# THE FUTURE OF BIOMETRIC DATA PROTECTION IN JORDAN IN LIGHT OF THE GDPR: DO WE NEED TO COMPLY WITH THE GDPR?

**Alaeldin Alkhasawneh, Yarmouk University-UAEU University**

## ABSTRACT

*The expansion of social media, artificial intelligence, and the Internet of Things has led to many challenges and risks for biometric data protection such as the unauthorized use or treatment of such data. The needs to protect biometric data and comply with the most important regulations have become paramount for information security, especially with the incorporation of new technologies based in biometric data into most of aspects of our daily life. Currently, data protection in Jordan is governed by several constitutional provisions and some sectoral laws, which have more recently been complemented by the new Data Privacy and Protection Bill, 2020, Draft Law. This study focuses on the future of biometrics data protection in Jordan and considers the compliance of new legislation with the General Data Protection Regulation (GDPR). This compliance is encouraged because of the universal nature of GDPR, by analyzing the ability of the new Jordanian data protection Draft Law to incorporate specific data protection principles. The novelty of this paper comes from the fact that little work has been done on best practices for biometric data privacy in Jordan, also, given the vital importance of judging and perfecting data privacy policies, especially in Jordan around this issue, this study provides insight on how Jordan might best perfect its Draft Law to protect human rights. It is certainly of interest to the fields of law and ethics. The author used content analysis to analyze relevant legislation and literature, we found that Jordan lacks a comprehensive legal framework for biometric data. Little information is available about how to best protect biometrics data, the nature of the system to which it is subject, and the extent of biometrics data protection. Accordingly, the Draft Law will require significant amendments before it can accommodate the level of legislation currently required.*

**Keywords**: Data Protection, Biometrics Data, Privacy, Jordan, GDPR Compliance.

## INTRODUCTION

Data protection has become one of the most important facets of information privacy, a pillar of digital human rights in the modern era. With the emergence and dissemination of big data, artificial intelligence (McDermott, 2017; Onikm et al., 2019), social media, smart cities, and biometric technologies, personal data has become more important and, moreover, a new fundament of economic, commercial, and administrative systems.

With increased mechanization, the emergence of the Internet of Things, and the use of biometrics authentication technologies, threats to privacy rights have multiplied (Data Breaches, 2020; Reidenberg, 2000). Many governments are now providing services digitally, and the digital economy is playing an increasingly important role in the growth of the global economy.

Hence, data have become more valuable and crucial for the process of innovation. Biometrics authentication technology is now used in all aspects of life: we use our faces or fingerprints to unlock our smart phones and our irises are now scanned in airports. These techniques offer many benefits: they save time; reduce human effort; and improve security, convenience, and service quality (Kindt, 2007; Erskine-Fox, 2020).

However, using biometric technology involves many risks for privacy and data protection. Storing biometric data in the system of a service provider may lead to misuse-such as unauthorized use, use for illegal purposes, use for a purpose other than that on which the parties initially agreed (Faqir et al., 2014 & 2013) and data profiling, discrimination (Sokolov, 2008), identity theft, the selling of data without authorization, and permanent undesired surveillance. Such risks may extend to relatives who share the same genetics as the original subject (interested parties may, for example, analyze relatives' behaviors or preferences and interests). Moreover, because biometric data are eternally unchangeable, many risks arise when such data is stolen, compromised, or copied.

Consequently, many countries have adopted legislation to protect personal data (Graham, 2017), limit data processing and movement abroad, and secure files and assets against breaches. On May 25, 2018, the European General Data Protection Regulation (GDPR) came into effect (Determann, 2018); this act represented a major turning point in the protection of personal data. The GDPR replaced all previous data protection laws (Directive 96/46) in EU member states. Similarly, Jordan has also been heading toward the preparation of data protection laws with its drafting of the Data Privacy and Protection Bill, 2020 (Jordanian Constitution Law, 2020) (Determann, 2017).

This paper analyzes the regulations relating to biometric data protection in Jordan and highlights the level of data protection available in the nation. The objectives of the paper are to discuss GDPR, the Jordanian legislation requirements, and the principles of biometric data protection. Our reasoning for discussing the GDPR principles in this paper is that because Jordanian legislations should comply with this regulation for many raisons such as the commercial relations between Jordan and EU, and the extra-territorial effect of GDPR. Moreover, this paper also seeks to describe the primary technical and legal risks of using these technologies and to explain legislatives measures that may help avoid these risks.

While this article focuses on biometric data protection in the GDPR, its key principles, and its potential implications for companies and websites, the study was limited to the collection, treatment, transfer, and protection of biometric data in Jordan under the new bill. Along these lines, this article highlights how Jordanian businesses will be affected by the new European regulations and Jordan's compliance with the GDPR. Ultimately, this study sought to shed light on the concept of biometric data protection, its risks, its legal facets, and the ability of Jordanian legislation to provide adequate data protection. My research questions included: is Jordan's bill sufficient and consistent with the GDPR? What is the scope of the right on biometrics data and what might this right mean? Should there be independent protection for this right? Is our privacy at risk because of biometric data? In this spirit, this paper illuminates the importance of a legal framework to protect biometric data in Jordan in light of the development of technologies that reveal identities and use biometric data.

Regarding research accuracy, it is important to note that I recognize the importance of the results of this study's examination of the legal aspects of biometric data and the seriousness of its impact on privacy-the public should be aware of such laws to which they are subject and ensure

that they do not trouble their privacy rights. Notably, the novelty of the topic of biometric data has resulted in related legislation being similarly novel in Jordan. Along these lines, this study was limited by the scarcity of facts and jurisprudential writings available on this topic in Jordan.

## RESEARCH METHODOLOGY

I used content analysis to analyse biometric data protection in Jordan. More specifically, the study analysed and interpreted Jordanian legislation regulating the protection of biometrics data; in particular, I examined Jordan's new Draft Law and clarified its ability to protect data in line with the GDPR. Notably, the study relied on two primary sources of information:

1. Articles, reports, and other online publications.
2. The European GDPR and other relevant pieces of international and Jordanian legislation.

Case law was not included because it was neither published nor available. The following section briefly overviews the GDPR. Next, I review the biometrics data protection system in Jordan and analyze its Draft Law.

## LITERATURE REVIEW

### Overview of the GDPR

On May 25, 2018, the EU began implementing the GDPR, which requires companies to protect the personal data and privacy of EU citizens related to transactions occurring within EU member states. The GDPR applies to all companies that manage the data of EU citizens (Goddard, 2017; Duncan, 2019).

The new European regulations introduced a number of new concepts that depend partly on technical solutions that could be embedded into legislative and regulatory frameworks, which could be more restrictive than all possible solutions, to ensure better protection. The regulations sought to integrate existing European data protection laws in the interest of transparency, individual rights, and the growth of the digital economy (Wolters, 2017).

It is undoubtedly important for commercial companies operating within the European market to avoid difficulties related to European laws (Lynskey, 2017). In addition to providing more latitude for protection, which helps raise confidence levels, companies find it easier to comply with European legislation that applies to different countries in the EU. This legislation responds to a central need as well: building confidence and security in cyberspace and protecting developments in information technology (Goddard, 2017). The new legislation has enforced new rules for data protection and respect for the rights of privacy on companies, government departments, and organizations that provide services to European citizens or EU residents or that collect and process their data, even if their place of residence is outside the EU. Additionally, this legislation enables the data owner to regain control of and review what is published and exchanged, even with the controller or processor of the data, who may not have personally collected the data-ultimately, the legislation reinforces the rights of citizens or residents of EU countries to request an electronic version of their data. More specifically, the legislation accomplishes this by adopting a number of new rights, such as the right to be forgotten and the right to know the purpose of the action.

## Defining Biometric Data

Biometric technologies have become the most important development in identification and authentication technologies. Biometrics improve security, efficiency, and accuracy. We use biometric authentication technologies in our daily life, such as fingerprint or facial recognition to unlock smartphones; fingerprints at work, the bank, and in police investigations and surveillance; the iris at airports and border control; and voice recognition with Siri and Alexa (Sokolov, 2018). Using biometric technologies helps determine identity (Krausová, 2018; Joseph, 2018) Can we thus consider biometric data personal data?

Notably, Article 4 of the GDPR can be applied to any personal data that may help to determine a person's identity. Here, "*personal data*" means any information relating to a person whose identity has been identified directly or indirectly, such as the person's name; social security number; site data (IP address or e-mail address); and physical, physiological, genetic, mental, economic, cultural, or social characteristics. The regulation aims to give users complete control over their data; thus, companies would be unable to obtain any data from users without their prior consent.

Technically, biometric technologies help to identify persons by means of their biometric features (Sprokkereef, 2008). Therefore, biometric data can be analysed with the help of pattern recognition systems and machine learning techniques to derive desired information, provided that a link has been identified between the data available from biometric sensors and a certain indicative quality. Consequently, biometric data allows the indirect identification of persons (Josserand, 2016). More specifically, biometric data can technically identify a person by converting a characteristic or behavioural trait of a specific person into a digital print. The data indicates a person's uniqueness by capturing constant and unchanging bodily features. Hence, we can classify biometric data as personal data.

Also, paragraph 14 of Article 4 of the GDPR defines "*biometric data*" as personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. The GDPR definition of biometric data is a vast definition that includes new types of biometric data that may arise with the development of technologies of biometric authentication. Notably, it refers to both the *"physical and physiological characteristics*" encompassing the traditional examples of fingerprints and facial images as well as iris recognition, voice recognition, DNA recognition, and behavioural characteristic recognition. The first category of biometric data is information pertaining to physical or physiological characteristics, such as facial information, fingerprints, iris scans, etc. The second category is behavioural information (Zimmerman, 2018). There is no doubt that behavioural characteristics permitting the identification of a person must be considered biometric data. However, it is unclear just how narrowly regulatory authorities will interpret this category or what limiting principles, if any, will guide their analyses. Information pertaining to a person's habits, actions, or personality could be considered behavioural information within the scope of the definition, this a potentially broad category as it has no nexus to the sort of bodily information typically thought of as biometric data. Due to this inherent uncertainty, privacy professionals should closely monitor guidance delineating the types of behavioural information deemed biometric data.

In addition, biometric data can contain information of a sensitive nature, such as information related to health conditions, predisposition to disease, and racial origin. With big data technologies, biometric data can be analysed to retrieve information about yet-undetected diseases and current mental and biological states. Such possibilities augment the indicative value of this kind of data. Moreover, they also give rise to questions about the scope of such augmented indicative values of biometric data, their impact on the vulnerability of data subjects, and their overall impact on privacy protection in the field of biometrics.

According to Article 4 of the GDP, biometric data are classified as a special category of personal data and are also treated as sensitive data (Sprokkereef, 2008). In contrast, the Jordanian bill does not define biometric data. Instead, biometric data is classified as sensitive data and the bill accordingly allocates biometric data with its provisions for sensitive data and does not address the conditions of its collection and treatment with any special rules. To conclude, biometric data are data of a particular nature resulting from a specific technical treatment of the physiological characteristics of a natural person or their behaviours.

As an example of compliance with the GDPR, Jordan's Draft Law includes under "*personal data*" any information in any form related to an "*identifiable individual*"-directly or indirectly identifiable-especially that accessed through their personal identification number; formal or physiological characteristics; or factors indicating their mental, cultural, economic, or social identity. Notably, the Draft Law is also compliant with the GDPR in that it determines whether an individual is capable of knowing and thus of taking into account all the means used by the data manager or any other person that may have been available to them. We can see that the definition contained in Article 2 of the Draft Law is a comprehensive and unambiguous definition of personal data. This definition of personal data has expanded the scope of law enforcement, so it is likely to ensure the reduction of cases of the infringement of personal data, especially in regard to the development of data collection techniques and participation on social networking sites and the Internet. We note that this definition is similar to the definition used in the GDPR.

The Draft Law did not specify the terms of the person identifiable but set several criteria that may contribute directly or indirectly to this identification; references to the identity number or Internet address; or one or more factors that could reveal an individual's physical, physiological, psychological, economic, cultural, social, genetic, or mental identity.

The Draft Law also introduces sensitive data and indicates that sensitive data may include any personal information that directly or indirectly reveals financial information, ethnicity, political or religious opinions, party affiliations, health or physical information, mental state, marital relationship, or religious beliefs. Although differing in terms of gravity and importance, and therefore requiring greater protection, sensitive data are identified, for example, without an exclusive enumeration of type. Notably, the Draft Law includes specific texts regulating the requirements for sensitive data operations but does not distinguish between the penalties prescribed for the use of personal data and those prescribed for the use of sensitive data.

## Current Data Privacy Laws in Jordan

Jordan does not currently possess a separate data protection law, and the Constitution of Jordan does not clearly grant the fundamental right to privacy. Subsequently, the GDPR sparked hope and interest in the country for a separate codified law relating to personal data protection in

line with the GDPR.

## Constitutional Law Context

Privacy is a constitutional right, and it could apply to both the government and the private sector. Article 7 of the Jordan Constitution states that "*Private life is inviolable*" (Jordanian Constitution Law**,** 1952) and Article 15 of the Constitution speaks about the freedom of communication and guarantees confidentiality in accordance with the law:

> *"Post, telegraphic, electronic, telephone, and other means of communication are inviolable, and their confidentiality is guaranteed and cannot be confiscated or accessed."*

The rights and freedoms of the citizen shall not be tolerated or prejudiced. Along these lines, Article 18 states:

> *"All postal and telegraphic correspondence, telephonic communications, and the other communications means shall be regarded as secret and shall not be subject to censorship, viewing, suspension, or confiscation except by a judicial order in accordance with the provisions of the law"*

## Other Legislation

The Jordan's penal code provides that the publication of personal data concerning the life of individuals or families is a crime punishable by imprisonment and a fine (Jordanian Constitution Law, 1960). Article 384 of the penal code states:

> *"Responding to the complaint of the victim, one is penalized for not more than three months in jail for breaching the private lives of others by eavesdropping, peeking, or any other medium, including recording audio. The penalty is multiplied in case of repetition"*

Meanwhile, Article 356 of the penal code states,

> *"Anybody who spreads the content of a private call within the capacities of his position in the telephony service will be penalized for six months or charged with 20 JOD."*

Additionally, the Cyber Crimes Act (Jordanian Constitution Law, 2015) penalizes a number of specific activities related to piracy and data protection. This includes a fine for unauthorized access to websites, information systems, and networks (Article 3/a) and imprisonment for any acts resulting in the canceling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring, or copying of data or information; the stopping or disabling of the operation of an information system; the changing of a website; or the canceling, destroying, or altering of its content or assuming its identity or the identity of its owner (Article 3/b). Article 4 states:

> *"Anyone who installs, publishes, or uses intentionally a program through an information network or information system, with the purpose of canceling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring, copying, capturing, or enabling others to view data or information, or obstructing, interfering, hindering, stopping the operation of an information system or preventing access to it, or altering a website or canceling it, destroying it, or altering its content or operating it, assuming its identity or the identity of the owner without authorization or in violation or*

*excess of the authorization".*

Article 5 penalizes:

> "*Anyone who intentionally captures, interferes, or intercepts what is transmitted through an information network or any information system."* Article 6 penalizes *"anyone who intentionally and without authorization obtains through an information network or any information system data or information relating to credit cards or data or information that is used in the execution of electronic financial or banking transactions."*

This covers anyone who intentionally uses an information network or any information system data or banking transactions to obtain for oneself or others the data, information, assets, or services of others.

The Cybercrimes Law punishes any act that compromises the privacy of another person through technological means, namely:

> *"Tapping, intercepting, recording, transmitting, or disclosing conversations, communications, audio, or visual materials and photographing others, creating, transmitting, disclosing, copying, or saving electronic images. The publication of news, photographs, scenes, comments, data, or information, even if they are true and correct."*

Article 21 covers imprisonment and a fine for the modification or processing of records, images, or scenes through technological means for the purpose of defaming or abusing another person or attacking or violating their privacy. The law penalizes any person (by fine or imprisonment) who illegally accesses someone else's computer without the person's knowledge or permission. The Telecommunications Law No. 13 of 1995 restricts the service providers from sharing customer data to third parties and prohibits telephone tracking of the customers. Article 29 of the Telecommunications Law (European Union, 1995; Jordanian Constitution Law, 1995) states

> *"That the licensee should commit to provide the necessary facilities to the competent authorities for the implementation of court and administrative orders that have to do with tracking communications specified in these orders."*

The Telecommunications Regulatory Authority (TRA) regulates electronic and commercial transactions. The TRA falls under the Telecommunications Law and protects the interests of the beneficiaries of telecommunication and information technology services. This includes the preservation of the confidentiality of the beneficiaries' data. Such data shall not be disclosed except by judicial orders based on the text of Article (29 g) of the Telecommunications Law. The TRA is concerned with the verification of private subscription contracts between the licensees and beneficiaries of telecommunications services and the extent to which the licensee complies with the contracts approved by the TRA. The TRA has a number of data protection laws, including the Electronic Transactions and Commerce Act and consumer protection regulations:

The Jordanian 2015 Electronic Transactions Act aims to protect the rights of persons conducting electronic transactions or promoting and facilitating electronic transactions and correspondence through the means of reliable electronic records; reducing fraud in electronic correspondence; and establishing standard rules, regulations, and standards for the authentication

and integrity of electronic communications (Jordanian Constitution Law, 2015). The law imposes a duty of confidentiality on electronic authentication providers and penalizes the violation of this obligation. The Jordanian 2018 Consumer Protection Law does not provide provisions for the protection of consumers' personal information (Jordanian Constitution Law, 2018). This law includes an article regulating consumer protection, the provision of assistance during complaints, and the establishment of a database related to consumer protection to help it conduct and publish research (Article 15). It is unclear if the sort of data that the Consumer Protection Society can gather includes consumer data (and, if so, how personal the data will be) or if it is limited to data concerning products and suppliers.

There is no doubt that changes regarding personal data and their treatment were not accompanied by other appropriate changes in the Jordanian legislation. These legal texts remain separate texts dealing with certain aspects of privacy in specific areas. They deal with the methods of collecting data by lawful means, determining how to preserve them, the duration of their preservation and intended purpose, and the use and processing of data without harming the owner. They penalize those who infringe upon it and protect the right of the data holder to modify or delete the data.

Traditional legal texts, therefore, cover only a portion of personal rights and are far from protecting individuals from the risks of collecting, storing, and transmitting data in the new technical environment. There is a legislative gap in dealing with personal information, and this legislation was designed in accordance with some provisions of the penal code that deal with the right to protect traditional secrets.

**Do we need a Specific Regulation for Privacy and Data Protection in Jordan?**

The necessity of regulating data and privacy laws can be justified by factual and legal considerations. These issues can be illustrated by numerous violations committed by public or private institutions against user privacy and by some steps adopted by the Jordanian government toward using technologies that may affect citizen privacy. In 2019, Access Now and Impact International prepared a study about the most important ISPs in Jordan. This study demonstrates that these providers violate the privacy of users by monitoring their use of the Internet and recording their surfing history (Samaro, 2019; Kanimozhi, 2019).

Consequently, the Ministry of Information Technology now verifies, through the Telecommunications Regulatory Authority responsible for the regulation of telecommunications services in Jordan, cases of major user privacy violations by the major Internet providers in Jordan. It also prepared a Draft Law on protecting personal data and submitted it for public consultation more than four times to address such observations. Meetings, workshops, and seminars were held with stakeholders on the subject of personal data from public and private sectors, the academic sector, and civil society organizations to enable the largest possible segment of stakeholders and partners to express their views and comments on the contents of the Draft Law.

Important to note here is that the European Union indicated that Jordan has not progressed in safeguarding the right to privacy.(European Union, 2018)In November 2018, at the thirty-first session of the universal periodic review, Jordan received two recommendations on the right to privacy-Estonia and Brazil drew attention to the need to respect the privacy of citizens. However, Jordan's experience has shown that threats to privacy and digital rights not only come

from the government, but also from international agencies and companies, including Internet service providers and emerging technology companies (Sharbain, 2019), Also, since 2018, The Jordanian government replaced the old Identification cards with smart ID cards that include chips that store iris and fingerprint data. Until now, Jordan did not have reader technologies or texts regulating information confidentiality stored in this chip; in addition, the nation also did not have penalties for the misuse of such information. Meanwhile, when activating a new phone line in Jordan, the subscriber was required to present an ID card to register a SIM card or a passport for foreigners, and there was a tendency to include fingerprints (Privacy International, 2019).

In 2018, The Telecommunication Regulatory authority declared that it was preparing new regulations that require new owners of SIM cards to submit fingerprints to authenticate their lines. Finally, The World Food Program partnered with the UNHCR and the Jordanian / British company Iris Guard to implement a dynamic transaction system by which refugees can purchase food and groceries and obtain cash from ATMs by scanning their irises. There are concerns about whether refugees are aware of the option to withdraw from this system, let alone whether they grant their prior approval.

Therefore, in 2019, the Ministry of Digital Economy and Entrepreneurship conducted the fourth round of consultation on the Draft Law for personal data protection (Privacy International, 2019). It confirmed that the new law would protect user data in Jordan and combine the relevant laws on data protection. This is of great importance, given how vital these data are for service providers. This Draft Law accommodates the growing need to protect personal user data throughout the region and the world in the face of growing electronic threats. Hence, preserving the privacy of open data and protecting the identity of individuals in the digital space are dilemmas currently faced by individuals and countries worldwide.

To be sure, several fundamental considerations situate the new Draft Law as of paramount importance. First, the current era is characterized by "*massive data*" resulting from the use of digital devices, computers, and the Internet of Things. In this Internet era of smart objects and homes, personal user data is no longer limited to names, photographs, and phone numbers, but instead now also includes vital data such as fingerprints, face patterns, and handprints as well as health data, geographic location, and other miscellaneous personal information. Second, the Draft Law is part of a long series of steps taken by Jordan to protect personal user data. In this context, users of e-government services, tablets, and smartphones are building a secure knowledge economy and reliable electronic commerce. Additionally, the new Draft Law entails adopting the best international practices aimed at protecting and controlling individual data within legal frameworks, particularly those in the EU, such as the GDPR. These facts, accompanied by the increasing use of biometric technologies, evidence the necessity of effective regulation concerning personal data protection.

## Critical Vision of the Data Protection and Privacy Draft Law, 2020, In Jordan

This section analyzes the Jordanian Draft Law in light of the GDPR by examining its features, flaws, and future recommendations. First, it is important to note that the Definitions and Scope of the Draft Law are broad and unrestricted. The Draft Law's provisions are applicable to all data controllers that conduct any operations on personal data, whether in electronic or non-electronic form, in whole or in part. The provisions of the law shall apply to the controllers within Jordan and to the personal data of natural persons in Jordan, even if the controllers are

outside Jordan if the treatment of these data monitors the behavior of the owner of the personal data, their commercial relationships, or services that they received. Additionally, excluded from the scope of the application of the Jordanian Draft Law are personal data that are dealt with by individuals in a familial or personal context (Jordanian Constitution Law, 2020). The Draft Law protects all individuals worldwide if their personal data are processed in Jordanian territory. Jordanian residents are also protected when their personal data are processed outside Jordan if the processing is in connection with business conducted in Jordan, the systematic offering of goods or services to data subjects in Jordan, or activity involving profiling Jordanian residents. The Draft Law applies to the processing of all personal data collected, disclosed, shared, or otherwise processed within Jordan. The definition of processing includes any outsourcing operation that transfers foreign personal data to Jordan. So, any foreign company that deals with data outside Jordan would have to comply if it processes personal data, and such processing is in connection with business conducted in Jordan, a systematic offering of goods and services to Jordanian residents, or activity involving the profiling of Jordanian residents.

The Jordanian Draft Law ensures the development of a data protection council that is autonomous and professional; however, the autonomy of the council has some limitations. The Draft Law requires the inclusion of two specialists and technicians with experience in the field of personal data protection, but this is achieved through a decision by the ministers' council and after a recommendation from the chief of the Data Protection Council. Article 4 states that the council shall consist of the Minister of Digital Economy and Entrepreneurship, the Commissioner of Protection, the Ministry of Communications, the Ministry of the Interior, the Ministry of Justice, the Army, the Information Commissioner, the National Council for Human Rights, and two competent members with experience in the protection of personal data. Regarding the Privacy Council or the Personal Data Protection Council, it is noted that the composition of the committee does not guarantee its autonomy (Hamouri and Reem, 2014). Most of its members are connected to the government, and while the draft stipulates that it should include technical specialists with experience in the field of personal data protection, it does not stipulate including legal members.

The Jordanian Draft Law gives authority to the Ministry of Digital Economy and Entrepreneurship. In addition, in Article 6, it requires the establishment of a personal data protection unit in The Ministry of Digital Economy and Entrepreneurship and the appointment of at least an appellate judge as Commissioner for the protection of personal data, which is advisable.

The Draft Law stipulates in Article 11 that the controller is responsible for the data under their control and the data delivered to them, the establishment of specific procedures with respect to personal data processing and the receipt of complaints, and the publication of these procedures in the media and on their website. The controller is obliged to designate a qualified observer to protect personal data and establish systems to prevent intrusion and document data operations.

The draft affirms the confidentiality of personal data in Article 13. The conditions cover the disclosure of data, the disclosure of the identities of the entities, what data could be disclosed, and the necessary permits under a special regulation. Article 13 also requires the controller to take security, technical, regulatory, and data protection measures to prevent data detection, alteration, destruction, breach, or other unauthorized actions, and this requirement complies with the GDPR.

In the event of a breach that could negatively affect any data subjects, the data controller

should inform the Commissioner of Protection of the source and mechanism of the breach and the data owners who were affected within 72 hours from the discovery of the breach. The controller also needs to notify the data owners within 24 hours and advise them of necessary measures to avoid the effects of the breach. The data controller is responsible for compensating the data holder for the breach (Article 13; Jordanian Constitution Law, 2020), and this procedure is in compliance with the GDPR.

The text does not clearly specify the cases in which government agencies are permitted to collect, process, or share data without the data owner's consent. Additionally, it uses broad terms such as "*national security*" and does not provide clear criteria for the concept of national security (Hamouri and Reem, 2014). Moreover, the draft does not refer specifically to the government agencies that are exempt from obtaining the data owner's consent but refers to the government agencies collectively instead.

The principles of transparency in dealing with personal data and maintaining data accuracy require the data owner to be informed. Additionally, for access rights, the bill grants the data owner the right to view and modify their data and requires data providers to provide suitable electronic or non-electronic means of access through which the data can be viewed and modified securely (Hamouri and Reem, 2014). Articles 17-2 and 19 cover the right to access and update personal data, and the provision of appropriate electronic or non-electronic means to do so in a secure manner (Jordanian Constitution Law, 20014).

The entity collecting data must ensure adequate precautions to protect data from hacking during data collection, processing, or sharing, and the data protection authority must ensure that these precautions are present and effective. The text indicates in Article 13-2 that strict measures are required to protect personal data. The data owner is entitled to compensation in the event of data damage due to the negligence of the party collecting or processing the data.

For the data protection authority to exercise its function of monitoring data operations, it must inform the parties dealing with the personal data. This is done through notifications or registrations of these entities with the personal data protection authority. However, the draft does not specify what data should be included in the notification, nor specify when the notification should happen, periodically or when modifying the terms or privacy policy. It does not specify the parties excluded from the notification both (Hamouri and Reem, 2014).

Regarding the activities and establishment of an observer, Article 3, paragraph 2 specifies that the data protection authority shall be notified by the observer of an internal representative. It also specifies that the provisions of the law shall not apply in exceptional cases, such as personal data exclusively maintained by natural persons or family, data processed to obtain official statistical data, or in the application of an independent legislative text relating to judicial investigations, terrorism cases, and all forms of organized crime. However, in such cases, the party responsible for such investigations shall first notify the personal data protection authority of the nature of the data in their possession and the purpose of their treatment, and their importance in such investigations.

## Features of Biometric Data Protection in GDPR and in Jordanian Draft Law

Reviewing the provisions of the Draft Law demonstrates that it significantly reflects the GDPR. It includes many of the requirements contained in the GDPR, and it has drawn inspiration from this regulation. Given the particular nature of biometric data and the increasing

amount of biometric technologies, regulation seems crucial to give consumer confidence and comfort to use these technologies in secure conditions. Unless the protection is efficient and sufficient, biometric authentication technologies represent a real risk for privacy; this has led many countries to legislate texts and provide better levels of protection for biometric than for other kinds of personal data.

The GDPR set many provisions that provide protection of biometric data. As biometric data constitute personal data, they should be governed by the legal framework reserved for personal data and, moreover, as the GDPR considers biometric data a special category of sensitive data, the requirements reserved for sensitive data should be applied to biometric data to afford them a higher level of protection. (Sokolov, 2018)

The GDPR has also left states with a process of regulating the handling of "*sensitive data*." Article 9 prohibits the processing of sensitive data that reveals racial or ethnic basis, political opinions, religious and philosophical beliefs or affiliations, and genetic and biometric data collected with the aim of identifying a natural person on their own as well as the processing of health or sexual data.

The GDPR's legal framework for personal data protection is characterized by many features and requirements. For our purposes, it is important to note that these requirements are applicable to biometrics data as follows. Notably, the GPPR sets stricter terms for data approval and acceptance with the Lawful Bases for Data Processing-explicit consent from the user is required before data collection, processing, or use. Clear consent must be delivered in understandable, unambiguous language, and the reason to process or store the personal information must be provided. Unambiguous consent is required for data that is not sensitive personal data as well as sensitive personal data such as biometric or physical or mental health data. However, companies will now need to work harder to prove that consumers have understood and agreed to the terms of use.

The new Jordanian Draft Law sets a lawful base for the processing of data including biometric data. Data processing includes a simple process of dealing with personal data that includes collecting, storing, modifying, using, and disseminating such data. The Jordanian Draft Law includes the crucial legal principles for the protection of personal rights, notably, consent, contractual necessity, and the complete legitimate interests of the controllers and the third party. Thus, this draft aims to raise Jordan's level to international standards, especially the GDPR.

Under the Draft Law, companies have to address a series of requirements similar to those established by the GDPR. In order to protect all "*personal data*," the Draft Law regulates the treatment of such data through "*processing*" as expressly defined by the law (Article 2 of the Draft Law); therefore, data controllers must provide a lawful processing basis to process both personal and sensitive data. The Draft Law specifies permissible bases for data processing for each category. For personal data, this includes any process or group of operations performed on personal data by automated or non-automatic means, such as, for example, organizing, classifying, storing, modifying, restoring, using, disclosing, transmitting, publishing, sharing, integrating, blocking, scanning, or destroying data. In addition, there are conditions that must be considered for the personal data being processed, such as, fair and legitimate treatment; data collection for a legitimate, specific, and clear purpose; any subsequent processing being conducted in a manner consistent with the collection purpose; and subsequent processing not exceeding the purpose of collection or treatment. The data should be true and accurate and subject to updates when appropriate. Additionally, the owner of the data should be permitted to

delete it after the purpose of the collection or treatment has been fulfilled. Data stored for longer periods for historical, statistical, or scientific purposes shall be preserved in an anonymized format by storing them in a form that does not enable the proportion of such data to the owner. If this is not possible, the identity of the owners should be encrypted.

However, some of the most important changes in GDPR are the new design and accountability principles (Van-Der-Hof and Lievens, 2018), which require the effective management and implementation of data protection principles, as well as the effectiveness of any institution complying with the requirements of the GDPR.

The right to be forgotten: Article 17 of the GDPR enables users to request the erasure of complete personal information unless there is a valid reason (Jones and Ausloos, 2013). It obliges companies to fulfill the request and survey the data. If these data are being used in other sites, then the company providing the data requests the recipient site to scan the content and user data based on user desire.

The transparency or the right to be informed, which entails the right of consumers to be aware of the information stored about them, as it will be used after obtaining explicit consent from them (Ross, 2017).

Privacy by design and default setting (Van-Der-Hof and Lievens, 2018). To ensure that personal information is sufficiently protected, the new regulations must implement protection to strictly control access to data and grant access only when necessary (Gjermundrød et al., 2016).

The right of access to data and transferability: anyone can request their personal data in an easily downloadable version at any time and can use or transfer the data to any other site or service (Article 12 and 20; European Union, 2016).

Portability (Lynskey, 2017): This is the right permitting individuals to access to their personal data to reuse across different services (Diker, 2018).

The right to the privacy of children (Article 8; European Union, 2016): parental consent will be required for the processing of personal data of children aged less than 16 years for online services. The age may vary depending on the member state, but consent is required, at least for children below 13 (Article 8; European Union, 2016). Data controllers are required to create a mechanism for age verification and parental consent to process children's personal data.

The "*right to correction*" enables individuals to erase or request personal data or to refuse to use it under certain circumstances, although there are several exceptions.

Appointment of representatives: the new data protection act requires that social media companies appoint a representative before the EU who can be held accountable for their firm commitment to the GDPR laws within Europe. This applies even if the company is based outside Europe and processes personal data related to the offering of products to data subjects in the EU or monitors the behavior of EU-based data subjects.

Regarding data owners' rights to personal data, the principle of transparency between the data owner and data controller is required to maintain the accuracy and integrity of the data, and the GDPR permits the data holder to view and modify it. The Jordanian Draft Law concurs with this text and permits data owners the right to view the data and its modification (Article 18; Jordanian Constitution Law, 2020), but it does not require the controller to provide the practical means to enable the data owner to view and modify their personal data. According to Article 18, personal data should be accurate and updated periodically, and the data owner shall be obliged to provide the controlling party with the necessary information to update and correct the data. The data controller, data processor, and the user are required to safeguard the appropriate information

to prevent penetration, ensure the detection and tracking of penetration cases, and provide the necessary means of security.

As for the obligations of the party dealing with the personal data, the GDPR requires them to notify the Data Protection Committee about this participation and its objectives and means, and the committee is required to monitor their interaction with the data. The Jordanian Draft Law does not require the committee to share data. Moreover, the law does not require the reasons and means of participation between these entities to be clarified. However, according to Article 20, no data may be transferred or exchanged electronically or non-electronically with any party within Jordan without express and written consent, and the transfer or exchange shall meet a legitimate interest of the regulator and the recipient of the personal data. The data owner should have sufficient knowledge of the recipient of the data and the purpose of transfer or exchange. The transfer of data for commercial purposes or the marketing of products or services is prohibited without the data owner's consent.

Regarding the issue of data sharing abroad, some companies resort to sharing personal data about individuals. This involves risks to personal data, especially with technical development. The GDPR requires special rules establishing a number of requirements to ensure the adequate protection of the personal data of EU citizens, especially in light of the proliferation of electronic means of storing data such as cloud computing (Al-Sharieh, 2011). The Jordanian bill complies with this provision, but it does not stipulate security measures like data encryption to protect personal data during participation. The Jordanian Draft Law stipulates that the transfer of data is limited to countries providing an adequate level of protection. Article 21 states that data may not be transferred or exchanged outside Jordan to countries or entities with insufficient data protection, and whose data protection level does not meet the provisions of this law. However, the bill accommodates some exceptions in this area: essential judicial cooperation in the fight against crime when it is necessary to deal with the data owner and to combat disease, epidemics, and health disaster, that is, a transfer or exchange under an international agreement. This is for the sake of national interest and permitted by the Council of Ministers. It is by the data owner's consent if they know that they have an adequate level of protection. The bill does not require the committee to be informed about the data sharing process between these entities and companies. The bill stipulates explicit consent for the transmission of data beyond borders, but it does not stipulate special security measures such as encryption during the transfer.

For the duration of the retention of personal data, the preservation of the data stored by the parties dealing with the personal data is considered to be contrary to the rights of the data owner and may infringe on the data protection rules. The GDPR has regulated this issue, but the Jordanian Draft Law does not specify a period after which the controlling parties are required to delete data, and it does not allow the data owners to delete it themselves or request that their data be deleted (Article 17-3; Jordanian Constitution Law, 2020).

The GDPR's consideration of biometric data as a special category of sensitive data suggests that such data should be treated according to the legal framework reserved for sensitive data, for which the GDPR provides a separate processing regulation (Zimmerman, 2018). Article 9 of the regulation preserved the principle of prohibiting the processing of this data and introduced some requirements for its processing; notably, these requirements were accompanied by a number of exceptions, such as informed consent of the person concerned, public interest, scientific research, and preventive medicine.

Biometric data may be processed only if the data subject has given explicit consent, if processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the fields of employment and social security and social protection law, if processing is necessary to protect the vital interests of the data subject, if processing is necessary for the establishment and exercise of defense of legal claims, or if processing is necessary for reasons of public interest.

Also, the protection of biometric data as a special category of sensitive data is governed by some requirements. More specifically, the Privacy Impact Assessment in Article 35 of the GDPR obliges the data controller to proceed with a Privacy Impact Assessment. The data controller should conduct an impact assessment and document it before starting the intended data processing. This assessment is mandatory for the automated processing of a large range of data and poses a high risk for human rights. This can be applied to biometric identification technologies: most biometric data may constitute a high risk and operate across large ranges using advanced technology. A data controller must identify related risks and adopt appropriate measures to reduce these risks. Moreover, a data controller should also consult with the supervising authorities before performing a high-risk treatment.

Privacy by design, this principle means that designers should have privacy in mind from the start when they define the features and architecture of a system of biometric authentication technologies.

Meanwhile, Article 37 of the GDPR obliges the data controller to appoint a data protection officer-if the data processing is carried out by a public authority or body, then the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope, and their purposes, involve the regular and systematic monitoring of data subject to a large scale.

Notably, the Jordanian Draft Law does not allocate specific texts for sensitive data. The deeper point here for our purposes is that while the Jordanian Draft Law is an important step in biometric data regulation, it still needs to take the following concepts into account. First, the Draft Law should distinguish between penalties related to sensitive data and normal data. Second, the lack of a requirement to inform the person concerned with the participation of different parties and the lack of a clear delineation of the reasons and means of participation between the parties for both the committee and the data owner need to be considered. Third, while the text of the law stipulates explicit consent for cross-border data sharing, special security measures, such as encryption, to protect data during its participation are not mentioned. Fourth, the Draft Law does not yet prevent parties from evading responsibility if a data breach results from negligence. Fifth, the Draft Law does not address surveillance cameras in public and private facilities as tools to collect personal data about citizens and does not note the importance of subjecting such technologies to the protection authority. Sixth, power remains concentrated in the hands of the executive: the Ministry of Digital Economy and Entrepreneurship is almost exclusively responsible for dealing with data processing requests. While the Draft Law grants the ministry these powers, it stipulates that

> *"Except for exemptions provided for in the preceding article, those wishing to collect and process personal data shall inform The Ministry of Digital Economy and Entrepreneurship in accordance with a duly authorized permit."*

Unlike other countries, such as France, that have data protection authorities composed of deputies, judicial authorities, various ministries, and sometimes the private sector, this bill limits these powers to one ministry. This structure does not include checks and balances from a wide range of stakeholders, which increases the risk of arbitrary decisions and abuses of power and, thus, exploits personal data. Seventh, the Draft Law still lacks significant preventive measures. The rules of data collection in the bill are ambiguous. The bill does not require that there be a particular objective for the data collection process or that the data collection process be proportionate to the objective; instead, it states that the collection process should not *"go beyond declared objectives"* and should be *"for legitimate, specific, and explicit objectives"* without defining these objectives.

Instead of enumerating cases that require a permit to process and report personal data, the bill provides a list of cases that do not require a license or permit. The bill does not require "the authorization or application of any license to process personal data" from such parties as

> "*Students and pupils by educational institutions*" or "*members of enterprises, commercial enterprises, trade unions, associations, and professionals.*"

Hence, individuals in this category do not enjoy the protection of the already weak guarantees of this bill, and the latter does not force exempted institutions to inform individuals of their data collection or request for consent.

The provisions on data-processing officials do not contain any clear regulations or interpretations. The law does not specify how to choose the officials and does not outline a code of conduct for them to comply with, unlike Article 40 of the GDPR, which provides for an overseeing body to enforce codes of conduct. In addition, there is no article requiring officials to inform individuals if there is a breach of data, which may lead to further abuses of authority. While Article 100 allows officials to object to "*arbitrary requests*" without specifying what is meant by "*arbitrary*," the restrictions they impose reduce access and correction because data-processing officials may determine the validity of requests in vague terms.

## RECOMMENDATION

Jordan's bill must still be reviewed and approved by the Ministers' Council, then placed before Parliament. Both Houses of Parliament must debate and pass the act in question before the King rectifies it, and the Jordanian Parliament must amend the law in light of the European GDPR and other new data protection legislation in order to ensure the protection of personal data.

To be sure, a number of additions are required. There is a need to reformulate and improve the bill to soften its lengthy statements, legalize its texts and definitions, and ensure unambiguity and clarity. There is also a need to state the reasons for the bill in accordance with national principles and international standards and link the articles and provisions of the bill to the extent of violations and the amounts of the penalties.

The concepts and terminology contained in the law, such as competent courts, personal data, sensitive data, and right to access, need to be redefined, and the number of references to regulations should be relaxed in the provisions of the law. It should be noted that some of the articles contradict some of the laws and regulations enforced in some bodies, including the Central Bank and general statistics and telecommunications companies-examples include articles

that prevent certain government regulators from obtaining personal data except through the judiciary body.

Also helpful to note is that the law includes some service providers that are forced to comply but are not mentioned in the articles of the law; this requires attention. Important bodies, such as the Department of Criminal Information, Department of General Statistics, and the Central Bank, need to be represented in the composition of the data protection board. In addition, the law should include clauses permitting regulatory bodies in each institution to outline the necessary instructions to implement the provisions of this law; currently, the law includes content that protects personal data in smart applications and social media. Above all, the amended law should provide for the establishment of an independent data authority, such as the National Commission of Information and Liberty in France, with limited powers to supervise personal data processing.

Moreover, the House of Representatives should amend this law to identify all cases where personal data processing permits are required, rather than cite cases where data processing permits are not required, ensuring the protection of the data of citizens and residents. Amendments should also take into account the conditions set out in the GDPR, specifying the choice of data processing officers and their responsibilities and granting those who collect their data the right to refrain from doing so. Institutions, entities, and individuals controlling personal data processing should be required to appoint an official to protect personal data in their institutions and destinations in order to ensure the privacy of individuals' data and the fulfillment of their rights provided for by this law. An appropriate level of legal and technical protection should be ensured for electronically processed personal data. Finally, mechanisms to manage risks resulting from both the use of citizens' personal data and the violation of data privacy should be established.

## CONCLUSION

This analysis of the Jordanian legal framework of data protection reveals that the proposed legislation contains insufficient laws and regulations for data protection and, moreover, that the level of protection currently available in the nation's constitution and existing laws is limited and sectorial. This means that Jordan requires new legislation for data protection to provide adequate protection and comply with the GDPR-to be sure, the new legislation should be drafted with consideration of the GDPR. This article analyzed the important provisions of the GDPR to provide appropriate suggestions on how to improve the new Jordanian data protection laws. Thus, as discussed above, the Draft Law provides many provisions that are similar to those in the GDPR but are applicable only to the residents of Jordan. However, this means that most companies would already have a privacy policy in place, which can now be further developed and extended to include and encompass the stricter regulations of the GDPR to ensure they do not face any penalties for breaches under the GDPR or the new Jordanian legislation.

This Draft Law applies not only to private corporations or corporate bodies, but also to state entities, government agencies, and any other persons acting on their behalf. Under this Draft Law, the definition of *"third party*" includes public authorities as well. While the provisions of the Jordanian Draft Law refer to genetic and medical data, they still lack precision. The suggestions made above on how to improve the Draft Law indicate areas that can be used by researchers to examine data protection in Jordan in the future. Nonetheless, this Draft Law,

which is still pending approval, is much more in line with the GDPR's norms and with minor revisions should be able to achieve its aim of protecting data.

## REFERENCES


Al-Sharieh, S. (2018). Securing the person and protecting the data: The requirement and implementation of privacy by design in law enforcement ICT system. In J.M. Monnici & J. Cannataci (Eds.), *Changing communities, changing policing* (pp. 174-180). NWV, Wieh-Graz.

Data Breaches. (2020). *Privacy rights clearinghouse.* Retrieved from https://privacyrights.org/data-breaches

Determann, L. (2017). *Determann's field guide to data privacy law*. Edward Elgar Publishing, Cheltenham, UK.

Determann, L. (2018). *Less than 20 weeks to the European Union GDPR–what to do now? Blomberg Law.* Retrieved February 20, 2020, from https://news.bloomberglaw.com/e-discovery-and-legal-tech/less-than-20-weeks-to-the-european-union-gdprwhat-to-do-now

Diker, V.A. (2018). The right to data portability in the GDPR: What lessons can be learned from the EU experience? *Journal of Internet Law, 21*(7), 1-11.

Duncan, B. (2019). EU general data protection regulation compliance challenges for cloud users. *Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization,* (pp. 27-28). Venice, Italy.

Erskine-Fox, E. (2020). Biometrics and data protection in financial services. *Global Banking and Finance Review*. Retrieved January 10, 2020, from https://www.globalbankingandfinance.com/biometrics-and-data-protection-in-financial-services/

European Union. (1995). *Directive 95/46/EC of the European Parliament and of the Council of October 24*. On the protection of individuals with regard to the processing of personal data and on the free movement of such data.

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April.* On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

European Union. (2018). *The eleventh meeting of the Jordanian-European association agreement committee*. Retrieved from https://eeas.europa.eu/delegations/jordan/54854/

Faqir, R. (2013). Cybercrimes in Jordan: A legal assessment on the effectiveness of information system crimes law no (30) of 2010. *International Journal of Cyber Criminology, 7*(1), 81-90.

Faqir, R., Sharari, S., & Salameh, S. (2014). Cybercrimes and technical issues under the Jordanian information system crimes law. *Journal of Politics and Law, 7*(2), 94-106.

Gjermundrød, H., Dionysiou, I., & Costa, K. (2016). Privacy tracker: A privacy-by-design GDPR-compliant framework with verifiable data traceability controls. In S. Casteleyn, P. Dolog, & Pautasso C. (Eds.), *Lecture notes in computer science* (pp. 3-15). Springer, Cham, Switzerland.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59*(6), 703-705.

Graham, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report, UNSW Law Research Paper, 45*(1), 1–13.

Hamouri, S., & Almasri, R. (2014). *Data protection act, what we can learn from other countries' experiences.* Retrieved December 3, 2020, from https://7iber.com/wp-content/uploads/2016/01/Reem.pdf

Jones, M., & Ausloos, J. (2013). The right to be forgotten across the pond. 2012 TRPC. *Journal of Information Policy, 3*(1), 1-23.

Jordanian Constitution Law. (1952). *Art. 7, Jordan constitution.* Retrieved December 20, 2019, from http://www.cco.gov.jo/en-us/Jordanian-Constitutional

Jordanian Constitution Law. (1960). *Jordanian Penal Code, JOR-1960-L-79914*. Retrieved January 22, 2020, from www.lob.gouv.jo

Jordanian Constitution Law. (1995). *Jordan telecommunications law No. (13) and its amendments.* Retrieved January 22, 2020 from https://www.wipo.int/edocs/lexdocs/laws/en/jo/jo056en.pdf

Jordanian Constitution Law. (2014). Anti-terrorism Law. Retrieved January 21, 2020, from www.lob.gouv.jo

Jordanian Constitution Law. (2015). *Jordan cybercrimes act.* Retrieved February 2, 2020, from www.lob.gouv.jo

Jordanian Constitution Law. (2015). *Jordan electronic transactions act.* Retrieved February 10, 2020, from

https://www.wipo.int/edocs/lexdocs/laws/en/jo/jo058en.pdf
Jordanian Constitution Law. (2018). *Jordanian consumer protection law*. Retrieved February 15, 2020, from https://www.mit.gov.jo/EchoBusV3.0/SystemAssets/PDFs/AR/Legislation/Other/Laws
Jordanian Constitution Law. (2020). *Jordanian draft law of personal data protection*. Retrieved January 26, 2020, from www.lob.gouv.jo
Joseph, R.C. (2018). Data breaches: Public sector perspectives. *IT Professional, 20*(4), 57-64.
Josserand, C. (2016). Legal nature of biometric data: From generic personal data to sensitive data. *European Data Protection Law Review, 2*(3), 297-311.
Kanimozhi, R. (2019). Adaptive and intelligent framework of data protection techniques for cloud storage. *International Journal of Cloud Computing, 8*(1), 50-67.
Kindt, E. (2007). Biometric applications and the data protection legislation. *Datenschutz und Datensicherheit, 31*(3), 166-170.
Krausová, A. (2018). Biometric data vulnerabilities: Privacy implications. *The Lawyer Quarterly, 8*(3), 295-306.
Lynskey, O. (2017). Aligning data protection rights with competition law remedies? The GDPR right to data portability. *European Law Review, 42*(6), 793-81.
McDermott, Y. (2017). Conceptualizing the right to data protection in an era of Big Data. *Big Data & Society, 4*(1), 1-7.
Onikm, M.H., Kim, C., & Yang, J. (2019). Personal data privacy challenges of the fourth industrial revolution. *Proceedings of 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 635-638). PyeongChang Kwangwoon Do, South Korea.
Privacy International. (2019). *State of privacy*. Retrieved from https://privacyinternational.org/state-privacy/1004/state-privacy-jordan
Reidenberg, J.R. (2000). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review, 52*(5), 1315-1375.
Ross, D. (2017). Processing biometrics data? Be careful under the GDPR. *Privacy Advisor.* Retrieved from https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/
Samaro, D. (2019). *New study: Jordanian ISPs violate customer's privacy.* Retrieved from https://www.accessnow.org/new-study-jordanian-isps-violate-customers-privacy/
Sharbain, R. (2019). *Data protection policy void threatens privacy rights of citizens and refugees in Jordan, government surveillance is a strong threat to privacy in Jordan.* Retrieved from https://advox.globalvoices.org/2019/12/30/data-protection-policy-void-threatens-privacy-rights-of-citizens-and-refugees-in-jordan/
Sokolov, S. (2018). Formation of common legal framework for biometric data security based on contradictions in international legislation. *IOP Conference Series: Earth and Environmental Science, 194*(2), 1-5.
Sprokkereef, A. (2008). Data protection and the use of biometric data in the EU. In S. Fischer-Hübner (Eds.), *The future of identity in the information society* (pp. 277-284). Springer, Boston.
Van-Der-Hof, S., & Lievens, E. (2018). The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. *Communications Law 23*(1), 1-11.
Wolters, P.T.J. (2017). The security of personal data under the GDPR: a harmonized duty or a shared responsibility? *International Data Privacy Law, 7*(3), 165-178.
Zimmerman, H. (2018). The data of you: Regulating private industry's collection of biometric information. *Kansas Law Review, 66*(1), 637-671.