Legal Protection of Digital Data in the Age of Artificial Intelligence

Article · September 2024

CITATIONS
0

READS
66

1 author:

Murtada Abdalla Kheiri
A'Sharqiyah University
63 PUBLICATIONS **69** CITATIONS

SEE PROFILE

Letters in High Energy Physics
ISSN: 2632-2714
Volume 2024

Legal Protection of Digital Data in the Age of Artificial Intelligence

Murtada Abdalla Kheiri1*, Nizar Qashta2, Dorgham Issa Aljaradat3
1,2Associate Professor at A'Sharqiyah University, Ibra, Oman
3Assistant Professor of Islamic Jurisprudence, College of Islamic Sciences, Palestine

Abstract:

Today, the world is witnessing rapid development in the field of technology, especially with the emergence of artificial intelligence and its multiple applications in our daily lives. Along with this development, new challenges have emerged that threaten our digital privacy. This research aims to examine these challenges and their impact on our daily lives. In addition to reviewing the current legal framework for the protection of personal data and proposing solutions for future challenges.

The main problem lies in the increasing ability of smart devices to collect and analyze vast amounts of personal data, which heightens the risk of privacy violations. Additionally, the difficulty of keeping legal regulations up to date with the rapid advancements in the field of artificial intelligence further complicates the problem. Additionally, the difficulty of keeping legal regulations up to date with the rapid advancements in the field of artificial intelligence further complicates the problem. The research also seeks to raise awareness among individuals and organizations about the importance of protecting their data and taking the necessary measures to safeguard it.

The research aims to: identify the data that deserves legal protection, analyze the impact of artificial intelligence on digital privacy, review international, regional, and Omani laws for the protection of personal data, and propose solutions to the challenges of protecting digital privacy in the context of artificial intelligence.

This research aims to contribute to the understanding of the legal and technical challenges arising from digital privacy violations in the age of artificial intelligence. The research, along with others, is expected to contribute to the development of legislation and laws to protect personal data and ensure individuals' rights to privacy.

Keywords: Digital Privacy, Artificial Intelligence, Personal Data Protection, Legal Legislation, Technology.

Introduction

Globalization has significantly contributed to shrinking time and space, turning the world into a small village where it is easy to reach any individual at any time, place, and under any circumstances. This has led to a qualitative shift in individuals' lives on all levels. The rapid technological advancements have raised many security concerns regarding privacy and digital safety, which are now at risk. Especially with the technological advancements that introduced features in smartphones capable of reading, understanding, and identifying facial expressions, determining the user's emotional and psychological state, tracking the most frequently used words, measuring the time spent on various applications, and even pinpointing the user's geographic location without being connected to the Internet. In addition, knowing everything typed on the phone via the keyboard allows hackers and smart applications to access sensitive personal data such as credit card passwords, as well as browsing history and communications (Samir Ziada, 2020).

The right to privacy is one of the rights inherent to human beings, and private life and its sanctity are protected in ancient civilizations, heavenly religions, constitutions, and positive laws.

With the advent of computers, smartphones, and the Internet, this right has gained a new dimension, particularly with social media communication over the Internet. People, both adults and children, share a significant amount of their personal information, photos, and videos related to themselves and their families on the Internet. This creates a risk of violating individuals' private lives in the realm of information technology.

The recent revolution in artificial intelligence has introduced many challenges and increased the risk of privacy violations due to its advanced features, vast storage capacity, and capabilities for analysis,

inference, and judgment. This has created numerous legal challenges, and this research will address the most prominent of these challenges, as well as the legislation and laws that have framed the ways of handling personal data and digital privacy.

Research Problem

The research problem lies in the legal implications and consequences of addressing the challenges of digital privacy in the context of the artificial intelligence revolution. These challenges have heightened the risk and deepened the impact of personal data violations, especially with the difficulty of regulating and keeping up with self-learning intelligent systems that rely on vast databases and complex algorithms. This poses a challenge to legislation at the global and regional levels in finding laws that control this huge revolution in information systems.

Research Importance

The importance of this research lies in its relevance to contemporary electronic issues and modern legal trends in the use of artificial intelligence technology. Additionally, the research highlights the importance of safeguarding personal data and digital privacy in the face of the ongoing challenges brought about by the artificial intelligence revolution. It also focuses on the most prominent laws and legislation that have addressed the numerous challenges related to the protection of personal data and digital privacy.

Research Objectives

- Define personal data and its characteristics.
- Identify the personal data that requires protection under laws and legislation.
- Highlight the importance of personal data in cyberspace and the necessity of its protection.
- Clarify the impact of artificial intelligence on the violation of digital personal data and the resulting legal challenges.
- Explain the scope of the right to privacy and the key principles of its protection.
- Shed light on global, regional, and Arab laws and regulations regarding the protection of digital personal data.
- Review Omani law and its key provisions related to the protection of personal data.

Research Methodology

The research adopts an integrative scientific approach that combines descriptive and analytical methods. It involves describing and defining the issue, as well as presenting opinions on it. The research also employs the historical method to outline the legislation related to personal data protection, as well as the comparative method to present different legal opinions. It then analyzes the data and viewpoints to reach conclusions.

Research Outline:

The research consists of two chapters, followed by a conclusion, as outlined below:

Chapter One: Digital privacy in the age of artificial intelligence.

Section One: Personal data and the importance of its protection.

Section Two: The concept of digital privacy.

Section Three: The impact of the artificial intelligence revolution on digital privacy.

Chapter Two: The legal framework for privacy protection.

Section One: Principles of personal data protection.

Section Two: Laws for the protection of personal data.

Section Three: Personal data protection in Omani legislation.

Conclusion: Contains key findings and recommendations.

Chapter One: Digital privacy in the age of artificial intelligence

Section One: Personal data and the importance of its protection

Personal Data: Refers to data that has been processed to achieve a specific purpose or for a defined use in decision-making processes. In other words, personal data is information that has gained value after being analyzed, interpreted, or meaningfully compiled. It can be exchanged, recorded, published, and signed in either formal or informal forms, or other formats (Mona Al-Ashqar & Mahmoud, 2018, 118).

The British legislator defined It as information about a living person that can identify them or, when combined with other information held by the data controller or potentially in their possession, can identify them (UK Data Protection Act, 1998)

Personal information is divided into two categories:

Ordinary personal information, which is subject to general regulations. Sensitive personal information is subject to general regulations as well as specific provisions. Examples of sensitive personal information include: racial or ethnic origin, political opinions, union membership, or health information, including genetic data (Article 4, Moroccan Personal Data Protection)

Although laws generally guarantee the protection of privacy, the concern over risks increases when it comes to sensitive personal data. It appears that the reasons for protection in this context stem from concerns over racial or ethnic discrimination, classifying individuals for the purpose of exclusion, tracking, surveillance, or favoritism toward certain groups, among other forms of discrimination (Al-Arabi Jinan, 2010, p 10).

Ordinary personal data can turn into sensitive data if certain circumstances arise that add a level of risk to them (Swailem Khaled, p 1889)

Characteristics of personal data:

1- They are rights related to human personality, such as retaining the personal data of any natural person, such as his right to retain his thoughts and the confidentiality of his relationships, which is not available in reality to the legal person.

2. They allow for the identification of a person, either directly or indirectly. This includes civil status and identity data, or data related to physical characteristics, or implicitly, such as age, gender, and occupation. These data are often used in various ways to assist the judiciary (Tlemcen Younis, 2008, p19)

Some studies suggest that data collected in personal accounts (profiles) on social media essentially represent an identity document, as the information available through these profiles pertains to personal privacy and is thus necessarily considered confidential.

Websites and applications may collect this information about users to improve and develop the services offered. Some of the key information collected includes Cookies, personal details, links, publication policies, private information, visitor and user statistics (Maha Al-Khathami, 2017, p 370), and sometimes stored communications and contacts on the device. These data are typically stored on the servers managing the website or application.

According to a study conducted by the Pew Research Center, most adults surveyed feel that privacy is being compromised in key aspects, such as the security of personal information and the ability to maintain privacy.

The same study revealed that 62% of respondents were willing to share some personal information in exchange for free services through smart applications, which are often sent to third parties such as advertising companies.

It may seem that the data shared on social media does not pose a risk to individuals, but in reality, it could present a significant danger if it falls into the hands of ill-intentioned individuals who exploit it for unlawful purposes such as blackmail, defamation, threats, and identity theft. Websites and applications may also exploit this data for commercial advertising and other purposes. Therefore, processing personal data is considered a form of violating human rights, specifically the right to privacy.

In fact, this data is considered to be of great value to economic entities seeking to develop their profits and attract new and large categories of consumers by exploiting the traces of their personal information that they leave on the information system, whether it is a computer, an information bank, a phone, a website, or a personal paper file such as a CV and acquaintance forms. The idea is based on examining, studying, and understanding the preferences and interests of individuals to become a fundamental pillar in the world of electronic commerce (Al-Jubouri, 2015, p 9)

It can also be exploited by certain companies for the benefit of political entities, as happened with Cambridge Analytica, which leaked the personal data of approximately 87 million Facebook users for the company's use during the 2016 presidential election campaign. In the referendum on the UK's

withdrawal from the European Union, emails were sent to influence voters' choices. These messages were designed to be deleted within two hours to impact the referendum results (Al-Hafezi, 2017)

Personal data, as aimed to be protected by laws and regulations, refers to any data, regardless of its source or format, that can identify a natural person directly or indirectly. This includes data such as voice and images, according to the definitions provided by Tunisian and Moroccan legislators. Personal data, as aimed to be protected by laws and regulations, refers to any data, regardless of its source or format, that can identify a natural person directly or indirectly. This includes data such as voice and images, according to the definitions provided by Tunisian and Moroccan legislators (Sheikh, & Sayed, 2018, p 8).

Section Two: The concept of digital privacy

In legal terminology, privacy is defined as an individual's freedom to choose their personal life without interference, and without the ability of others to access or publish it without their consent. This extends to all aspects of a person's life, including their family, professional, health, and romantic life, as well as their income, religious, intellectual, and political beliefs, correspondence, conversations, and all non-public aspects of their personal and professional life (Al-Muqabali, 2024)

Privacy of information: is the individual's right to control the collection, processing, and storage of their personal data. This includes regulating how such information is gathered, distributed, and used (Al-Ostath, 2013, p. 433).

Some researchers have defined it as the right of individuals to determine when, how, and to what extent their information reaches others.

Some legal scholars define it as the ability of individuals to control the flow of information related to them (Ayoub, 2009, p. 56).

Violation of privacy or personal life: Refers to accessing, disclosing, or using another person's private matters without their knowledge or consent, even if the information is not classified as a secret (Lami, 2017, p 6).

Privacy is violated through modern electronic means, especially smartphones, which are equipped with advanced cameras that allow taking pictures and videos from long distances. Similarly, voice recording devices in phones, call and message recording mechanisms, and other technologies may be used unlawfully to infringe upon others' lives, track their conditions, and disseminate this information through social media, reaching millions of people without the knowledge of those being recorded.

The concept of personal information privacy includes a number of dimensions (Al-Sheiti, 2014, p 4), which are:

1- The privacy of the person related to his physical safety, such as vaccination or blood transfusion without the person's permission, or forcing him to provide samples of body fluids or tissues.

2- Information privacy, which includes the rules governing the collection and management of personal data, such as ID card information, financial data, and more.

3- Communication privacy, which includes the freedom and privacy of phone correspondence, emails, etc.

4- Territorial (spatial) privacy, which pertains to the regulations governing entry into homes, workplaces, or public spaces, as well as tracking a person's geographic location.

All aspects of privacy are protected in laws and regulations, as they are part of an individual's personal rights, and they may not be violated.

The term "electronic privacy protection" refers to safeguarding personal data stored in information systems from the risks of automated processing (Arab, 2001, p. 2). Privacy policies are documents that define the extent of electronic privacy protection, how this privacy is exploited, and the resulting ethical and legal issues (Al-Jaradat, 2022)

Section Three: The impact of the artificial intelligence revolution on digital privacy.

The recent revolution in artificial intelligence has posed numerous challenges and increased the risk of privacy violations due to its advanced features, immense storage capacity, and ability to analyze, infer, and make judgments.

The widespread use of artificial intelligence applications has increased the potential for violations of individual rights, including the following prominent issues:

1-The Right to privacy: Artificial intelligence primarily relies on the collection of big data, and personal information is often gathered without individuals' consent or knowledge, leading to privacy violations. This data may be used in ways that do not align with individuals' desires (European Union Charter).

2-The Right to equality and non-discrimination: Artificial intelligence depends on certain algorithms built on specific databases, which may include intentional or unintentional biases. This can result in discrimination against certain groups or communities. For example, if a model is trained on data containing historical biases, it could lead to discriminatory outcomes in areas such as employment, lending, and other fields (Article 26, 27 of the International Covenant on Civil and Political Rights, Al-Jabour, 2024)

3- The Right to freedom of expression: Artificial intelligence systems may impact the right to expression by monitoring online content or imposing certain restrictions on what can be written or spoken. Techniques such as sentiment analysis or voice recognition can also be used to determine acceptable or unacceptable content (Article 25 of the International Covenant on Civil and Political Rights)

4- The right to security: AI systems have advanced technologies for surveillance, tracking, and control, which can threaten personal security. These systems and companies can monitor and track an individual's location, enabling governments to impose stricter restrictions on freedom of movement. As well as predicting an individual's path, which is an area where errors are possible if automation and decision-making are entrusted to artificial intelligence technologies (Taha, 2023, p 447).

5- The Right to access information: The way algorithms function may limit access to certain information by directing individuals to view specific content based on algorithmic preferences. This can influence individuals toward making certain decisions or choices while withholding other information that may be equally important (Taha, 2023, p 447-448).

Legal challenges to the right to information privacy in the age of the AI revolution:

The major issue with AI systems is that they lack a central authority to which one can refer, as they are not owned by anyone in particular. AI applications are widely accessible and can be used by any individual or entity. The legal challenges to privacy protection in light of this revolution can be summarized as follows:

1- The speed of technological development makes it difficult for laws to keep up with these successive changes. Laws that were appropriate in the recent past may not be effective in confronting accelerating technological innovations.

2- Big and complex data: The data used in artificial intelligence is vast and complex, making it difficult to identify its source, control it, and manage how it is processed. This poses a challenge in enforcing laws related to data protection.

3- Privacy vs. innovation: There needs to be a careful balance between promoting innovation and protecting privacy. Strict restrictions on data use may hinder the development of new technologies, creating a conflict between these two demands (Innovation in Data Privacy, 2024).

4- Cross-border regulation: Many companies operate in global environments, collecting and processing data across different countries. This requires international coordination in laws and regulations, which is highly complex due to varying cultures and legal frameworks among nations.

5- Discrimination and bias: AI algorithms can lead to biased decision-making or unfair discrimination, necessitating a clear, advanced, and up-to-date legal framework to address such issues and ensure fairness (Technological prejudice, 2024)

Chapter Two: The Legal Framework for Privacy Protection.

Section One: The Scope of the Right to Privacy and Principles of Protection.

The principle of the right to protect private life is widely agreed upon globally, but there are differences in its practical application. Every

individual has the right to prevent intrusion and curiosity from others and to control the dissemination of information about themselves or their family. He also has the right to take measures he deems appropriate to protect this aspect of his life. Laws generally agree that the foundation of privacy protection is an individual's personal right to the sanctity of their private life. This implies that individuals have the right to seek judicial intervention to stop or prevent violations of their privacy without waiting for harm to occur. It also imposes a general obligation on everyone to respect this right (Sorour, 1991, p 13).

There are two main factors that generally define the scope of privacy:

1- Individual interest: This encompasses personal freedom and the sanctity of one's private life.

2- The Right of Society: This involves the community's interest in guiding individual behavior and obtaining certain data about individuals through lawful means to protect public interests such as security, public order, and the right to information.

There must be a balance between these two rights, considering that private life is not just an individual issue but also a social and security concern. Protecting privacy is a societal necessity if it contributes to the stability and security of the community (Othman, 2006, p 18)

The fundamental principles that should be considered when processing personal data can be summarized as follows:

1. Transparency and legality: The processing of any personal data must be carried out clearly and lawfully by informing individuals about how their data will be used and the purposes for which it is being processed.

2. Purpose limitation: Collected data should not be used for purposes other than those for which it was originally collected.

3. Data limitation: It is not permissible to collect unnecessary data about users.

4. Accuracy: Ensure data is accurate and up-to-date by taking practical steps to correct any errors in the information.

5. Storage limitation: Personal data should not be kept for longer than necessary to achieve the purposes for which it was collected (Lilian, 2019, p 46).

Section Two: Laws and regulations for personal data protection.

Human rights laws vary from country to country, particularly concerning the violation of privacy through technological means. European countries have strict laws that stand against any violation of an individual's privacy. Therefore, smart applications are required to protect user information and comply with the privacy conditions imposed on them. In the Middle East, most countries in the region have been late in issuing strict laws in this regard, which has allowed some applications to violate users' privacy without fear of legal accountability. Technology experts have warned about the dangers of privacy violations in some applications and have urged users to seek alternative, more secure apps (WhatsApp is not alone, 2024)

Global and regional efforts in this regard can be summarized as follows:

International Conventions:

1. Universal Declarations: Such as the Universal Declaration of Human Rights issued by the United Nations in 1948, which affirmed the right to privacy for individuals, highlighting the international community's commitment to protecting this right (Declaration of Human Rights, 2024).

2. Budapest Convention: This is one of the most prominent international agreements aimed at combating cybercrime. It seeks to enhance cooperation between countries in the field of personal data protection and combating cybercrimes in light of the use and development of technology. The convention was adopted in 2001 and came into effect in 2004 (Balas, 2021, p 14).

International Organizations:

1. United Nations: The UN General Assembly has emphasized the protection and promotion of human rights, including the right to privacy. The UN has affirmed this right in the context of the internet to the same extent as it is protected offline. It issued a special report on protecting individuals' privacy from electronic surveillance, interception of digital

communications, and data collection (Right to Privacy in the Digital Age, 2014).

The UN reinforced this protection with Resolution 7/34, one of its key provisions being the expansion of privacy to include data collected and analyzed through various technological means and algorithms. The resolution stated that even mere access to or secret surveillance of individuals' private data infringes upon the right to privacy (Right to Privacy in the Digital Age, 2018).

2. Organization for Economic Co-operation and Development (OECD): It was one of the first organizations to establish a set of guidelines for the protection of the right to privacy in information, introduced in 1980. It issued a set of rules under the title (Guidelines for the Protection of the Right to Privacy and the Free Flow of Data) (Abu Bakr, 2022, p. 78). They were reviewed and updated in 2013 (Organization for Economic Co-Operation and Development, 2013).

Regional Cooperation

1-The Council of the European Union: It has issued several decisions since 1981 AD that approved the protection of private data, as it set strict standards on how data is collected and used. It has also affected many countries that deal with European citizens' data (Jabour, Mona Al-Ashqar, and Jabour, Mahmoud, 2018, p. 52).

It was updated in 2016 under the title (European Data Protection Regulation) (Law No. 679/2019, Al-Salmi, 2008).

2. Arab League: The Arab agreements on combating cybercrimes, held in Egypt on 25/12/2010, followed the approach of global organizations in protecting and respecting the right to privacy. The agreements aimed to enhance cooperation in the field of information and technology and to combat cybercrimes (Ben Salem & Al-Shaibani, 2023, p 465).

International Legislation

The first law related to personal data protection appeared in the German state of Hesse in 1970, followed by Sweden in 1973 (Toby, et al., 2016, p. 52). By 2016, the majority of countries had established specific laws related to personal data protection, with reports indicating that 108 countries had implemented such laws (Directive 95/46/EC of the European Parliament).

Arab Legislation:

Arab legislation has shown concern for the right to digital privacy by either applying traditional legal provisions to this new concept or by introducing specific laws. Examples include:

Tunisian Law: In 2004, Law No. (63) was issued, which includes the protection of personal data. The first article of the law, states: "Every individual has the right to the protection of personal data related to their private life, as it is one of the rights guaranteed by the Constitution" (Basic Law No. 63)

Moroccan Law: In 2009, the Moroccan legislator issued a special law to protect natural persons in the field of automated processing (Al Shamsi, 2022, p. 14).

UAE Law: In 2012, the UAE legislator issued Decree No. 5, which addresses combating cybercrimes and the protection of personal data (Al Dhahabi, 2017, p 154).

Algerian Legislation: In 2018, the Algerian legislator enacted a law focused on the protection of natural persons in the field of automated data processing. It is a comprehensive law dedicated to protecting individuals' privacy and personal data in the digital world (Law No. 7/18).

Egyptian Law: In 2020, the Egyptian legislator enacted Law No. (151), which is specifically concerned with the protection of personal data (A Critical Study of Personal Data Protection, 2020, p 13).

Saudi Law: In Saudi Arabia, the Personal Data Protection Law was adopted in 2021 (Royal Decree issued on: 9/16/2021).

Jordanian Law: In 2022, the Jordanian legislator enacted a specific law for the protection of individuals' personal data (Al Shamsi, 2022, p. 14).

Section Three: Privacy protection in Omani legislation.

The Sultanate of Oman has issued legislation related to the protection of personal data, which is considered to be specialized and applies within a limited scope. The protection of personal data was

addressed in the Electronic Transactions Law issued in 2008 under Royal Decree No. 69/2008. In its seventh chapter, it specifies that the protection of personal data is covered in Articles 43 to 49 of the law, which address personal data and the legal provisions related to it.

In 2011, the Anti-Information Technology Crimes Law was issued by Royal Decree No. 12/2011, which stipulates strict penalties for those who violate the privacy of individuals through unlawful interference using information technology means.

Elements of the crime of violating the sanctity of private life: The crime of violating the sanctity of private life requires the presence of several basic elements to constitute the crime. The elements include the legal element, the material element, and the moral element. They are detailed as follows:

The legal element: It is the legal text that criminalizes the act and defines the penalty. Crimes related to the violation of private life are regulated under the Law on Combating Information Technology Crimes, issued by Royal Decree No. 12/2011. The law stipulates strict penalties for those who infringe on individuals' privacy using information technology tools.

The material element: It consists of three main components:

- The criminal act: This includes any action that leads to a violation of private life, such as taking photos or recordings (audio or visual) without permission, or publishing news and personal information without the consent of the concerned individual.
- The means used: In these crimes, the means are often information technology tools, such as smartphones, the internet, or social media platforms.
- Resulting Consequence: The action should lead to a violation of the privacy of the affected individual, such as publishing photos or personal information without permission, thereby causing harm to the person concerned.

The moral element: It requires the presence of criminal intent on the part of the perpetrator. The perpetrator must have the intention to commit the criminal act, knowing that it infringes on the private life of the affected person (What are the crimes of violating, 2024).

In 2022, Royal Decree No. 6/2022 was issued issuing the Personal Data Protection Law, which included thirty-two articles that address aspects of data privacy in terms of its definition, preservation, responsibility for its preservation, and detailed penalties for those who violate it.

The definition of personal data in Article No. (1) of the law states: Data that makes a natural person identified or identifiable, either directly or indirectly. This is done by referring to one or more identifiers, such as a name, civil number, electronic identification data, or location data, or by referring to one or more factors related to genetic, physical, mental, psychological, social, cultural, or economic identity.

It has been previously mentioned that legislation defines personal data as any information related to an identifiable natural person. However, some legislations tend to narrow the scope of this definition. Including the Tunisian legislation, which excluded information protected under the Personal Data Protection Law related to public life.

In most Arab laws and legislations, the definition of a natural person includes both the living and the deceased. British law, on the other hand, provides protection only for the living, not the deceased. In this regard, Arab legislation might be seen as more accommodating and in harmony with the principle of honoring human beings both in life and after death (Sheikh, 2018, p 8).

It is noted that the definition in Omani law is more detailed by mentioning the things that make a person identifiable either directly or indirectly. This detail will determine the aspects that define a natural person with great precision, and will prevent anyone who might defraud the legal texts.

Article (10) of the law stipulates the aforementioned principles related to the processing of personal data, as stated in its text: "Personal data may only be processed within the framework of transparency and integrity, respecting human dignity, and with the explicit consent of the data subject."

The request to process personal data must be written and in a clear, explicit and understandable manner, and the controller is obligated to prove the written

consent of the personal data subject to process his data.

The law explicitly outlines the obligations of the data controller and processor in Articles (13-15). These articles state:

Article (13) stipulates that the data controller must establish controls and procedures to be followed when processing personal data. These must, in particular, include the following:

A. Identify the risks that the data subject may face as a result of the processing.

B. Procedures and controls for transferring and converting personal data.

C. Technical and procedural measures to ensure that processing is carried out in accordance with the provisions of this Law.

D. Any other controls or procedures specified by the regulations.

Article 14 – The controller shall, before starting to process any personal data, notify the owner of the personal data in writing of the following:

a. The data of the controller and the processor.

b. Contact information for the data protection officer.

c. The purpose of processing the personal data and the source from which it was collected.

d. A comprehensive and accurate description of the processing and its procedures, and the levels of disclosure of personal data.

e. The rights of the data subject, including the right to access, correct, transfer, and update the data.

f. Any other information that may be necessary to meet the requirements of processing.

Article 15: The controller and processor must adhere to the controls and procedures set by the ministry to ensure that the processing of personal data is carried out in accordance with the provisions of this law.

Article 21: The controller must ensure the confidentiality of personal data and not disclose it except with the prior consent of the data subject, as specified by the regulations.

At the beginning of 2024, the Ministry of Transport, Communications, and Information Technology issued Circular No. 6/2024 regarding the personal data protection policy of the State Administrative Apparatus Unit.

This circular is more detailed, especially with regard to the responsibilities of the data controller and processor, in a way that specifies what each party must do specifically.

It is noted that this circular attempt to restrict the information controller in terms of obtaining all the required licenses before the storage process and requesting the minimum amount of data that would achieve the purpose, such as improving the quality of services.

It also outlined the duties of the third party (processing unit):

1. Protect all personal information and data in its possession, including information and data received from other units, or that has been disclosed to other units.

2. The processing unit or third party shall not carry out any processing except in accordance with the instructions of the controller.

The circular also stipulated: The rights of the personal data owner, which are as follows:

- The right to be informed, including being informed of the purpose of collecting his data.

- The right to access his personal data available to the controller in accordance with relevant regulations and policies.

- The right to request access to his personal data available to the controller in a readable and clear format.

- The right to request the correction, completion or updating of his personal data available to the controller.

It is noted that Omani legislation and the subsequent circular in 2024 covered many aspects related to data protection and processing methods, and were largely in line with rapid technological developments. It also detailed the responsibilities of each party in a manner that leaves no room for dispute over the interpretation of the legal text."

Conclusion

First: Key Findings:

1- The meaning of personal data that laws and regulations have aimed to protect: Any data, regardless of its source or form, that identifies or makes an individual identifiable, either directly or indirectly, including voice and image.
2- The right to electronic privacy is: The protection of personal data stored in information systems from the risks of automated processing. A privacy policy is a document that specifies the extent to which electronic privacy is preserved, how this privacy is exploited, and the ethical and legal issues that arise from this.
3- The major problem with artificial intelligence systems is that there is no central authority to refer to. They are not owned by any specific entity. AI applications are widely distributed and can be used by any individual or organization.
4- The principle of the right to protect privacy is internationally agreed upon, but there is disagreement about the practical application of this right.
5- It is necessary to balance between the individual right and the community's right in the field of electronic data privacy, taking into account that private life is not an individual problem, but rather a social and security problem. Giving sanctity to life is a social need if it contributes to the stability and security of society. Thus, protection privacy is a social necessity if it contributes to the stability and security of society.
6- Omani legislation has kept pace with rapid technological developments and is detailed, addressing many legal gaps in regional and international legislations.

Second: Recommendations:

The research recommends the following:

1. Increase academic research into the legal frameworks imposed by the challenges of artificial intelligence on the protection of personal data.
2. Call on research centers and decision-makers to join forces to develop a unified Arab law on the protection of personal data to address the legal problems arising from the rapid development of artificial intelligence systems.
3. Urge the Omani legislator to continue keeping pace with technical developments and continuous modernization in line with the size of the great challenges.

References

1. A Critical Study of Personal Data Protection Law No. 151 of 2020 AD, Law and Technology Research Center, British University in Egypt, 2020.
2. Al Dhahabi, Khadouja, 2017, The Right to Privacy in the Face of Electronic Assaults, Al-Ustadh Al-Baheth Journal for Legal and Political Studies, 1(8).
3. Al Shamsi, Reem Gharib, 2022, Protecting Digital Privacy in Light of Artificial Intelligence Applications - A Comparative Analytical Study - Master's Thesis, College of Law, United Arab Emirates University.
4. Al-Arabi Jinan, Data processing of a personal nature, drugs, Marrakech, Morocco, 2010.
5. Al-Hafezi Hassan, 2017, Legal protection for data of a personal nature between national legislation and international agreements, Master Thesis, Moulay Ismail University, Morocco.
6. Al-Jabour Radwan Saleh, 2024, Algorithmic Biases and Favoritism in Artificial Intelligence, an article on LinkedIn. Accessed on: 7/27/2024.
7. Al-Jaradat, Dhurgham Issa, Jurisprudential Rulings Related to the Use of Smartphones, Dar Al-Basheer, UAE, 1st ed., 2022, (2/794).
8. Al-Jubouri Salah Hussein, 2015, Rights of Personality and the Methods of Protecting them "A Comparative Study," Dar Al-Fikr University, Alexandria.
9. Al-Muqabali Salah, 2024, What is privacy? And what is the penalty for violating it using technology? an article published in Atheer electronic newspaper,

(https://www.atheer.om/archives/25358), accessed on: 7/30/2024.
10. Al-Ostath Susan, 2013, Violation of the sanctity of private life online, Damascus University Journal of Economic and Legal Sciences, 29(3).
11. Al-Salmi, Alaa Abdel-Razzaq, 2008, Information Technology, Qatar Development Institute.
12. Al-Sheiti Enas, 2014, Evaluating the security and privacy policies of information in educational institutions in the Kingdom of Saudi Arabia: an applied study on Al-Qassim University.
13. Arab Yunus, 2001, Privacy and Information Security in Wireless Business by Cellular Phone, Search, Toot Shamy Teaching School, published on the school website: (tootshamy.com).
14. Article (4), Moroccan Personal Data Protection Law, No. (08/08),
15. Article 25 of the International Covenant on Civil and Political Rights.
16. Article 26, 27 of the International Covenant on Civil and Political Rights
17. Ayoub Paulin Antonius, 2009, Legal Protection for Private Life in the Field of Information, A Comparative Study, Al-Halabi Human Publications, Lebanon, 1st edition.
18. Balas, Yasmine, and Qadir, Nabil, 2021, Right to Digital Privacy, Independent Journal for legal and political studies, 5(1).
19. Basic Law No. (63) dated 4/27/2004 AD. Relating to the Protection of Personal Data from (Chapter 1-105).
20. Ben Salem, Wadad, and Al-Shaibani, Abdullah, 2023, The Right to Information Privacy in Light of Artificial Intelligence, Journal of Legal and Economic Studies, 6 (2) 2023.
21. Declaration of Human Rights, the official United Nations website, (https://www.un.org/ar/about-us/universal-deraration -f-human-rights). Entry on: 5/7/2024.
22. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.
23. European Union Charter for Basic Rights, Article 7, 8.
24. Innovation in data privacy: Innovation in the privacy of data and opportunities available to your company, an article on the site (https://fasstercapital.com). Entry on: 7/15/2024
25. Jabour, Mona Al-Ashqar, and Jabour, Mahmoud, 2018, Personal Data and Arab Laws, Arab Center for Legal and Judicial Research, Lebanon, 1st edition.
26. Lami Bariq, 2017, Crime of violating privacy through electronic means in Jordanian legislation is a comparative study, Master Thesis, Middle East University.
27. Law No. 679/2019 to enter into force in 2018.
28. Law No. 7/18 published in the Official Gazette of the Algerian Republic on 6/10/2018.
29. Lilian Mitrou, 2019, Data Protection, Artificial Intelligence, and Cognitive Services: Is the General Data Protection Regulation? (GDRP) Artificial Intelligence-Proof? SSRN Electronic Journal.
30. Maha Al-Khathami, 2017, Privacy Policy at Saudi Public Universities' Sites on the Internet an Analytical Study, Journal of Research and Educational Studies, University of Jordan, 44 (4), Appendix 6, p. 370).
31. Mona Al-Ashqar Jabour, Mahmoud Jabour, 2018, Personal data and Arab laws, Arab Center for Legal and Judicial Research, Lebanon, 1st edition, 2018.
32. Organization for Economic Co-Operation and Development (OEOD), "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (2013) [C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79]
33. Othman Tariq, 2006, Criminal Protection for Private Life, Master Memorandum, Muhammad Khidr University - Biskra, Algeria.
34. Right to Privacy in the Digital Age for session No. 27, Resolution: 68/167 issued on 6/30/2014.

35. Right to Privacy in the Digital Age for session No. 29, Resolution No. 7/34, issued on 8/3/2018.
36. Royal Decree issued on 9/16/2021. In implementation of Resolution No. 98 dated 9/4/2021.
37. Samir Ziada, 2020, How do I know that my mobile phone is hacked, and how do I protect my phone from penetration? an article on Egyptian Stars website: (https://www.ngmisr.com/tech). Entry on: 3/5/2020.
38. Sheikh Hussein Muhammad Yahya, Sayed Mohamed Ahmed, 2018, Legal Protection of Personal Data, A Comparative Study in British Law and UAE Law, Journal of Judicial and Law, Center for Research and Judicial Studies, No.4.
39. Sorour Tariq, 1991, Criminal Protection of the Secrets of the Paradise in the face of publication, Arab Renaissance House, Egypt.
40. Swailem Khaled, Legal Protection of Electronic Personal Data, Comparative Study, Legal Journal, p. 1889.
41. Taha, Amina Hussein, 2023, International Protection for Human Rights in the Digital Age, Journal of Law and Technology, College of Law, British University in Egypt, 3 (2).
42. Technological prejudice: a critical vision of the role of "algorithms" in culture and politics/ an article published on the Future Center for Research and Advanced Studies in Tarh: February 27, 2024. (https://futureuae.com/ar-ae/mainpage/item/9052). Entry on: 7/17/2024.
43. Tlemcen Younis, Criminal Protection of Personal Data, Marrakech, 2008, p. 19.
44. Toby, Mendel, et al., 2016, A Global Survey on Internet Privacy and Freedom of Expression, UNESCO Publications.
45. UK Data Protection Act 1998 section 1 (1).
46. What are the crimes of violating the sanctity of private life in Omani law? An article on the website of the Protected Sultanate of Oman (https://lawfirmoman.com), the website was accessed on 12/8/2024.
47. WhatsApp is not alone. Violation of privacy to where? Article on the news portal. https://www.albawabhnews.com/4285208)). Entry on: 7/7/2024.