Vol (04) | Issue (01) Year (2024) (589-605) Pages

Journal of Science and Knowledge Horizons

ISSN 2800-1273-EISSN 2830-8379

Artificial Intelligence and the Challenge of Protecting Personal Data in Light of European Directive EC/9/96 on the Legal Protection of Databases

Dr. Ouafi Hadja* **Lecturer -A-, Faculty of Law and Political Science, University of Mostaganem (Algeria)**

https://orcid.org/0009-0001-6348-7501

hadja.ouafi@univ-mosta.dz

Date of send: 25/ 04 / 2024	date of acceptance: 23 / 05 /2024	Date of Publication: 30/06/2024

Abstract:

The reliance on the current international, regional, and national legislative frameworks, including their criminal aspects and their applications aimed at protecting personal data, despite considerable efforts The existing international, regional, and national legislative frameworks, including their criminal provisions, are currently inadequate for protecting personal data despite significant efforts at various doctrinal and judicial levels. The presumption that existing protections are sufficient without acknowledging the rapid advancements in science and technology calls for new regulations that are in tune with sophisticated artificial intelligence systems, thereby ensuring robust and effective legal safeguards against emerging crime forms that jeopardize personal and private data.

Therefore, it is crucial not to merely extend existing legal frameworks, which were primarily designed for an earlier era, to address new challenges posed by technological advancements that have significantly widened the scope and flow of data. We must adopt a fresh approach that is tailored to meet the challenges posed by artificial intelligence systems and the diminishing influence of state sovereignty in this area.

The intrusion and manipulation of an individual's right to confidentiality and exclusive control over their information are more extensive than anticipated. Hence, it is imperative to thoroughly investigate how artificial intelligence and its applications infringe upon these rights. The assumption that current legislation,

particularly in terms of criminal protection, provides adequate safeguards is increasingly questionable for several reasons:

- International legislation, including the Universal Declaration of Human Rights, tends to treat the protection of personal data as a cursory reference, characterized by general rules and provisions that lack binding legal force or mandatory obligations, and thus fail to offer the requisite protection.
- A review of the current legislative system underscores a trend towards harmonizing laws to enhance effectiveness and applicability. This is particularly evident in regional initiatives within Europe, such as the European Directive, which is explicitly designed to adapt to technological progress and provide suitable protection for personal data in a collective and unified manner.

Keywords: Personal Data; European Data Protection Directive; Artificial Intelligence; Digital Sovereignty.

*** Dr. Ouafi Hadja**

Introduction:

The European Directive, rooted in the foundational principles, provisions, and rules established by international legislation—from the Universal Declaration of Human Rights to the International Covenant on Civil and Political Rights—mandates stringent obligations on states along with a series of guarantees. What sets this Directive apart, despite its regional scope, is its role in unifying legislation across all European countries. This unification has led to significant advancements in various domains, most notably in the vital area of protecting individuals' personal data and information.

This legal framework serves as an effective model for overcoming barriers to adequate data protection. It includes legal rules and provisions that govern the movement of data and individuals' rights to control and monitor their information, ensuring that data usage is confined to legitimate and legal contexts.

However, this framework encounters numerous challenges, particularly from the rapidly evolving artificial intelligence systems and applications. These challenges are compounded by the unique characteristics of AI, which is primarily fueled by data and information, and the shifting dynamics of power.

The increasing involvement of entities that share and divide control and ownership of data with states -major centers for data collection- raises significant concerns. Thus, a critical question emerges:

How effective is the European Directive in safeguarding personal data against the challenges posed by artificial intelligence systems?

Before delving into the details of the European Directive concerning data and personal information protection, its principles, and the challenges it confronts, it is essential first to define artificial intelligence. This definition will cover its characteristics, applications, and the impact these have on the protection of individuals' personal data and information.[1]

1. The Concept of Artificial Intelligence

Artificial Intelligence (AI) has sparked significant debate, particularly as it has surged to the forefront of the technological revolution, profoundly impacting the digital landscape. While AI is a familiar term within specialized digital communities, its concepts and intricacies often remain elusive to the general public. AI is a subject steeped in technical complexity and depth. To avoid straying from the scientific discourse into a more generalist realm due to a lack of deep technical understanding, this section aims to clarify and define artificial intelligence in an accessible manner.

1.1 Definition of Artificial Intelligence

The term "Artificial Intelligence"[2] has gained popularity not merely because it is a new concept, but because of its association with contemporary applications like the interactive chat program Chat-GPT4. AI continuously evolves, reflecting the advancement of modern methodologies and innovations. It strives to enable computers to undertake tasks traditionally performed by the human mind.

The concept of artificial intelligence was first articulated in 1956 by John McCarthy, an American computer scientist recognized as one of the founders of AI, with numerous significant contributions to the field. He defined AI as "the science of making a machine behave in ways that would be considered intelligent if a human were behaving in the same way."

Marvin Minsky, another pioneering figure, described AI as "the science that enables machines to perform tasks that require intelligence when undertaken by humans."

Peter Norvig and Stuart Russell, in their seminal book "Artificial Intelligence: A Modern Approach," define AI as "a branch of computer science concerned with the study and design of intelligent agents," where an agent is a system that perceives its environment and takes actions that maximize its chances of success at some goal.[3]

Allen Newell offered another perspective, defining AI as "the degree or level of knowledge at which an AI system can approximate human cognitive processes.[4]"

Lastly, Ray Kurzweil, a notable inventor and director at Google, characterized AI in a Time Magazine article as "a technology that intelligently learns using skills akin to human intelligence, including the capabilities to perceive, learn, think, and act independently."

Despite the variety of viewpoints and the complexities inherent in defining AI, there is a consensus that its core aim is to "simulate human intelligence through machine operation." In essence, AI manifests as intelligence exhibited by virtual machines, smart robots, and sophisticated software systems capable of mimicking human-like behavior to achieve specific objectives.

This branch of computer science focuses on developing systems that can analyze, store information, and assist in problem-solving, thereby saving human effort and time. AI systems feed on data, derive insights, comprehend multiple languages, and perform many tasks previously thought to be exclusive to human capabilities.[5]

1.2 Characteristics of Artificial Intelligence:

In this section, we delve into the distinctive characteristics that define artificial intelligence, highlighting its capabilities from data comprehension and self-learning to its profound ability to mimic human behavior, which marks its most transformative aspect. These are not mere programs; they are advanced

frameworks designed to undertake functions beyond the reach of traditional software.

A. Data Comprehension:

The rise in popularity of artificial intelligence applications has led to an exponential increase in data movement. Unlike traditional systems where data entry was predominantly manual, AI-enhanced systems excel not only in data storage but also in data analysis through self-learning algorithms. This involves the concept known as 'learning from past experiences,' where AI systems utilize neural networks to extract and analyze patterns.

This capability enables AI to draw logical conclusions from vast data sets and optimally manage data storage, thus safeguarding the information from potential loss or damage.[6] Storing data on computers equipped with AI programs offers a robust solution, though it also presents potential risks, particularly when data is misused or improperly accessed within the digital space.

B. Ability to Learn:

Beyond basic automation, general artificial intelligence approaches the complexity of human cognition, encapsulating what is known as machine learning. The defining feature of AI programs is their capacity for self-learning, which allows them to refine their operations by learning from past errors. This ongoing improvement is facilitated by feeding the system a continuous stream of data, from which it extracts insights and adapts.

These adjustments enhance the system's proficiency in handling diverse and complex scenarios. It is crucial for AI training to utilize non-personal and non-sensitive data while ensuring adherence to stringent privacy protection standards. However, challenges remain, particularly in the transparency of the learning process, which often remains opaque to non-specialists. Concerns also persist about the integrity and precision of the data used in training phases, as well as accountability for mistakes or breaches of privacy. Despite these issues, the financial benefits generated by machine learning are considerable.

Though current AI systems have yet to achieve the sophisticated level of learning akin to human cognition- lacking in consciousness, perception, and deductive reasoning- their potential to assist humans in complex, time-sensitive, or memory-intensive tasks is undeniable. The trajectory of AI development suggests a future where artificial intelligence could become an invaluable ally in enhancing human capabilities, especially in areas that are traditionally challenging for human beings.[7]

1.3 Applications of Artificial Intelligence:

The scope of artificial intelligence applications has expanded dramatically, permeating nearly all sectors, especially with the maturation of their practical implementations. These applications have reached levels previously unimagined, impacting a wide array of fields including industry, renewable energy, military, space exploration, language comprehension, and medicine. Among these broad applications, those that most significantly affect individual privacy and data protection are predominantly observed in social networking sites.[8]

A. Chatbots:

Chatbots stand out as a transformative aspect of artificial intelligence in digital communication platforms. They are prime examples of AI's capability to excel in intelligent language processing and user interaction. These systems demonstrate advanced self-learning abilities and can engage with users in ways that closely resemble human interaction.

Predominantly based on neural networks and deep learning algorithms, chatbots excel in understanding natural language, allowing them to provide precise and instantaneous responses across various domains. Moreover, they enhance customer service by leveraging extensive data to pinpoint user needs and devise effective solutions.

However, the deployment of chatbots raises significant concerns about potential job displacement, privacy and security risks, biases, and discrimination. These issues are pressing and have been highlighted by experts, underscoring the need for cautious and considerate implementation of such technologies.[9]

B. Facial Recognition:

As another significant application of AI, facial recognition technology employs advanced methods like deep learning and image analysis to identify and differentiate individuals based on facial images. This technology has become widespread in various security applications, from unlocking personal devices like phones and computers to securing digital financial transactions.

Beyond individual uses, facial recognition is capable of monitoring urban environments by tracking individuals through public and private spaces. It is also utilized in access control systems, marketing strategies, and other applications. However, the proliferation of facial recognition technology poses substantial privacy concerns. Its potential misuse can lead to severe violations of individual

privacy, making it imperative to exercise extreme caution. The integration of such technology in social networking within the digital landscape necessitates heightened vigilance to prevent abuses and protect personal data.

2. Legal Protection of Digital Databases Regionally

The circulation of digital data through the internet, social networks, and various other sectors has become widely accepted, logical, and necessary, reflecting its crucial role in responding to technological advancements and the digital transformation driven by the revolution in artificial intelligence and computing. This digital reality, however, has introduced new forms of data infringement, particularly concerning personal data. This situation has spurred an ongoing search for effective legal protections.

Observations from practical applications indicate that the European approach is particularly noteworthy. European legislation has demonstrated resilience and effectiveness, being suitably adapted to keep pace with technological advancements in the digital and AI domains. This model of legal framework serves as a benchmark for developing robust protections tailored to the evolving landscape of digital information and artificial intelligence systems.

2.1 Legal Protection of Databases According to the European Directive

Amid various international efforts, the regional approach at the European level has emerged as a leader, demonstrating effectiveness through its rapid adaptation to the evolving needs of the digital age and the fourth technological revolution. The European Union's efforts to harmonize legislation have significantly advanced the protection of personal data for European citizens.

Both the European Parliament and the Council of the European Union have played pivotal roles in developing a unified legal framework, culminating in the adoption of the European Parliament and Council Directive EC/9/96 on March 1, 1996, which specifically addresses the legal protection of databases.

First: The Concept of Personal Data:

The term "personal data" is preferred within this context over the "personal information" terminology used by French law, as issued on January 6, 1979, though the distinction largely rests on terminological differences.

The French legislation later aligned with the European Directive's terminology through the law issued on August 6, 2004, which adopted the definition of personal data as presented in the European Directive. According to the first paragraph of Article 2 of the Directive, personal data is defined as: "Any

information or data that could be used to identify a specific natural person, or make them identifiable."

The Directive elaborates in the same paragraph that "the person can be identified directly or indirectly, particularly by reference to an identification number or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity."

It is important to recognize, as stated in Article 1 of the Directive EC/95/46 [10]and EC/2002/58, that the primary aim of these provisions is to protect the fundamental rights and freedoms of natural persons during the processing of personal data, with a particular focus on the rights related to their private lives. Consequently, the protection afforded by these rules extends beyond information that directly identifies an individual, such as their name or domicile.

It also encompasses data that can indirectly identify an individual through modern technologies, including but not limited to mobile numbers, email addresses, credit card numbers, or personal identifiers such as voice, fingerprints, DNA, or even biometric data. This comprehensive approach reflects the Directive's recognition of the complex ways in which personal data interacts with individuals' rights in the digital era.[11]

Second: Principles and Fundamentals of Data Protection:

The core of any data protection legislation is anchored in the principle that personal data must be collected through means that are "legitimate and normally under the circumstances of the situation," as highlighted by the Hong Kong Personal Data (Privacy) Ordinance. Additionally, such data can only be used or disclosed for the purposes for which it was initially collected, or for purposes that are directly related, unless explicit consent is provided by the data subject.

This framework is reinforced by the "six data protection principles," which are fundamental to the legislative mechanisms governing data protection:

- **First Principle:** The collection of data is restricted to lawful purposes directly related to the activities or functions of the data user, who must collect personal data through legitimate and fair means. This principle mandates that data users clearly inform data subjects about the specific purposes for which their data will be used.
- **Second Principle:** Data users must ensure that all data retained is accurate and kept up-to-date. If the accuracy of the data is in doubt, its use must be immediately suspended. Additionally, data should not be retained for longer than is necessary for the purposes for which it was collected.
- **Third Principle:** This principle stipulates that without the consent of the data subject, personal data should not be used for any purpose other than that for which it was originally collected.

- **Fourth Principle:** Data users are required to implement appropriate security measures to protect personal data. This includes safeguarding against unauthorized access, processing, erasure, use, or other unauthorized activities.
- **Fifth Principle:** This principle pertains to the transparency required of data users regarding the personal data they hold. It involves the issuance of a "privacy statement" that details the accuracy of the data, its retention period, security measures, usage policies, and the procedures related to data access and correction requests by data subjects.[12]
- **Sixth and Final Principle:** This principle concerns the rights of data subjects to access their personal data. It allows them to request copies of any personal data held by the data collector and, if discrepancies are found, to demand corrections.

Both data subjects and users are guided by these principles, which are continually disseminated through foundational documents issued by the commissioner after extensive consultations with relevant stakeholders. Furthermore, while the laws stipulate that a failure by data users to comply with any part of the regulations does not subject them to civil or criminal lawsuits, asserting such non-compliance in trials is deemed acceptable as evidence.[13]

2.2 Harmonization of Domestic Legislation within the European Union:

European nations are actively pursuing a cooperative approach across various legislations, laws, regulations, and directives. A significant challenge in these efforts lies in addressing issues related to applicable laws and striving to eliminate any barriers that could hinder the success of the European Directive as an effective legal framework for the protection of personal data and information. This endeavor reflects a commitment to creating a harmonized legal environment that upholds the integrity and confidentiality of personal data across the European Union.

First: Applicable Law

A. Traditional Principles:

When considering the traditional principles of determining applicable law, it is essential to address the complexities introduced by cybercrime, which often transcends the territorial boundaries of a single state and affects multiple jurisdictions, thus leading to severe conflicts of law. Such conflicts typically arise in scenarios where a cyber incident involves multiple states.

For instance, if a breach occurs within a database located in state (A) and the effects of that breach are realized in state (B), while the database user resides in another state (C), determining the applicable law becomes challenging.

The traditional principles for determining the applicable law hinge on three foundational tenets:

- **Principle of Territoriality:** This principle asserts that the law of the state where the crime occurs should govern. It underpins the sovereignty of each state over its territory.
- **Principle of Realism:** This principle allows a state to protect its interests by applying its laws to acts that affect it, even if those acts occur outside its territorial boundaries.
- **Principle of Personality:** This principle operates in two dimensions. The positive aspect applies the state's law to all individuals holding its nationality, regardless of where the crime was committed. The negative aspect allows a state to apply its laws to any crime committed against its nationals, even if the perpetrator is foreign and the crime occurs outside its territorial boundaries.[14]

Despite these principles, the Principle of Territoriality faces limitations, especially in dealing with international cybercrimes that do not strictly occur within a single state's territory, thus rendering it insufficient for addressing global cyber threats. The Principles of Realism and Personality also encounter shortcomings in their scope and applicability across jurisdictions.

To address the challenges posed by the applicability of laws to computer operations and data movement across borders, modern jurisprudence has seen a division into three distinct approaches: One approach advocates for the application of the law of the state where the data was sent from. Another proposes applying the law of the state where the data is received. A third suggests applying the law of the state that seeks protection or is most significantly impacted, each supported by its respective justifications.

B. Issuance of the European Directive:

The European Directive on databases was specifically issued to harmonize national legislation across EU member states and to address the inconsistencies and disparities in database protection laws. The preamble of the directive highlights the existence of these disparities and underscores the imperative to overcome them. The directive's intent is clear in its efforts to eliminate legislative differences that negatively impact the protection of databases.

By aligning the legislative and judicial frameworks within the European Union, the directive has successfully mitigated many of these disparities. This harmonization is reflected in the texts adopted by most European countries,

influencing even non-European nations, which have drawn inspiration from the European model. The outcome has been a more unified and coherent approach at both legislative and judicial levels in handling cases related to database protection, demonstrating the directive's effectiveness and its pivotal role in shaping data protection standards internationally.

Second: Challenges Facing the European Directive:

The European Directive faces significant challenges in its endeavor to legislate compliance across all involved parties and stakeholders, particularly concerning the governance of digital content movement and control over data collection centers. One of the central issues revolves around who holds the monopoly over the infrastructure, which is typically dominated by large corporations. The challenges can be broken down into several key dimensions of digital authority:

1. **Digital Authority:**

We return to remind ourselves of the key challenges in the digital world, specifically in the realms of digital authority, as detailed above. The concept of digital value chains may facilitate our understanding of the network of authority relationships—who exercises it, who is subject to it, and how we can resist it. Digital authority is grounded in four major essential value chains:

A. Geopolitical Dimension:

This aspect concerns authority over the physical infrastructure of the digital world, including satellites, terrestrial networks, undersea cables, and associated equipment. The main conflict in this realm is between economically dominant powers such as the United States and China. In contrast, less powerful states or continents like Africa and Latin America find themselves sidelined. Only states that are part of regional or continental alliances have the capability to engage effectively at this level.

B. National Dimension:

This dimension covers authority over the digital industry, encompassing everything required in the digital age—from economic to social, political, cultural, and environmental aspects. Control here is mostly in the hands of industrialized nations and some emerging countries. National states must engage actively if they are to protect their social and sovereign security.

C. Soft Power Dimension:

This dimension is related to the digital knowledge produced by scientific research and the soft infrastructure that facilitates digital life, such as search engines, networks, and content management systems. Unlike the national dimension, control in this area is predominantly held not by national states but by individuals and massive private corporations.[15]

D. Public Soft Dimension:

This includes social networks and specialized sites, whether they are scientific, literary, or artistic in nature.

These four chains of digital value production illustrate a complex network of power relationships, highlighting who exercises this power, who is subjected to it, and how it can be resisted. The current distribution of digital authority is uneven and often does not benefit all parties equitably. It is clear that without vigorous resistance and active engagement from various political, scientific-technological, intellectual, and civil rights groups, these chains will not serve universally recognized human interests.

The task of building digital societies and states, and ensuring their advancement and security, represents some of the most profound challenges facing fields such as political science, sociology, and economics today. Consequently, the traditional concepts of sovereignty and security are now prominent in public discourse.

In the digital age, the conventional understanding of sovereignty, typically based on national borders, is becoming obsolete. Digitalization, propelled by neoliberal globalization, has effectively dismantled these traditional boundaries. As such, considering the challenges of sovereignty and security within national borders is increasingly impractical for national states due to the prohibitive costs involved. This reality makes regional or continental blocs a more viable framework for achieving and maintaining digital sovereignty and security.[16]

2. Controlling Data Collection Centers:

The expansion of companies into the European market has led to the construction of substantial databases containing vast amounts of human knowledge, which are primarily viewed as economic assets. These databases not only fuel the artificial intelligence programs that generate significant profits[17] but also necessitate the development of a legal framework that ensures effective regulation in line with the stringent European legislation on data protection. This framework is designed to define responsibilities, mitigate risks, and curb the expansive digital authority these companies hold. Several key challenges need addressing:

A. **Data Security:**

Companies often project a commitment to comply with European data protection legislation to safeguard their users' data. They endeavor to elevate security measures when handling this sensitive material within the digital environment. However, even amid stringent legislations regulating data movement and establishing comprehensive digital security strategies, certain aspects may be overlooked by tech giants. For instance, companies like Facebook manage social connections for over a billion people, creating a vast infrastructure for collecting digital data in data centers. This scenario raises multiple concerns regarding the confidentiality levels maintained during the use and management of these data.

B. **Information Confidentiality:**

Laws are crafted to protect the confidentiality of sensitive personal information, shielding it from access by unauthorized parties who may not respect privacy norms or who might tamper with or transfer data to unmonitored third parties. Essential measures include ensuring that users can access their information—every user should have the right to know what data is collected about them, to whom it is disclosed, how it is utilized, and how they can access or request the deletion of their data.

C. **Information Integrity:**

Data integrity is often compromised by companies that modify data without owner consent or violate stipulated durations for data retention and use, including the freedom to copy and transfer data. Many companies also neglect proper encryption standards during these processes, which jeopardizes data integrity. It is crucial that all standards and safety methods inspired by the European Directive for data protection are adhered to.

These include data segmentation and regular verification against original data. Another critical measure is ensuring that users have easy access to their information, the right to correct inaccuracies, and the right to delete their data—often referred to as the "right to be forgotten." Furthermore, involving users in securing their data through training in encryption processes can significantly enhance security levels.

D. **Usage Policies:**

The monitoring, formulation, and implementation of usage policies pose significant challenges in the enforcement of data protection legislation. With companies having the ability to investigate and access all information provided by their users across various services, the digital environment demands a rigorous

quality of specific policies to safeguard privacy and align them with legislative and regulatory requirements. Key aspects include:

- Ensuring user consent is obtained before merging personal identification information with cookies that are shared with advertising networks.
- Striving to standardize privacy policies across all services offered by these companies.
- Prioritizing data security, confidentiality, and transparency in the presentation of these policies.

From the discussion above, it is evident that the success of these efforts and challenges hinges largely on the extent to which these corporate actors comply and cooperate with regulatory authorities and their commitment to optimally implement these laws.

Conclusion:

In the grand scheme of digital evolution, crafting effective international or regional legislation stands as a crucial endeavor. This legal framework, encompassing both penal consequences and procedural intricacies, must remain agile to keep pace with digital advancements. Its primary aim? To tackle head-on the ever-evolving challenges of safeguarding privacy while navigating the complexities posed by the rise of artificial intelligence (AI) systems and applications.

At the forefront of this legal landscape is the European Directive, meticulously designed to shield personal data and information. While laudable in its adaptability to digital progress and privacy exigencies, the Directive grapples with a formidable obstacle: the rapid ascent of AI systems.

These intricate systems, fueled by complex algorithms and voracious data consumption, herald significant data security threats, especially concerning the sanctity of personal data. This stark reality accentuates the urgent need for the Directive to fortify its provisions comprehensively, ensuring robust protection mechanisms for all forms of sensitive data.

Moreover, a pressing challenge looms large: the imperative of forging consensus with entities wielding control over digital domains. These entities hold sway over digital content, critical infrastructure, and pivotal data management hubs, often dominated by corporate behemoths. Navigating this terrain necessitates proactive engagement with international bodies, pertinent organizations, and a diverse array of civil society stakeholders.

In light of these formidable challenges, we put forth the following recommendations:

- Establishment of a precise and nuanced legal framework tailored explicitly for artificial intelligence. This framework must address the intricate web of legal responsibilities associated with AI systems.
- Persistent efforts to harmonize international and regional laws, providing a robust blueprint for national legislation. Such legislation should not only ensure the protection of data and personal information but also bolster criminal policy measures aimed at curbing digital malfeasance.
- Collaborative engagement with key stakeholders steering digital technologies. This collaborative approach seeks to strike a delicate equilibrium, balancing the imperative of safeguarding individuals' data and privacy rights with the legitimate interests of corporations, employees, and users alike.

References:

A. Books:

1. Alan Bunnie, "Artificial Intelligence: Its Reality and Future," Dar Al-Farouk Publishing, no edition, 2015.
2. Mohamadi Ahmed Nassim, "Revolution of the New Intelligence," Adlis Belzma for Publishing and Translation, Batna, Algeria, 2021.
3. Margaret A. Boden, translated by Ibrahim Sand Ahmed, "Artificial Intelligence," Hindawi Publishing, Egypt, 2022.
4. Khaled Nasser Essayed, "Foundations of Artificial Intelligence," College of Sciences, University of the Section, Riyadh Library, Saudi Arabia, 2004.
5. Raymond Wax, "Privacy," Hindawi Foundation for Education and Culture, first edition, Egypt, 2013.

B. Legal Texts:

1. European Parliament and Council Directive No. EC/9/96 dated March 1, 1996, on the legal protection of databases, adopted on March 11, 1996, effective from January 1, 1998, and amended by Directive No. 2019/790

issued by the European Parliament and the Council on April 17, 2019, on copyright and related rights in the digital single market.

C. International Reports:

1. United Nations High Commissioner for Human Rights, "Core International Human Rights Treaties," New York Geneva, 2006.

D. Scientific Articles:

1. Mohamed Ahmed Al-Madawi, "Protection of Informational Privacy for Users on Social Networking Sites," Faculty of Law Journal, Benha University, Egypt, Issue 33, Part 4, 2018.
2. Naji Hakima, "Cyberspace and the Crisis of Democracy: From Digital Extras to Political Action," Mo'menoon Without Borders, Studies and Research Section, 2022.
3. Claudine Guerrier, "Protection of Personal Data and Biometric Applications in Europe," Communication Commerce Electroniques, July 1, 2003, n7.
4. Michael Nielsen, "Who Owns Big Data?" Technology Review, 2015, available at: https://www.technologyreview.com/2015/01/05/169719/who-owns-big-data/

Footnotes:

[1] Alain Bunnie, "Artificial Intelligence, Its Reality, and Its Future," Dar Al-Farouk Publishing, 2015, p. 7.

[2] Alain Bunnie, Ibid, p. 8.

[3] Mohamadi Ahmed Nassim, "Revolution of the New Intelligence," Adlis Belzma for Publishing and Translation, Batna, Algeria, 2021, p. 24.

[4] Margaret A. Boden, "Artificial Intelligence," translated by Ibrahim Sand Ahmed, Hindawi Publishing, Egypt, 2022, p. 11.

[5] Khaled Nasser Essayed, "Foundations of Artificial Intelligence," College of Sciences, University of the Section, Riyadh Library, Saudi Arabia, 2004, p. 21.

[6] Khaled Nasser Al-Sayed, Ibid, p. 21.

[7] Margaret A., op. cit., p. 46.

[8] Mohamadi Ahmed Nassim, op. cit., p. 78.

[9] Mohamadi Ahmed Nassim, Ibid, p. 112.

[10] European Parliament and Council Directive No. EC/9/96 dated March 1, 1996, on the legal protection of databases, adopted on March 11, 1996, effective from January 1, 1998, amended by Directive No. 2019/790 issued by the European Parliament and the Council on April 17, 2019, on copyright and related rights in the digital single market.

[11] Claudine Guerrier, "Protection of Personal Data and Biometric Applications in Europe," Communication Commerce Électroniques, July 1, 2003, n7, pp. 17-22.

[12] Raymond Wax, "Privacy," Hindawi Foundation for Education and Culture, first edition, Egypt, 2013, p. 121.

[13] Raymond Wax, Ibid, p. 122.

[14] Mohamed Ahmed Al-Madawi, "Protection of Informational Privacy for Users on Social Networking Sites," Faculty of Law Journal, Benha University, Egypt, Issue 33, Part 4, 2018, p. 39.

[15] Naji Hakima, "Cyberspace and the Crisis of Democracy: From Digital Extras to Political Action," Mo'menoon Without Borders, Studies and Research Section, 2022, p. 13.

[16] Naji Hakima, Ibid, p. 14.

[17] Michael Nielsen, "Who Owns Big Data?" Technology Review, January 5, 2015. Accessed January 12, 2024, 11:48 AM, available at: https://www.technologyreview.com/2015/01/05/169719/who-owns-big-data/.