pointed out, the right to privacy is one of the fundamental constitutional rights inherent in the natural person as a human being as a public asset. It represents the basis of every healthy society, so societies, especially democratic ones, are keen to ensure this right, and consider it an independent right in its own right. Thus, it does not only enact laws to protect it, but seeks to establish it in the mind, by instilling moral values that play a great and effective role in preventing intruders from interfering in the

privacy of others and revealing their secrets.

Thus, it shows that in addition to the constitutional nature of privacy, it also represents one of the ethical guarantees that some international organizations and national entities have been keen to include within their issued creative topics to reduce the risks of the use of artificial intelligence applications by the state in general and the administration in particular. What is its contribution as an ethical guarantee to reduce the risks of this use on the rights and freedoms of those dealing with the administration? It should be clarified at the outset that the role played by moral guarantees in this regard does not in any way mean dispensing with or reducing the important function of legal rules in this regard, but rather it is a complementary role to them in light of the breadth of moral rules in comparison with the legal, as it includes what is not felt by what is not subject to interpretation and assumption. The law, by virtue of its function and the nature of its rules, does not enter into abstract intentions, and it is preferable not to interfere if it is impossible to adapt actions without revealing the depths of souls. The relationship between moral and legal rules is an integrative relationship in order to control social behavior. (Musa). Both the moral rule and the legal rule have a specific field of work, as the latter is of a legal nature, while the former is of a literary nature, and criminalization is not based on the fact that the act is immoral, but because it is an act that disrupts the order of society. Whenever the law interferes with morality, it is affected, not influential, so it is only a means of protecting moral value. In general, it can be said that the legal system depends on the moral climate of society and the effectiveness of this law does not depend only on the threat of material sanctions, but is based on a general social climate that believes in the legal system, that is, the acceptance of the legal system must become an ethical issue that members of society consider part of their moral values . Guided by the above, privacy can contribute to supporting the safe use of artificial intelligence applications by developing strong policies and practices to protect personal data. This is embodied through several mechanisms, the most important of which are:

1. Require the prior consent of the owners of personal data before it is used by artificial intelligence systems, and whoever the role of privacy as a barrier prevents the use of this data in unethical ways, such as excessive surveillance without the consent of individuals.
2. Use data minimization techniques to limit the amount of personal information processed as encryption and anonymization can increase the protection of sensitive data.
3. Adhere to the principle of transparency on data collection, use and storage as a vital mechanism in the protection of personal data. (Veena, 2024) , meaning that AI systems used in public utilities must be transparent, so that individuals understand how their data is being used and what actions are being taken to protect it. In addition, there should be clear accountability mechanisms in case of violations.

4. Privacy should be an essential part of the design of AI systems from the outset, so that technologies such as encryption, anonymization, and limiting data collection ensure that these systems are compatible with ethical principles.

7.4 Does the breach of the personal data privacy guarantee raise the ethical responsibility of the administration?

We presented that privacy is a necessary right to preserve human dignity, defend human independence, and protect human work. Therefore, privacy must be respected, preserved, and enhanced throughout the life cycle of artificial intelligence systems. (United Nations Educational, Scientific and Cultural Organization (UNESCO), 2021) **..** It is necessary to determine the extent to which the administration adheres to respect for privacy as an ethical guarantee to complement the constitutional basis for the right to privacy, and therefore what is the mandatory value of ethical guarantees, especially the privacy guarantee?

First, the administrative authorities using artificial intelligence systems must respect fundamental freedoms and should defend and promote them, and bear the moral and legal responsibility they bear, in accordance with the provisions of national law and the provisions of international law. Ethical responsibility for decisions and actions based in any way on any AI system should ultimately be attributable to AI actors according to their respective roles in the life cycle of the AI system. Despite the importance of acknowledging the moral responsibility of the administrative authority or its employees in the event that they violate the ethical guarantees governing their use of artificial intelligence applications, the main difficulty in this regard is to determine the controls and scope of this responsibility and determine its effects on the one hand, and to estimate the extent to which ethical guarantees contribute to reducing the harms of uses of artificial intelligence due to the lack of these guarantees of mandatory value on the other hand. (Boddington, 2017). In this context, the activation of these guarantees approved by some ethical charters in the above manner requires the development of clear mechanisms for ethical accountability and their conjunction with appropriate penalties in the face of States in general and administrative authorities in particular in the event of their practices that violate these guarantees, foremost of which is the guarantee of personal data privacy., and this is not without difficulty. This difficulty in determining ethical responsibility controls imposes the importance of adopting technical measures of a preventive nature to support the privacy of personal data, and this is achieved through the development of artificial intelligence systems to be protected in a secure manner that takes into account the relevant regulatory requirements in order to prevent illegal access to data and the system, which may lead to damage to reputation or cause psychological, financial or professional damage, including those related to the protection of the privacy of personal data holders, on the one hand. AI systems, on the other hand, can be designed using mechanisms and controls that enable the

management and monitoring of results and progress throughout their lifecycle, to ensure their compliance with relevant privacy and security rules and controls. (Saudi Authority for Data and Artificial Intelligence (sdaia, September 2023, p. 14)

7.5 The role of the legislator in establishing a mandatory framework to protect the privacy of personal data as an ethical guarantee?

Ethical charters adhere to a set of guarantees, including the guarantee of the privacy of personal data, but these charters, as we have presented, stand at the limit of philosophical and literary value, and require some kind of mandatory framework to ensure compliance with them. It seems that achieving this is not easy as the legislator needs to anticipate the rapid developments of artificial intelligence technologies, and this means that the legislative role in general is still deficient, as it does not go beyond merely seeking to establish some laws without going into effect.

However, one of the commendable attempts - as well as the project approved by the Shura Council as advanced – is what was proposed by the European Commission on 21 April 2021 and approved by the European Parliament on 13March 2024, which we referred to in advance in the context of a draft law to regulate artificial intelligence as a legislative framework aimed at regulating the use of artificial intelligence technologies in a way that ensures safety, promotes human rights, encourages innovation, focuses on determining the levels of risk associated with various artificial intelligence applications, and relies on the principle of gradual regulation. (European Parliament) Among its objectives, the project seeks to ensure that artificial intelligence is not used in a way that threatens privacy or leads to discrimination against individuals, and to enhance confidence in the use of artificial intelligence technologies by ensuring that they adhere to security standards. In this regard, it is possible to highlight the mechanisms adopted by the European Artificial Intelligence Project to protect personal data, which can inform the national legislator in supporting ethical guarantees for the uses of artificial intelligence. (masaar)

<u>The most prominent of these mechanisms are as follows:</u>

(1) Acknowledgement of public and private obligations to control the uses of artificial intelligence:

The aforementioned European project has established two types of obligations as a mechanism to control the uses of artificial intelligence, namely public obligations and private obligations. In this regard, we are interested in seeing how these two obligations are positive and their repercussions on the guarantee of personal data privacy.

General obligations mean those imposed on all applications of artificial intelligence regardless of their classification in terms of degree of risk, and these

obligations seek to ensure the responsible development, deployment and use of artificial intelligence systems.

This is highlighted by the analysis of Articles 8 and 9 of the European Parliament's draft in its affirmation of adherence to transparency and protection of personal data, where the processing of data for use in artificial intelligence systems should adhere to the established principles of data protection, such as accuracy, proportionality, fairness, and adherence to the necessary minimum limits, and this ensures responsible practices for both the collection, use, and storage of data, on the one hand. On the other hand, the project added two important obligations within the framework of the general obligations of service providers with artificial intelligence mechanisms. Article 17 of the project stipulates that all artificial intelligence systems shall be designed and developed to ensure the safety of people, considerations of their intended uses, and potential damage, including measures to reduce risks and prevent harm. Article 60 also imposed that developers and providers of artificial intelligence systems should take appropriate measures to ensure the security and confidentiality of the data used in these systems, meaning that the information available in a database is publicly available, with the assurance that it will not contain personal data except to the extent necessary to process the information. This will be done under the responsibility of the European Commission in terms of database management and ensuring the provision of appropriate technical and administrative support to system providers. (artificial intelligence) Alongside general obligations, EU AI law creates **special requirements and obligations for AI systems** classified as high-risk as these requirements aim to deal with this risk category and ensure that these systems are responsibly developed, deployed and used.

(2) Data governance as a means of securing personal data:

The relationship of artificial intelligence systems to the collection, processing and storage of data, especially personal data, has sparked widespread controversy,so the data governance guarantee is one of the main requirements that any regulatory framework for artificial intelligence technology should seek to cover, and it is one of the most prominent principles adhered to by the European draft law for the protection of personal data used by artificial intelligence applications.

The mechanisms of personal data governance are represented in several aspects, namely the establishment of controls for the collection and processing of data. Article 10 of the Artificial Intelligence Bill approved by the European Parliament imposed the need to ensure that appropriate design choices are made with regard to data collection operations, taking into account the relevant legal frameworks and ethical principles, such as establishing transparency regarding the source of data, especially personal data, and taking into account the original purpose of data collection.

The same article stipulated the need to document data preparation processes, such as appending distinguishing marks and cleaning the data, and compiling them in a categorical manner suitable for their intended use. In addition to the above, another mechanism to support the governance of personal data emerges. This is also exemplified by Article 59 of the European project that individuals have the right to access data used in high-risk artificial intelligence systems that affect them, in addition to information about the logic of its processing and decision-making related to it.

Another mechanism for the governance of personal data can be added to the provision of Article 61 of the same project to set time limits for data retention. The data should not be retained for longer than necessary for the intended purpose, taking into account both legal obligations and potential risks. Despite the appreciation of these efforts by the European Parliament to establish the first semi-integrated law to regulate artificial intelligence, which aims, among its various purposes, to protect the privacy of personal data provided by individuals for the purpose of obtaining public utility services and others, it is regrettable that it has not activated a specific mechanism to compensate for the damage caused by the uses of artificial intelligence. Guided by the above, it can be said that the ethical guarantees for the use of artificial intelligence technologies are in dire need of a binding framework to activate their role as an effective officer to reduce the risks of compromising the privacy of personal data. It is expected that future artificial intelligence laws will provide a more unified regulatory framework to address the risks resulting from the use of these technologies ,especially with the European project included in Article 56on the need to establish a body on behalf of the European Council for Artificial Intelligence, which is supposed to play a vital role in supporting the implementation of the Artificial Intelligence Law and guiding its future development. (European Artificial Intelligence Board)

8. The Extent to which the supervisory role contributes to supporting privacy as an ethical guarantee?

Despite the keenness of many countries and concerned entities to launch ethical charters to control the use of artificial intelligence systems technologies, the ethical guarantees contained in these charters are not enough to stand by it only without seeking mechanisms to ensure their activation, which reflects positively on achieving this goal. Having already addressed the limits of the legislative role in this regard in establishing a mandatory framework for these charters, we find it appropriate to determine the impact of the supervisory role on the extent to which the ethical principles and guarantees contained in these charters are respected, including the guarantee of privacy. In this regard, some legislative and regulatory frameworks at the Arab level have been keen to establish formal mechanisms to control the use of artificial intelligence systems (The Shura Council)**,** which requires shedding some light in this regard to determine the extent to which these mechanisms contribute to controlling the

administration's use of artificial intelligence systems at the level of the Bahraini legislator and at the comparative level in general and protecting privacy as a guarantee in particular.

At the national level, the proposed law approved by the Shura Council, as mentioned above in Chapter Five, embodied the establishment of the Artificial Intelligence Unit, with recognition of its members as judicial officers, and entrusted it with several supervisory competencies over the exercise of artificial intelligence activities in light of the provisions of the proposed law. Article 15 of this proposal outlined these regulatory competencies, the most prominent of which is the tightening of control over artificial intelligence systems and their uses to reduce the risks arising from misuse, and the development of strong security systems to protect confidential information and personal data. In addition to the above, perhaps the most prominent among these terms of reference of this unit is proposing standards for the use of artificial intelligence in accordance with international ethics and standards of use and presenting them to the Minister for a decision after presenting them to the Council of Ministers. This represents an important pillar for controlling the uses of artificial intelligence systems according to ethical standards.

At the comparative level, the Code of Ethics for Artificial Intelligence issued by the Saudi Authority for Data and Artificial Intelligence (SDAIA) issued in September 2023 has highlighted several mechanisms to control and follow up compliance with the principles of this Charter, and these mechanisms vary from the level of the implementing agencies to the national level. At the level of the implementing agencies, the entity shall be responsible for ensuring that it is ethically and ethically funded, in accordance with its own medical principles , and in accordance with its ethical principles, through the use of artificial resources, and in accordance with its ethical principles, and in accordance with the principles of human rights, and in accordance with the principles of human rights. While the manifestations of control at the national level are embodied in the work of the Saudi Authority for Data and Artificial Intelligence (SDAIA) in carrying out a challenge and challenge to the development of ethical standards and guidance of the industrial sector, which includes the management of national institutions, including the management of national institutions. The Authority relies on several multi-pronged mechanisms to accomplish its supervisory mission on the extent of commitment to artificial intelligence ethics, including : the preparation of an ethical challenge to industry intelligence, when the need arises, and the preparation of an ethical plan to raise awareness of this need, and the state of awareness of this need. The medical service provider is funded by the medical service provider, who provides the medical service provider with an ethical, industrial,and applied service provider, as a whole, who is responsible and humiliating for the development of the medical service provider. Ethically,it is also possible forthe Tensing Authority to

applythe ethics of artificial intelligence in the sector that is subject to regulation by the Tensing Authority. (Saudi Authority for Data and Artificial Intelligence)

The European project, in turn, provided in Articles 26 and 27 of the aforementioned draft law on the regulation of artificial intelligence, the right to complain by the concerned parties to the concerned authorities in the event of violation of the provisions of the law, and to request information about high-risk artificial intelligence systems that affect them in order to allow these authorities to verify this violation, and take the necessary measures.

It can be concluded from the above that the supervisory role of the competent or concerned entities provides a positive step towards the activation of ethical guarantees, including the guarantee of privacy if it is carried out within a framework of continuity, objectivity and evaluation of the extent of compliance with the regulated standards specified by the regulating legislation and ethical charters in this regard, provided that this role is accompanied by granting these supervisory authorities the authority to stop the use that violates the ethical guarantees according to specific controls as a mandatory step, and therefore this supervisory role will have a prominent contribution to controlling the administration's uses of artificial intelligence.

9. Conclusion

Artificial intelligence is one of the obvious manifestations of the scientific development of humanity. Artificial intelligence in general means the machine's simulation of human mental abilities. It emerged as a promising technology in the last century that would have brought about a major transformation in all aspects of life in general, and in turn was reflected in the performance of countries and their authorities. In this context, the advantages of this promising mechanism and its positive repercussions must be balanced with strict privacy protection through cooperation between governments, companies, and users to ensure the safe and ethical use of artificial intelligence, by introducing continuous controls and legislation. This is the key to protecting privacy in this accelerated digital age. Many countries, including the Kingdom of Bahrain, are working globally to develop and implement artificial intelligence regulations to guide the ethical and responsible use of artificial intelligence technologies. These regulations aim to achieve a balance between innovation and ethical considerations and to protect individuals and society from potential risks associated with artificial intelligence innovations. In this context, privacy is an indispensable ethical guarantee in the use of artificial intelligence in public facilities. By respecting the privacy of individuals, a balance can be achieved between taking advantage of modern technologies and protecting human rights, which ensures the enhancement of confidence in artificial intelligence and its use in a fair and sustainable manner.

Thus, the role of activating privacy as a guarantee confirmed by many ethical charters to control the administration's use of artificial intelligence

systems in the field of public utilities, and in a way that limits the risks of this use as discussed in the study.

This study has resulted in some results and recommendations, which we present as follows:

1. Artificial intelligence is the machine simulation of some human mental abilities through specific technologies designed for specific purposes.
2. Privacyis the circle close to the human being, which includes his private affairs related to him, whether in his individual, family or professional life.
3. The right to privacy is of a special nature. It is a constitutional right that finds its basis at the national level in the Constitution on the basis of what is enshrined in constitutional texts on the one hand, and being a human right at the international level on the basis of what is embodied in the texts of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights on the other hand, and a third party that is considered a right intrinsic to personality and therefore has criminal and civil protection in accordance with the special rules in this regard.
4. Privacy is one of the fundamental aspects of the ethical safeguards that must be observed when using artificial intelligence in public facilities. Despite the great benefits offered by artificial intelligence in terms of improving services, increasing efficiency, and reducing costs, the irresponsible use of this technology may lead to a violation of individuals' privacy, which raises many ethical and legal concerns.
5. The continuous and steady growth in artificial intelligence applications is not matched by a parallel growth in processing and legislative regulation, which creates a state of deficiency in covering the damage caused by its uses.
6. The accelerated growth of the uses of artificial intelligence creates great difficulty in setting ethical standards that govern, control and keep pace with this use.
7. It has become necessary and inevitable to establish ethical controls for the uses of artificial intelligence to mitigate the uncalculated risk in its escalating growth.
8. Commitment to ethical AI helps positively impact society and sets the standard for responsible AI practices.
9. Regulations and adherence to them contribute to ensuring that AI technologies are developed and used responsibly so that innovation and integrity can be balanced, and that AI serves humanity in a positive and beneficial way.
10. The entities concerned with oversight of the administration's use of artificial intelligence systems represent a positive mechanism towards the activation of ethical safeguards, including the guarantee of privacy.

There are many recommendations as follow:

1. Establishing ethical standards that are agreed upon at the official and private levels and that are adopted within the framework of a formal system of unified commitment by all public and private law persons.
2. Supporting the development of the database on the uses of artificial intelligence, provided that it is coupled with it as a system for operating a set of ethical duties as a technical officer to reduce the tendency of self or personal use of these uses.
3. Privacy should be an essential part of the design of AI systems from the outset, so that technologies such as encryption, anonymization, and limiting data collection ensure that these systems are compatible with ethical principles.
4. The technical qualification and ethical preparation of those in charge of providing public utility services while providing a binding guide, and thus the ethical implications of artificial intelligence can be better addressed when they have a good understanding of different artificial intelligence concepts through the holding of training programs and workshops on topics such as bias, transparency, accountability and data privacy.
5. Preparing advanced programs to educate AI users to access public utility services on how to deal with the risks expected from such use, thus enhancing the use of privacy protection tools such as virtual private networks (VPNs) and anti-tracking programs.
6. Appealing to the legislator to proceed with the enactment of an integrated artificial intelligence law that takes into account the adoption of technical and ethical guarantees associated with the imposition of sanctions and deterrent penalties in the event of waste to provide safe use.
7. Directing entities and institutions to create unbiased artificial intelligence systems using diverse data sets, prioritizing privacy, and ensuring data security, to be effective and ethical at the same time.
8. We recommend integrating ethical considerations such as fairness, transparency, accountability and privacy into the development of AI applications in general and in the provision of public services in particular, in order to innovate technologies that go beyond innovation and adhere to the highest standards of responsibility.
9. Recommending moving forward towards the establishment of specialized independent entities entrusted with specific tasks of technical and administrative control over the uses of management and companies for artificial intelligence systems, while recognizing them with strong powers to ensure their proper control so that these systems are subject to periodic audit to ensure their compliance with ethical and legal standards.

References:

Abdellatif, M. M. (2021, May 24). responsible for artificial intelligence in public and private law, research submitted to the Conference on the Legal and Economic Aspects of Artificial Intelligence and Information

Technology. p. p. 12.

Alan, E. B.-S. (March 2020). *Ethics of artificial intelligence: issues and initiatives.* European Parliamentary Research Service Scientific.

Al-Homsani, S. (1979). *The Pillars of Human Rights: A Comparative Research in Islamic Law and Modern Laws.* Egypt: Dar Al-Alam for Millions.

Al-Mujam Al-Wasit, Al-Maani Al-Jamaa Complex. (n.d.).

(April 24, 2024). *Article Thirteen of the proposal attached to the report submitted by the Legislative and Legal Affairs Committee of Majlis Al-Shura*. unpublished.

Article 1 of the proposal attached to the report submitted by the Legislative and Legal Affairs Committee of Majlis Al-Shura. (24 April 2024). *Article 1 of the proposal attached to the report submitted by the Legislative and Legal Affairs Committee of Majlis Al-Shura*.

(15 July 2020). *Published in the Egyptian Official Gazette, Issue 28bis(E).* the Egyptian Official Gazette.

Law No. 78-17 , on Information Technologies, Data Files and Individual Liberties. (1978, January 6). Retrieved from https://www.wipo.int/wipolex/ar/legislation/details/18963

Azzawi, D. S. (2000). Views on Democracy. p. p.81.

Bakheet, M. S. (2023). The Impact of Artificial Intelligence Applications on the Development of Public Utility Services (Smart Management as a Model). *Forty-third Issue*, p. p. 3405.

Boddington, P. (2017). *teaches philosophy.* the New College of the Humanities, London: Springer.

(16 December 1966.). *International Covenant on Civil and Political Rights.*

(n.d.). *Transparency and accountability in AI systems safeguarding wellbeing in the age of algorithmic decision-making.* Retrieved from https://www.frontiersin.org/journals/human-dynamics, doi 10.3389/fhumd.2024. 1421273..

Commission euro penne. (8avr.2019). *Lignes directrices en matière d 'éthique pour une intelligence artificial digne de confi.*

Council, t. L. (April 24, 2024). *Article 5 of the proposal attached to the report submitted.* the Legislative and Legal Affairs Committee of the Shura Council.

(1948). *Article 12 of the Universal Declaration of Human Rights.* Paris: the General Chest, B.

Dr. Fahad Saeed Al-Dhuhoori, M. A.-N. (2024, March). The Administration's

Responsibility for the Uses of Artificial Intelligence on the Basis of Error. *Volume 21*, p. p. 308.

Draft Arab Charter for the Ethics of Artificial Intelligence. (n.d.). *Ministry of Communications and Information Technology in coordiwithin the project on Responsible Artificial Intelligence Governance for Development.* Palestine : Ministry of Communications and Information Technology in coordination with Birzeit University.

European Artificial Intelligence Board. (n.d.). the 'Board') is established.

European Parliament. (n.d.). Retrieved from https://www.europarl.europa.eu

Fawzi, W. (2024). *Principles and Ethics of Artificial Intelligence, Al-Bayan Center for Studies and Planning.*

Glaser, A.-S. C.-G. (2018). *Responsabilité civile du fait du robot doué intelligence artificielle:faut-il créer une responsabilité robotique?*

Glenn, R. (2003). *The Right to Privacy: Rights and Liberties under the Law (America's Freedoms).* ABC-CLIO.

Huang, C. (2023, August). An Overview of Artificial Intelligence Ethics, IEEE, Transaction, Vol, no4,9. *Vol, no4*.

Karim, A. A. (2024). The Ethical Risks of Artificial Intelligence Applications, Analytical Study. *Journal of the Faculty of Education, Benha University, Egypt, , Issue 137*, Issue 137, C(1) p. 341.

Mahmoud, W. R. (2022, April). Constitutional and Legal Protection of Personal Data, Comparative Study between Egyptian and French Legislation,. *Volume 113*(Part Two), p. p. 397.

Masaar. (n.d.). *Masaar* . Retrieved from Masaar : https://masaar.net/ar

McCarthy. (1989). *Artificial Intelligence, Logic, and Formalizing Common Sense Philosophical Logic and Artificial Intelligence.* .

McCarthy. (1993). *Artificial intelligence A Philosophical Introduction 1st Edition, Wiley-Blackwel.*

Mengchen Dong, K. B. (2024). *Responsibility gaps and self-interest bias: People attribute moral.*

Merriam-Webster. (n.d.). *"Right of privacy." Merriam-Webster.com Legal Dictionary.*

Miller, K. (2024, March 18). Privacy in an AI Era: How Do We Protect Our Personal Information's? human cantered artificial intelligence,.

Musa, A. H. (n.d.). Moral Obligation and Legal Obligation, Nature and Scope.

others, L. F. (2018). *AI4 People —An Ethical Framework for a Good AI Society.*

political encyclopedia. (n.d.). Retrieved from https://political-encyclopedia.org/dictionary/

Rabhi, A. H. (n.d.). Limits of liability of the public utility for the uses of artificial intelligence devices? . *Introduction to the Conference on Artificial Intelligence. unpublished.* Facultyof Law, Universityof Sharjah, unpublished.

Ramos, G. (n.d.). *Ethics of Artificial Intelligence.* Retrieved from unesco: https://www.unesco.org/ar/artificial-intelligence/recommendation-ethics

Saleh, D. t. (2000). The Reality of Computer Crimes in Jordanian Penal Legislation. (p. p.10). the Faculty of Sharia and Law, United Arab Emirates University.

Saudi Authority for Data and Artificial Intelligence (sdaia. (September 2023). *Principles of Artificial Intelligence Ethics.*

Saudi Authority for Data and Artificial Intelligence. (n.d.). *the Principles of Ethics of Artificial Intelligence.* Retrieved from https://sdaia.gov.sa

Smart Dubai. (2021). *Principles and Guidelines for the Ethics of Artificial Intelligence.*

Sorour, A. F. (1978). The Right to Private Life. *Journal of Law and Economics, , No. 54*, No. 54, p. 47.

Taylor, J. (2020). forecast combinations for value at risk and expected short fall. *36*, p. p428.

The Egyptian Supreme Constitutional Court. (1972). *The judgment of the Egyptian Supreme Constitutional Court in the session of March 18, 1995in Case No. 23 of 16 judicial year after the constitutionality of the sixth item of Article 73 of the State Council Law promulgated by Law No. 47* .

The European Commission. (2021). *The draft law.*

The European Court of Human Rights (ECHR). (5 September 2017). *Judgment of the European Court of Human Rights (ECHR)in Case No. 61496/08.*

The Shura Council. (n.d.). *Principle 16 of the Egyptian Charter for Responsible Artificial Intelligence.*

the website of the National Portal of the Kingdom of Bahrain. (n.d.). Retrieved from https://bahrain.bh/wps/portal/ar/

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2021). *The Recommendation on the Ethics of Artificial Intelligence.*

United Nations Educational, Scientific and Cultural Organization (UNESCO). (November 22, 2021). *Recommendation on the Ethics of Artificial*

Intelligence.

United Nations. (n.d.). *United Nations*. Retrieved from www.un.org

Veena, A. (2024, July 19). *The ethical use of AI balances innovation and integrity*. Retrieved from https://www.ultralytics.com/ar/blog/the-ethical-use-of-ai-balances-innovation-and-integrity