THE LEGAL PROTECTION OF PERSONAL DATA IN THE DIGITAL ENVIRONMENT

[1]FATIMA MOHAMED ALHEBSHI, [2]MAHER ALJABER

[1]Master of Cybersecurity Law, Fujairah University
[2]Associate Professor of Cybersecurity Law, Faculty of Law. Fujairah University
E-mail: [1]2025210333@fu.ac.ae, [2]m.aljaber@fu.ac.ae .maheraljaber@bau.edu.jo

Abstract - In light of the rapid transformations taking place in the field of information and communication technology, and the accompanying significant expansion in the collection, processing, and circulation of personal data via electronic means, the issue of personal data protection in the digital environment has come to the fore due to the diverse forms of infringement to which personal data is exposed. The problem addressed in this study is to examine the adequacy of the legal framework governing the protection of personal data in the digital environment in light of the rapid development of modern technologies and the resulting expansion in the collection, processing, and circulation of data through advanced electronic means. To achieve the objectives of this study, a descriptive-analytical approach was adopted by addressing concepts related to personal data and its characteristics, and analyzing the legal texts governing it, while utilizing a comparative approach in certain aspects to highlight the positions of various legislations in regulating this field. This study concluded that there is a wide variety of forms of personal data breaches in the digital environment, including unlawful collection, unlawful processing, hacking, data theft, and other forms of infringement. Therefore, this study recommended the need to develop the legal framework for personal data protection in a manner consistent with the nature of the digital environment, and to strengthen the obligations of data controllers, while adopting flexible legal standards to determine liability, thereby striking a balance between the requirements of technological development and ensuring the protection of individuals' privacy**.**

Keywords - Personal Data, Legal Protection, Privacy, Data Processing, Legal Liability.

I. INTRODUCTION

Rapid technological advancement, particularly in the field of information and communication technologies, has given rise to a new digital reality in which the digital environment has become an integral part of the daily lives of individuals and organizations. The widespread adoption of the internet, smart applications, and online platforms has brought about fundamental shifts in the ways we communicate, interact, and exchange information. This has led to increased reliance on digital tools in various social, economic, and administrative activities, making personal data a central element in this growing digital space and an indispensable foundation for the delivery of modern digital services.

Personal data has become one of the essential components of an individual's digital identity, as it reflects various aspects of their private and professional life and encompasses a wide range of information that distinguishes them from others, whether it be simple identifying data or sensitive information related to their health, beliefs, or financial circumstances. The cross-border nature of the digital environment has further complicated the issue of personal data protection, as data is no longer collected or processed within a specific geographic or legal jurisdiction, but rather travels across global networks and is subject to multiple legal systems, raising legal challenges regarding the determination of jurisdiction and the applicable law in cases of personal data breaches.

As electronic transactions have expanded, the need has emerged for clear legal regulation governing the mechanisms for collecting, processing, and using personal data, thereby ensuring the protection of individuals' privacy and limiting forms of infringement on their data. Modern digital practices have revealed various forms of infringement on privacy, whether through the collection of data without the owners' knowledge or explicit consent, its use for purposes beyond the original intent for which it was collected, or the failure to provide adequate technical safeguards to secure it.

1.1. Problem of Study

The research problem is to examine the adequacy of the legal framework governing the protection of personal data in the digital environment in light of the rapid development of modern technologies and the resulting expansion of data collection, processing, and circulation through advanced electronic means, which has led to a diversification of forms of data breaches and made it more complex to regulate them legally. This raises several questions regarding which party is liable for the informational harm resulting from the infringement of personal data, given the multitude of parties involved in data processing.

1.2. The Importance of Study

The importance of studying the legal protection of personal data in the digital environment is growing in light of technological transformation and legal challenges that require a precise legal approach to the mechanisms for processing and storing personal data. The significance of this topic also stems from its direct connection to the protection of individuals' privacy and fundamental rights in the face of

potential violations of their data in the digital environment. The significance of this study lies in highlighting the adequacy of the legal rules governing personal data in light of the complexity of digital relationships and the multiplicity of parties involved, and the resulting issues regarding the determination of legal liability.

1.3. Methodology

To achieve the objectives of this study, a descriptive-analytical approach was adopted, involving a presentation of the concepts related to personal data and its characteristics in the digital environment, an analysis of the legal rules governing its protection, and an examination of the forms of infringement to which it may be subject, along with an explanation of the resulting legal liability. A comparative approach was also adopted by examining the provisions of various pieces of legislation, with the aim of highlighting the differences and similarities among them, leading to conclusions that support the strengthening of legal protection for personal data in the digital environment.

II. THE NATURE OF PERSONAL DATA AND FORMS OF INFRINGEMENT AGAINST IT

The protection of personal data is a relatively recent legal issue, as its emergence is linked to the rapid development of information and communication technology and the widespread use of computers and the internet in various aspects of life. This has led to an increase in the volume of information circulating about individuals and the ability to collect, process, and store it using advanced electronic means, making personal data more vulnerable to circulation and exploitation in ways that may infringe on individuals' privacy. This data includes various pieces of information associated with a person through which their identity can be identified or certain aspects of their private life revealed, such as name, photograph, gender, nationality, age, marital status, and other information that can be circulated through various means, particularly via modern digital media (Rahmani & Zain Alabdeen, 2025).

European Directive No. 46/95 defines personal data in Article 2 as "any information relating to an identified or identifiable natural person, directly or indirectly, by reference to an identification number or to one or more factors specific to his or her physical, psychological, economic, social, or physiological identity." Similarly, European Convention No. 108, adopted on December 13, 1999, by the Council of Europe, adopted a similar concept in Article 2, defining personal data as "any information relating to an identified or identifiable natural person," which indicates the adoption of the criterion of identifiability as the basis for determining the scope of such data.

It is not limited to information that directly identifies a natural person, but also extends to data through which a person can be indirectly identified by linking it to other data. This legislative trend reflects a growing awareness of the risks posed by technological advancements in data processing, as modern technologies are now capable of analyzing large volumes of information and linking them together, which may lead to the disclosure of individuals' identities or certain aspects of their private lives. The researcher argues that adopting a broad and flexible concept of personal data is essential in the contemporary digital environment, as it contributes to providing more effective legal protection for individuals' privacy and limits the risks of misuse of their personal data, especially with the continuous expansion of digital technologies and the exchange of information via electronic networks (Qogom, 2021).

Personal data is characterized by a number of features that distinguish it from other types of data, given its connection to a natural person and the potential impact of its use or processing on individuals' privacy. Most legislation agrees that personal data is linked exclusively to a natural person, meaning it pertains to information about individuals that affects their identity or private life. It also constitutes knowledge of a person's identity, meaning it enables others to identify the natural person to whom this data relates, whether directly through the data itself or indirectly by linking it to other data.

The methods and forms of personal data infringement in the digital environment vary, with the collection of personal data without the explicit consent of the data subject being one of the most prominent forms of privacy infringement in the digital environment, as all data collection or processing must be based on lawful and informed consent. This violation occurs when certain websites collect, process, or share users' data with third parties—such as for advertising purposes—without their knowledge, which constitutes unlawful conduct entailing legal liability (Qogom, 2021). The use of personal data for commercial purposes is also one of the most prominent forms of infringement on individual privacy in the digital environment, where data is collected and circulated through social media platforms and sold to advertising companies that analyze and categorize it to identify user preferences and target advertisements according to their interests. Furthermore, the ease and low cost of data collection have contributed to the emergence of what is known as the data economy or information economy, on which many companies rely to provide free services in exchange for the commercial exploitation of data within the context of digital marketing (Qogom, 2021).

The crime of unlawful processing of personal data is also one of the most significant offenses affecting privacy protection in the digital environment. It involves violations of fundamental data processing

principles, such as allowing unauthorized access to data, disclosing protected information, or transferring data outside the country without complying with legal regulations (Muneera, 2023). Other forms of infringement include hacking, extortion, and interception of communications, given their direct impact on individuals' privacy and dignity. Those responsible for collecting and processing data are obligated to implement adequate security measures to protect it from loss, damage, alteration, disclosure, or unauthorized access, commensurate with its nature and importance, and must report any breach or threat to it (Qogom, 2021). Other forms of personal data abuse include its theft for financial gain, either through extortion or sale, or the use of data to defame the individual to whom it belongs (Muneera, 2023).

III. LEGAL LIABILITY ARISING FROM INFRINGEMENT OF PERSONAL DATA

Civil liability is based on the occurrence of harm, whether in its contractual form resulting from a breach of contractual obligations, or in its tortious form based on an unlawful act. With the evolution of the digital environment, informational harm has emerged as a serious form of harm due to its potential consequences affecting individuals and society, which may extend to threatening public security when personal data is misused. The application of contractual liability does not raise issues in this area, as a contractual relationship exists between the user and social media platforms through the terms of use. However, controversy surrounds the extent to which tort liability—particularly that related to the custody of property—applies to digital data, given its intangible nature. Traditionally, liability for property is based on the presumption of fault on the part of the custodian, which can be rebutted by proving an external cause; however, applying this to digital data faces difficulties due to the multitude of parties involved in its processing, as well as the dispute over its legal nature. The modern approach, however, tends to regard data and information as elements of economic value, which justifies subjecting them to liability rules. This aligns with the recognition in Islamic jurisprudence that information constitutes a valuable asset, where liability is based on the principles of harm and causation, whether within or outside the framework of a contractual relationship (Qogom, 2021).

There are multiple parties liable for information-related harm on social media platforms, including the user, those authorized to access the content, the platform's management, companies contracted to manage content and analyze data, as well as web hosting providers. This makes determining liability complex and necessitates its distribution among these parties. In this context, the user bears some responsibility when publishing their data and determining the scope of its privacy by agreeing to the terms of use and privacy settings, as they have control over the extent to which their data is made available to others. Conversely, the platform assumes a supervisory role through content management, both before and after publication, with the ability to intervene to remove illegal content; this also extends to comments associated with published content, reflecting the overlap of responsibilities among the various parties (Alsadeq, 2016).

This necessitates the adoption of a clear legal framework that precisely defines the scope of each party's obligations, taking into account the nature of the role it plays in processing or disseminating data, in a manner that strikes a balance between freedom of use and the protection of personal data, and mitigates the difficulty of assigning liability in the digital environment.

Legal doctrine distinguishes between the publisher and the data host on the internet, where the host's role is limited to providing the technical infrastructure to store and make content available without interfering with its content, while the publisher has the authority to select and manage the content. This distinction is reflected in the differing scope of liability: the publisher is held accountable for the content under their control, whereas the host remains liable only when aware of the illegality of the content and fails to take the necessary measures to prevent or remove it. The intermediary is also treated as a host, and their liability arises only in the event of a failure to protect data or upon knowledge of illegal content without intervention (Qogom, 2021).

The researcher argues that distinguishing between publishers, data hosts, and service providers is a crucial basis for determining the scope of liability in the digital environment; however, practical application reveals a clear overlap in roles, making it difficult to draw a clear distinction between these categories. Comparative legislation has addressed the liability of internet service providers in some detail; the European Directive on Electronic Commerce determined that technical intermediaries are not obligated to monitor the legality of content, while requiring them to take necessary measures to prevent unauthorized access to it, and exempts the service provider from liability when it is not the source of the harm or involved in the selection or modification of information, while considering that temporary storage does not give rise to liability, and that it may be required to remove unlawful content in accordance with national laws.

Despite all these efforts to regulate the legal liability arising from harm caused by the processing of personal data, they still fall short of keeping pace with the rapid evolution of the digital environment, particularly regarding the overlapping roles of service providers, intermediaries, and platforms. More precise criteria must be adopted based on the degree of actual control over data and content, and the technical capacity to prevent or limit its

dissemination. It is also essential to strengthen preventive obligations on service providers, rather than merely reacting after harm has occurred, by imposing technical and legal measures that ensure more effective protection of personal data, thereby striking a balance between the freedom to use the internet and the protection of individual rights.

IV. CONCLUSION

The protection of personal data has become a central legal issue in light of the rapid development of digital technologies and the expanding use of the internet and social media, which has given rise to complex legal challenges regarding how to regulate the collection and processing of data and ensure its protection, as well as determining legal liability for damages resulting from its misuse. This research sought to clarify the conceptual and legal framework of personal data, review the most significant forms of its misuse, analyze the legal basis for liability, and identify the parties involved, thereby contributing to a deeper understanding of the requirements for protection in the digital environment.This study reached the following conclusions:

1. The concept of personal data has expanded to include all information through which a person can be identified directly or indirectly, reflecting legislative developments to keep pace with the digital environment.
2. The variety of forms of personal data violations, ranging from unlawful collection and illegal processing to hacking, data theft, and defamation, which increases the severity of these acts.
3. The inadequacy of some national legislation in precisely regulating the obligations of internet service providers, despite the pivotal role they play in data processing.
4. The overlapping roles of liable parties in the digital environment, making it difficult to definitively determine liability according to traditional standards.
5. The trend in legal doctrine toward recognizing digital data as an asset with economic and legal value, thereby justifying its subjection to civil liability rules.

Based on the findings of this study, a set of recommendations has been formulated, which we summarize as follows:

1. The need to strengthen the principle of transparency in the handling of personal data by requiring data processors to disclose the methods of data collection and use.
2. The need to adopt flexible standards for determining legal liability based on the extent of actual control over the data and the degree of knowledge of the violation.
3. The need to raise legal awareness among users regarding their rights to the protection of their personal data and ways to prevent its infringement in the digital environment.

REFERENCES

[1] Alsadeq, M. 2016. Social Media Networks and the Risks of Violating the Right to Privacy. Dar AlnahthaAlarabiya. Dubai.

[2] Muneera, A. 2023.Cybercrime related to personal data in the light of Algerian legislation. Judicial Ijtihad Journal15 (2). 177-194.

[3] Qogom, I. 2021. The Legal Protection of Personal Data on Social Media Platforms in Qatari Law and Comparative Law. Master Thesis. College of Law. Qatar University.

[4] Rahmani, I., Zain Alabdeen, L. 2025. Data Protection in the Digital Age. Tabna Journal for Academic Scientific studies. 8(2). 203-418.

★★★