Journal of Politics and Law; Vol. 16, No. 3; 2023
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Personal Data Protection in the Iranian Legal System

Mohammad Mustafa Mohiqi[1]

[1] School of Law, Université Paris-Est Créteil, Paris, France

Correspondence: Mohammad Mustafa Mohiqi, School of Law, Université Paris-Est Créteil, Paris, France. E-mail: mohammad-mustafa.mohiqi@u-pec.fr

Received: January 11, 2023 Accepted: May 4, 2023 Online Published: June 6, 2023

doi:10.5539/jpl.v16n3p10 URL: https://doi.org/10.5539/jpl.v16n3p10

Abstract

Currently, legislators are paying special attention to the personal data of individuals since these data can be processed, transferred quickly and are available in cyberspace. The purpose of this article is to describe the process by which Iran's legal system protects personal information and privacy. There is no specific law in Iran regarding the protection of personal data, and therefore this data should be protected in accordance with other laws. While there is no specific legal sanction in the Iranian legal system for the violation of data privacy, it is not without legal consequences, and for the legal consequences, one can refer to other Iranian laws and foundations. For example, for civil remedies, it is possible to make reference to the Civil Liability Act. Based on the different laws of Iran, it can be seen that in this country, the principle is to safeguard the privacy of the individual. Although the right to privacy may not be violated in all cases, it may be violated in exceptional circumstances, such as when it comes to national security, because in every country, issues such as order and public interest take priority over the rights of individuals.

Keywords: Iran, personal data, personal data protection, privacy

1. Introduction

Technology advancement and virtual space growth have facilitated people's access to the capabilities of virtual space. This issue requires governments to adopt approaches to prevent the invasion of citizens' privacy. In Iran, the privacy and personal data protection issues were considered in a fourth development plan, and the privacy protection bill was also prepared to implement Article 100 of the same plan and submitted to the parliament. Unfortunately, it was subsequently withdrawn by the government in 2015, and subsequent efforts to develop a certain legal system for privacy protection did not succeed (Habibi, 2016).

There are no coherent regulations regarding personal data protection in the Iranian legal system, and the recently formulated plan entitled "Personal Data Protection Plan" has not yet been approved by the parliament. That is why privacy protection should be sought in various regulations, such as the Constitution, Islamic Penal Code, Electronic Commerce Act (2002), and Publication and Free Access to Information Act (2009).

2. Methodology

Since this research examines Iran's legal system with respect to data protection, it is descriptive and analytical in nature. With a focus on Iran's laws, the situation of data protection and privacy has been examined and analysed, and a variety of laws have been reviewed in order to create a comprehensive assessment of the status. Among the regulations contained in this list are the Constitution, the Islamic Penal Code, the Electronic Commerce Law, the Law on Publication and Free Access to Information and the Criminal Procedure Code. Furthermore, to get a better understanding of the future status of personal data protection in Iran, we have examined the personal data protection draft law, which has not yet been approved by parliament, and which is in the process of becoming a law.

Different sections of this research discuss the status of personal data protection and privacy protection under GDPR, so there is a comparative aspect to this study. Research is conducted using a documentary method. This method uses official documents as sources of information and analyses them. The use of documentary research is one of the fundamental principles of humanities and social sciences research (Jashim, 2010).

3. Results

Based on the findings of the current study, Iranian law enforcement officers have demonstrated positive efforts in

protecting personal data. There are, however, no consistent regulations in the legal system of this country in this regard, so personal data is not adequately protected in Iranian law. The protection of privacy is provided by traditional laws, however, personal data requires new laws based on its unique circumstances. Iran has first enacted scattered laws regarding the protection of personal data, and then gradually migrated toward the European approach and drafted a comprehensive data protection law.

4. The Constitution

The right to personal privacy has been emphasised in the Iranian Constitution, which has been emphasised in the International human rights law (IHRL) and the laws of other countries. Although the phrase "privacy" has not been explicitly referred to in the Constitution of the Islamic Republic of Iran, examples of privacy protection can be seen by analysing several of its articles .According to Article 25 of the Constitution, any spying is prohibited, and according to the concept of spying, many cases of invasion of privacy can be seen as spying, which is prohibited. Privacy is one of the most important human rights, as it is emphasised in Articles 14 and 20 of the Constitution to respect the human rights of all people. The word "rights" in Article 22 can also be subject to privacy. This right has been declared inviolable (Vaezi& Alipour, 2012).

In accordance with Article 167 of the Constitution and Article 3 of the Code of Civil Procedure, judges are required to refer to Islamic sources in the absence of a legal provision. As the Qur'an and the Prophet of Islam do not use the term privacy, topics related to privacy should be explored within the context of topics such as the prohibition of spying, the prohibition of divulging confidential information to others, as well as the prohibition of entering another person's home without permission. Surah Noor, verse 27 mentions the importance of obtaining permission before entering another person's home. There are also those who argue in favour of privacy who cite the words of the Prophet Muhammad as evidence. It is stated in the words of Prophet of Islam that you should not search the secret and open activities of others (Montazeri, 1988). As a matter of fact, the Iranian constitution is strongly influenced by the Qur'an and Islam's orders, and by examining several significant principles of this law, it is clear that privacy is of paramount importance.

5. Islamic Penal Code

In Iran, invasion of privacy through information and communication technology is subject to two types of criminal regulations: first, traditional laws that protect the privacy of people in general; including the crime of revealing secrets and secondly, new criminal laws, such as privacy-related those concerning computers, processing systems, and information and communication technology in general.

Iranian legislators have addressed the issue of revealing secrets in Article 648 in the Islamic Penal Code. According to the article, all those who keep secrets in accordance with their job, whenever they reveal the secrets of people other than in legal cases, they will be considered guilty and will be imprisoned from 3 months and one day to one year or from one million hundred thousand million to six million IRR is imposed. According to Article 648 in the Islamic Penal Code, the owners of official government and non-government jobs who communicate with the public in a way are considered guilty and should be punished if they reveal the secrets of the people. According to the legislator, a person who commits the crime of revealing secrets is a person who becomes privy to people's secrets in accordance with his/her job. Because of the trust that people have in him/her, they tell him/her their secrets or because he/she is naturally aware of people's secrets (Pod, 2013). In cases where a person is allowed to disclose secrets, he/she must report it to the competent authorities, and if he/she reports to another person(s), he/she has committed illegal revelation of secrets and will be punished. The person disclosing secrets should limit himself/herself to revealing people's secrets as much as necessary, and if he/she reveals more than that, he/she will be subject to Article 648 .There is a compatibility between article 648 of the Islamic Penal Code and paragraph one of article 90 of the GDPR. In accordance with this article, the member states of the European Union are entitled to establish rules that prohibit controllers or processors from sharing information with supervisory authorities due to professional confidentiality obligations (Voigt & Von Dem Bussche, 2017).

The third chapter in Iran's Islamic Penal Code, entitled "Computer Crimes Law" (2018), deals with privacy and personal data protection. According to Article 1 of the first topic of the law, "Article 729 of the Islamic Penal Code" entitled "Unauthorised Access": Anyone who has unauthorised access to data or computer or telecommunication systems that are under the protection of security measures shall be imprisoned from ninety-one days to one year or a fine from five million to twenty million IRR, or both punishments will be imposed. Any unauthorised access to protected data, whether direct or indirect, is considered a crime under Article 1 of the Computer Crimes Law. It is therefore an absolute crime in Iran's legal system to access other people's information without their consent. Since these crimes are committed only by doing the act without considering its consequences (Etooii, 2021).

According to Article 2 of the law: anyone who illegally listens to the content of non-public communications being

transmitted in computer or telecommunication systems shall be imprisoned from six months to two years or fined from ten million to forty million IRR, or both punishments will be imposed. Eavesdropping means receiving data in transit or accessing them in any way. Non-public communications are personal or private communications, and the general public is unaware of their content (Aghababaie & Ahmadinatur, 2016).

According to Article 17 of the law, violating the principles related to data disclosure and transmission is also considered a crime: anyone who publishes family audio or film or other secrets through computer or telecommunication systems without his consent or makes available to others, in a way that leads to loss or damage to his reputation, he will be sentenced to imprisonment from ninety-one days to two years or a fine from five million to forty million IRR or both punishments. It should be noted that in the drafts of the law, a wide range is defined for examples of personal secrets, but in the text of the law, only sound, image, and film are referred to. From this article, it can be understood that the publisher of the sound, image or film must obtain the consent of the owner of the secrets before publication, and this consent must be obtained at the time of publication or revelation (Mohseni, 2010). This article indicates that consent is the basis for the processing of personal data in Iran. As stated in Article 59 of the Electronic Commerce Law 2012, consent is required for the storage and processing of personal data. The main criticism of this article is that it does not protect privacy absolutely and only protects it when a violation of privacy has caused damage to the data subject. Aside from protecting personal data, the GDPR also refers to compensation. In accordance with paragraph one of Article 82 of GDPR, any person who has suffered material or nonmaterial damage as a result of the violation of these regulations can seek compensation from the controller or processor.

Given the computer crimes law, it can be found that the law, while identifying unauthorised access, theft or seizing of data, asks internet service providers to save and maintain user data for a certain period of time to enable access if needed. However, the explicit subject of the law is not personal data protection (Ansari& Attar, 2021).

6. Electronic Commerce Law

On the one hand, the law defines personal data. On the other hand, it specifies the principles of personal data processing and the rights of data subjects and predicts the data value to prove a lawsuit. By approving the Electronic Commerce Law in 2002, regulations regarding personal data protection in the virtual space and internet environment were considered. The e-commerce law does not specify whether the controller or processor is required to comply with security measures, and failing to mention the conditions under which data may be transferred outside Iran is another deficiency. (Ghannad & Aligholi, 2020). However, GDPR stipulates the conditions for international transfers of personal data in articles 44 to 49, which aim to enhance the protection of personal data. Because data controllers and processors outside of the EU, who are subject to their own laws, may not comply with data protection requirements or may use methods for processing data that violate the fundamental rights of data subjects.

According to Article 58, it is illegal to stave, process, or publish personal data revealing ethnicity, race, ideological, religious views, moral characteristics, or physical, mental, or sexual status of people without their explicit consent. Article 58 deals with the data subject's consent to collect sensitive information related to him/her. In the Iranian legal system and according to the phrase "express consent" used in Article 58 in the Electronic Commerce Law, undoubtedly in the field of sensitive data that Article 58 refers to, consent must be explicited. However, tacit consent is also sufficient regarding other data, including contracts-related data, because, according to Articles 191-193 of the Civil Code, consent is either explicit or implicit (Katouzian, 1997).

In Article 6 of the GDPR, paragraph 1 refers to the requirement of consent in order to process personal data. According to paragraph 1 of article 7 of the same law, the controller must demonstrate that the data subject has consented to the processing of his data. Iran's law also acknowledges this issue, since Islamic jurisprudence adheres to the principle of non-consent (Velai, 2008). Paragraph 11 of Article 4 specifies the characteristics of correct consent, which include free, informed, and unambiguous consent. For companies that engage in e-commerce and for controllers and processors, these characteristics have significant implications. It is recommended that these companies and individuals use more pop-ups and other methods to obtain explicit consent in accordance with GDPR (Custers, Van Der Hof, Schermer, Appleby-Arnold& Brockdorff, 2013). Unlike Iran's law, which considers only explicit consent to be acceptable, the GDPR provides a more comprehensive protection of the individual's rights because it specifies several essential features of valid consent.

It is possible to criticise Article 58 in a number of ways. As a matter of fact, it does not provide any protection for non-personal private information, contrary to Article 669 of the Islamic Penal Code. Moreover, Article 58 of the Electronic Commerce Law refers only to three acts of storing, processing, and distributing sensitive data of others. It does not define unauthorised collection of data as a crime, which is of greater importance than storing, processing,

or distributing data. Therefore, Iranian law does not provide criminal protection for the unauthorised collection of other people's sensitive data, and the controller or processor is not subject to restrictions in this regard (Mohseni, 2010).

Article 59 considers saving, processing, or publishing personal data to be subject to the following conditions: the objectives must be specified and clearly described, the data must be collected only as necessary and appropriate to the objectives described for the data subject during data collection, and used only for certain objectives, the data must be correct and up-to-date, and the data subject must have access to his/her personal data and be able to remove or correct incomplete or incorrect data. The data subject must be able to completely remove his/her data at any time.

The following rights are provided to data subjects in accordance with Article 59: Right to rectification, according to which the data must reflect the truth (Finck, 2018). Right of access (Article 15 of GDPR stipulates that data subjects have the right to access their data). Furthermore, in terms of the right to be forgotten, the data subject has the right to request that his data be deleted immediately pursuant to Article 17 of the GDPR. There are, however, some important rights that are not mentioned, such as transparency. There are two types of transparency: individual transparency and systemic transparency. The concept of individual transparency implies that a person who is affected by an automated decision should be provided with sufficient information regarding the process involved in making the decision. As an example, the loan applicant's request has been rejected. In this situation, the reasons for this decision should be explained in simple language so that the applicant will be able to understand them. In contrast, systemic transparency facilitates the correction of errors or discrimination in both machine and human decision-making processes. Source code for an algorithm may be made available to a panel of experts, for example (Kaminski, 2020). Furthermore, it has been forgotten to pay attention to details. Data collection, for example, is only permitted with the consent of the data subject according to the principle of consent, but the exceptions to this principle are not specifically mentioned in the law, and according to Article 61, the regulations should determine them. If exceptions are specified in a regulation, it can be very risky since the government may easily expand the exceptions and thereby weaken the protection of data subjects' rights.

The punishment for not complying with Articles 58 and 59 is discussed in Articles 71-73 of the act. Anyone who violates the conditions stipulated in Articles 58 and 59 of the acts is a criminal and will be sentenced to one to three years in prison (Article 71 of Electronic Commerce Act). Whenever the responsible institutions commit data-related crimes, they will be sentenced to 3 years in prison (Article 72 of Electronic Commerce Act). If the officials commit crimes related to personal data (messages) due to recklessness and imprudence, they will be sentenced to three months- one year in prison and pay a fine of fifty million IRR(Article 73 of Electronic Commerce Act). Although Iran's e-commerce law provides only for criminal punishment for personal data privacy violations, if there are elements of civil responsibility, the violators may also be sentenced to compensation. According to the Civil Liability Law, the person who intentionally or unintentionally damages material or moral property of others is responsible for compensating those damages. When it comes to the amount of compensation, it should be noted that the amount of compensation will be determined by the court in accordance with the circumstances (Article 3 of the Civil Liability Law). Islamic law contains principles relating to compensation. Accordingly, it appears that the best principle from which compensation can be derived is the principle of preventing harm. As a result of this principle, causing harm to others is prohibited in Islam, and if this harm is caused, the person who caused it must compensate the victim (Naraghi, 1996).

7. Publication and Free Access to Information Act

The Iranian legislator recognised the necessity of freed access to information and finally approved the *Publication and Free Access to Information Act.* The scope of the act is the only access to data or their publication, and it is silent about the personal data collecting and processing (Yaghobi & Soltanifar,2020). Chapter 4 of the act deals with exceptions to access to information, including government secrets, privacy protection, health protection, and commercial and national security information.

According to paragraph B of Article 1 of this law, personal information includes information such as a person's name and surname, address of residence and workplace, family life situation, habits and physical ailments, and bank account number and password. Personal information is not defined in this article, and only examples are provided. A precise definition of personal information can be found in paragraph 1 of article 4 of GDPR. It is defined in this article that personal data are any information relating to an identified or identifiable natural person. It is only natural persons or their legal representatives who may request access to personal information pursuant to Article 6. According to Article 15 of GDPR, data subjects have the right to access their personal information. According to Article 16 of this law, health and business information are also protected. As long as the institutions

subject to this law are aware that providing the requested information would endanger the life or health of the data subject, or would result in financial or commercial harm, they should refrain from providing that information to the data requester. According to GDPR Article 9, the processing of health-related data is prohibited; however, if the processing is necessary to protect the vital interests of the data subject and obtaining his consent is not possible, health-related data may be processed.

8. Approvals of Supreme Council of Cyberspace

Several of the approvals issued by the Supreme Council of Cyberspace refer to the issue of data processing in general and personal data processing in particular. As these approvals constitute the general policy of the Islamic Republic of Iran in the area of cyberspace, they are not directly enforceable, and therefore, a substantial part of them are not observed. (Ansari & Attar, 2021).

8.1 Organising Social Media Messaging Act

The act was approved by the the Supreme Council of Cyberspace in 2016, which refers to the necessity of storing data of Iranian users in internal servers (data localisation). In China, according to Article 1 of the Cybersecurity Act and based on Cyber Sovereignty, cyberspace is a function of the country's interests and values. According to Article 37 of the Cybersecurity Act, operators collecting or generating personal or sensitive data are required to store data in China. Also, data transfer is done only if necessary and after security evaluations (Pernot-Leplay, 2020). In this regard, China has succeeded to some extent. For example, it has been able to oblige the American company "Apple" to establish a local data center. In other words, in 2016, China passed the Cybersecurity Act forcing Apple to store customer data on local servers.

In Iran, according to paragraph 2 of the Organizing Social Media Messaging Act, in order for foreign social media messaging to receive a license to operate, they must store and process data inside the country, and in the process of obtaining a license, it is necessary to should be introduced their authorised legal representative who is a person living in Iran to the Ministry of Communications and Information Technology.

Articles 44 to 49 of the GDPR contain the conditions for international transfers of personal data. These articles were approved by European legislation in order to protect personal data. This is due to the fact that controllers or processors located outside of the European Union may not adequately protect the rights of data subjects (Voigt & Von Dem Bussche, 2017). Among some countries such as Iran and China, the discussion of transferring data abroad has received attention because of security concerns. The transfer of large quantities of personal data abroad may pose a risk to national and social security. It is therefore necessary to store personal data on internal servers. (Ansari, Attar, & Salehi, 2021)

8.2 The Internet of Things Act

On October 22, 2018, in a meeting, the Internet of Things Act entitled "Requirements Governing Internet of Things in the National Information Network" was approved by the Supreme Council of Cyberspace. In this resolution, the role of the Internet of Things in developing society and technology is emphasised. In addition to the necessity of protecting the privacy of people and the necessary measures to maintain the security of users, it has also been emphasised. (Article 2 of Requirements Governing Internet of Things in the National Information Network).

The Internet of Things is extremely vulnerable when it comes to security for several reasons. The first is that most of its components are unsupervised, which makes them easy to attack physically. The second is that most of them use wireless communication, making them vulnerable to eavesdropping. Lastly, it should be noted that the majority of Internet of Things components lack sufficient energy and computing resources - particularly in the case of inactive components - thus preventing the implementation of complex security-oriented designs. (Atzori, Iera, & Morabito, 2010).

9. Supreme Council of the Cultural Revolution Acts

There are a variety of existing laws pertaining to the protection of personal data, including those approved by the Supreme Council of the Cultural Revolution during the 482nd to 488th sessions, which include three regulations. The Internet service providers are prohibited from illegally accessing users' internet activities, disclosing private relationships and violating their privacy, and any unauthorised access to private information centers or any attempt to monitor information passing through the network in accordance with these regulations. Developers of the international contact points and Internet Service Providers are prohibited from collecting, using, or disclosing personal data of subscribers except in accordance with applicable privacy laws.

9.1 International Contact Point Act (2001)

According to paragraph b of Article 6 of the act, all the developers of the international contact point are obliged to

design and implement a firewall proper to protect the network against theft and disclosure of information. The issue of national security is one of the exceptions to privacy protection in the Iranian legal system. According to paragraph c of Article 6 of the act: the developers of the international contact point are obliged to make their internet activity bank available to the Ministry of Communications and Information Technology so that they are available to the Ministry of Information based on the approvals of the Supreme National Security Council and the judge's ruling.

9.2 Internet Service Provider ACT (2001)

According to part 5-3-15, the privacy of users is protected, and any illegal access by the media and any other authorities to the internet activities of users is prohibited. According to paragraphs 6-13, it is forbidden to violate the privacy of people. According to the national security-related exceptions in paragraph 5-3-16, Internet Service Provider is obliged to provide the bank of internet activities of its users to the Ministry of Communication and Information Technology. According to paragraph B-9 of the act, if the Internet Service Provider does not comply with its legal duties and obligations, it will be subject to a warning, temporary suspension of license, or license cancellation. Civil liability-related lawsuits can also be filed in court.

9.3 Internet Service Provider Offices Act (2001)

The Internet Service Provider Offices, are prohibited from violating the privacy of citizens, eavesdropping, and unauthorised access to their private data. The legal duties of Internet Service Provider Offices are determined by this regulation, the most important of which are: paragraphs 15-7: not to disclose private relationships of people,7-19: not to have unauthorised access to centers that have private and confidential information, paragraph 7-21 not to attempt to eavesdrop and check information packages belonging to others. Note 2 deals with the guarantee of the invasion of the discussed acts. First, the official of the office will be warned in writing. The second time, the license of the internet service provider office will be cancelled for one month. The third time, the license will be cancelled for six months; the fourth time, the license will be permanently cancelled, and the private and juridical persons responsible for the office will not be allowed to obtain new licenses throughout the country.

These regulations, while emphasising the privacy of users, have also made violations of that privacy subject to administrative sanctions. Furthermore, these administrative sanctions do not prevent a plaintiff from suing for damages in civil court. In the Iranian legal system, the responsibility of internet service providers is based on the theory of fault, however in some cases the victim does not have to prove fault (Abhari & Miri, 2012). In light of the fact that the Internet is a transnational phenomenon with high speeds of information transfer, internet service providers must take appropriate safety measures to prevent users' privacy from being violated. As a result, if a loss occurs, it is assumed that the internet service provider did not take sufficient safety measures and was careless (Ansari, 2002). While the regulations describe many examples of privacy violations, no criminal punishment is provided for those violations (Ghannad & Aligholi, 2020). For criminal punishment we should refer to Article 648 of the Criminal Penalty Law.

10. Criminal Procedure Act

In the last three decades, the Criminal Procedure Act in Iran, has undergone a general transformation several times. The formulation of new criminal procedures is an example of these improvements. The act was approved by the parliament in 2013 and announced by the president for implementation in 2013, but due to the lack of facilities and conditions, its implementation was postponed to July 2014.

The disclosure of information about individuals related to the case is limited by legal order according to Article 40. It is evident that the information includes personal data. As a result, in Iranian law, it is possible to disclose private personal information and data with a legal order. As a result of Article 23 of GDPR, some of the rights and obligations of data subjects, as well as some of the principles of processing can be limited by the laws of the Union or the country where the controller or processor resides. As long as these limitations respect the individual's fundamental rights and freedoms, they will be acceptable.

According to Article 658 of the Criminal Procedure Law, the judiciary is required to take all necessary technical and legal measures in order to protect the privacy and security of individuals' personal information. According to GDPR Article 32, the controller and processor must take appropriate measures to ensure the security of personal data. Controllers must include in the contract with the processors the obligations necessary to implement Article 32, which are transferred to the sub-processors as well (Finck, 2018).

The examination and recording of data must be proportionate to the detection of crime. Alternatively, if it is necessary to examine a part of the information to discover the crime and identify the accused, the entire information should not be examined and recorded (Article 675 of the Code of Criminal Procedure). It is prohibited to review

documents that are not related to a crime according to Article 8 of the Law on Respecting Legitimate Freedoms and Citizen Rights. Iran's criminal Procedure Law, article 675, outlines the principle of data minimization, which is recognized in GDPR as one of the principles governing data processing. As a consequence of this principle, the controller is responsible for determining how much personal data is required for the processing purposes and must ensure that irrelevant data is not collected. (Kubben& Dumontier, 2019).

According to the enforcement guarantee considered in articles 660 and 661, invasion of data protection is followed by imprisonment or fine and dismissal from service. In general, in Iran's legal system, the legislator has enacted criminal laws and set punishments in order to protect the privacy of its citizens both at work and at home, and does not allow individuals' privacy to be violated except in exceptional circumstances, such as national security. (Tadion, 2009). Specifically, GDPR is composed of three main components, including the obligations of data controllers and processors, the rights of data subjects, and the role of supervisory authorities. In order to ensure the protection of personal data in the European Union, one of the most important components is the proper functioning of independent supervisory authorities in each member state. (Giurgiu & ALarsen, 2016).

The new criminal procedure law of Iran is considered a great revolution in the country's criminal system in such a way that with its innovation, it is considered a significant step to achieving global human rights standards and respecting the principle of respect for private human rights. Despite the innovations and positive aspects that this law brings, some experts do not see it without problems and criticise it. Since government officials or persons under their supervision can easily commit privacy violations, the punishments considered in articles 660 and 661 of this criminal procedure law are not sufficient, and there is a need to consider heavier punishments (Raisi &Ghassemzadehliyasi, 2020). Although the law of criminal procedure is based on the prohibition of checking and recording people's data, except in cases where the legislator allows the checking of personal data. However, the border of the exceptions to checking personal data is not well defined. Also, general terms such as the need to detect a crime have been used, which causes abuse and invasion of the data subject's privacy (Tadaion, 2009).

11. Charter of Citizenship Rights

On December 19, 2016, the Charter of Citizenship Rights was signed by the President. Based on 120 articles included in the charter, the government does its best to protect human rights and a sense of personal and social security. The articles in the Charter of Citizenship Rights are taken from the Constitution and other acts in the Islamic Republic of Iran(Introduction of Charter of Citizenship Rights). The charter is divided into different chapters following the introduction, and there is a mention of the right to privacy in some of the articles.

As outlined in Article 31, the data subject has certain rights, including the right to access and correct information, which is also acknowledged in Articles 15 and 16 of GDPR. According to Articles 35 and 36, citizens are entitled to the protection of their personal data and privacy, and the government must take all necessary measures to protect such data. The controller and the processor must take appropriate measures to ensure the security of personal data according to Article 32 GDPR. According to Article 37, 38, and 39 of the Charter, as well as article 6 of the GDPR, the basic elements of data processing include the consent of the data subject and the legal order.

The most crucial criticism of the charter is what position this charter has in the Iranian internal legal system. According to the investigations and how it was formulated and communicated, the charter cannot be more than an ethical program for the government. As discussed in the introduction of the charter, this is a statement from the president to the nation and specifies the priorities of the government. The next point is that in the Islamic Republic of Iran, the duty of protecting the rights of citizens is the responsibility of the judiciary. The Constitution, in Article 156, considers the judiciary to be the protector of the individual and social rights of the society and introduces this authority responsible for the expansion of justice and legitimate freedoms and monitoring the act enforcement. As a result, the responsibility of guaranteeing citizens' rights is the responsibility of the judiciary.

12. Personal Data Protection Plan

According to paragraph 8 of the Charter of Citizens' Rights entitled "Right of Access to Cyberspace," access to personal data and privacy is the right of citizens. In this regard, the personal data protection plan was announced in the public session on September 15, 2021, of the parliament, but it has not yet been approved. The plan signed by 31 representatives consists of 56 articles and 6 chapters.

Chapter 1 deals with "Generalities," "Project Objectives," and "Definitions". Chapter 2 deals with the rights of data subjects, which includes the key parts, such as consent to the processing, request to process or stop, and performing processing. Chapter 3, which is one of the most important parts of the plan, consists of 24 articles about "Obligations of Controllers and Processors". Chapter 4 deals with the issue of regulating and monitoring personal data processing. Chapter 5 also deals with the issue of responsibilities and enforcement guarantees related

to the plan. Finally, in Chapter 6, according to Article 56, from the date of approval of the act, all laws and regulations contradicting it are terminated.

The main objective of this plan is to eliminate the data-related legal gap. This plan complements the data protection-related acts, including Islamic Penal Code, Electronic Commerce Act, and *Publication and Free Access to Information Act (*Introduction of Personal Data Protection Plan). Another objective of the plan is the protection of data subjects, realised in the following ways: clarifying the rights of data subjects, legalising personal data processing, holding the controllers and processors of personal data accountable, and compensating for damages caused by the personal data processing (Article 1 of Personal Data Protection Plan). According to Article 3, the subjects included in the plan are Iranian citizens whose personal data is processed inside or outside of Iran, as well as foreigners whose personal data is processed by the Iranian controller or processor.

Iran's legal system requires a plan to be approved by the parliament before it can be sent to the Guardian Council. As soon as the plan has been approved by the Guardian Council, signed by the president, and published in the official newspaper, it becomes a law (Mehrpour, 2006). As the Personal Data Protection Plan is far from becoming a law, we will examine some of its most important points in the following sections.

12.1 Rights of Data Subject

According to the plan, the consent of the data subject is a condition for processing personal data. Consent must be obtained before data processing, and it must be possible to attribute the consent to the individual (Article 4 of Personal Data Protection Plan). If the person herself/himself has exposed the data to the public and has not prohibited their processing, it is possible to process personal data related to public situations without the consent of the data subject (Article 5 of Personal Data Protection Plan).

The data subject has the right to request the suspension of part or all of his data processing at any time, provided that the data is incorrect or leads to incorrect results, or the data is processed outside the scope of his consent (Article 6 of Personal Data Protection Plan). The data subject has the right to access his/her data under certain conditions, provided that data does not include important public or personal data of others and does not harm the data reliability (Article 8 of Personal Data Protection Plan).

According to Article 9, a person's consent to personal data processing does not mean revealing his identity. Identity disclosure means unauthorised access to a person's private data, such as name and surname. According to Article 10, personal data processing is permitted in cases without the consent of the individual when it is necessary to protect the life or property of the data subject, for public security, to discover crimes, to protect the life or property of another person or stop them from suffering serious financial loss, from identifying an accused, and enforcement of judicial orders are necessary.

12.2 Regulating and Monitoring the Personal Data Processing

The following authorities are responsible for regulating and monitoring personal data processing: Personal Data Protection Commission, specialised groups and a supervisory council (Article 13 of Personal Data Protection Plan). The Minister of Communications and Information Technology serves as the head of the Personal Data Protection Commission. Other ministers, including the ministry of intelligence and the interior minister, are also commission members (Article 14 of Personal Data Protection Plan). Approving the guidelines needed for personal data protection and resolving disputes between specialised groups is one of the critical duties of the commission (Article 15 of Personal Data Protection Plan).

the specialised groups consists of representatives of government institutions related to data protection in specific issues, including health, banking, social affairs and so on. Within four months, the act for forming these working groups will be approved by the Council of Ministers by order of the Ministry of Communications and Information Technology (Article 19 of Personal Data Protection Plan).

The rules of formation and working approaches of the supervisory council will be approved by the commission. Among the important members of the supervisory council the attorney general as the head of the council and the personal data protection commissioner can be referred to (Article 21 of Personal Data Protection Plan). From the duties of the council, handling complaints about data protection violations and introducing particular supervisors to the commission can be referred to (Article 22 of Personal Data Protection Plan). A special supervisor is chosen in cases such as processing sensitive personal and big data (Article 23 of Personal Data Protection Plan).

12.3 Duties of Controllers and Processors

The controller is the person who determines the objectives, conditions, characteristics, and tools of data processing (Article 2, paragraph 3 of Personal Data Protection Plan). A processor refers to a person whom the controller

chooses for processing (Article 2, paragraph 4 of Personal Data Protection Plan) The entire process of personal data must be according to the documented request of the controller; otherwise, the processor is also known as the processing controller (Article 27 of Personal Data Protection Plan).

The controller or processor is responsible for providing all the facilities and workforce required to monitor the processing. The controller's or processor's agreement with data subjects or others about their monitoring of processing is valid to the extent that it does not conflict with the act (Article 28 of Personal Data Protection Plan). Obtaining permission from a competent authority is a prerequisite and key to processing personal data, even if it is temporary, whether for profit or non-profit. The license does not mean an exemption from other legal requirements, especially obtaining the consent of the data subjects. The personal data controller or processor is exempted from having a license only if they process the personal data of their customers only for the objective of their activity (Article 30 of Personal Data Protection Plan).

The controller or processor is obliged to make data available to data subjects, including the objective of processing, the type and way of processing, the identity and activities of the leading and related controllers or processors, sources of processing, characteristics and technical conditions of processing, licenses received from competent authorities, the security level of processing and its costs, the rights of data subjects regarding the processing of their private data, and the authority they can refer to for complaints. Within one month from the date of receiving personal data, it is necessary for the controller or processor to inform the data subject of this information (Article 33 of Personal Data Protection Plan).

It is necessary for the controller or processor to keep data for 18 months after processing personal data, including log files, data resulting from personal data processing, identity information of data subjects, information on the types of processing performed on the data, the objective of the data processing, and the identity data of the leading and related controllers or processors (Article 40 of Personal Data Protection Plan).

12.4 Enforcement Guarantee

The responsibilities of the controller and the processor are independent, and the injured party can demand compensation for all their losses from the controller and the processor simultaneously. Under certain conditions, the processor is exempted from his/her responsibility, including if the processing is harmful, permission is obtained from the special supervisor (Article 45 of Personal Data Protection Plan).

In case of damage to the data subject, according to the conditions of the injured party and to ensure that no further damage is caused, compensation will be made in ways, such as an apology and help restore the physical, mental, and social position of the victim (Article 48 of Personal Data Protection Plan). Also, the competent judicial authority can fine the perpetrator in accordance with the amount of damage caused (Article 49 of Personal Data Protection Plan). According to the criminal enforcement guarantees of Article 51 of the plan, if personal data is processed without the consent of the data subject, the perpetrator will be sentenced to 5th-degree charges.

13. Conclusion

As a result of GDPR adoption, the European Union has been a pioneer in the field of personal data protection. Article 3 of GDPR outlines the scope of this law, while Article 4 identifies key terms such as personal data processing, controller, and processor. As part of this law, there are principles for processing personal data that must be followed in all processes. Iranian law does not provide detailed information on the protection of personal data, including the scope of this protection. A number of amendments, including personal data processing, controller and processor, which are the most important concepts pertaining to the protection of personal data and the rights of data subjects, have not been defined, and Iranian legal sources do not provide a description of the principles that govern the processing of personal data.

Various rights have been granted to the data subject under GDPR, including the right to data portability, the right to object, and the right not to be subjected to automatic decisions. Iranian e-commerce law does not include any reference to these rights. One of the important topics specified in GDPR is the obligations of controllers and processors. The fourth section of this law contains these obligations. The primary responsibility for processing lies with the controller, in accordance with this section. By researching the basic principles of Iranian law, it is possible to examine these obligations. However, specifying the obligations of processors using this method is extremely general and is not sufficient to protect data subject rights. If the processors do not comply with GDPR's provisions, they will be subject to various legal sanctions. Iran's legal system, however, does not specify the authorities responsible for data protection.

It is imperative that appropriate legislation supports people and their data today, in order for users to be able to take advantage of the benefits of the information technology era without having to fear sharing their personal

information. In Iran, a comprehensive data protection law has not been approved as part of the legal system, which creates a gap in the legal system. There are several laws aimed at protecting privacy, most notably the e-commerce law and the computer crimes law. In spite of their being considered innovations in Iran's legal system, none of these laws provide comprehensive protection for personal data.

The most significant challenge facing Iranian law is the absence of a comprehensive law on personal data protection, which has adversely affected the rights of data subjects. As a result, Iran has attempted to pass regulations regarding personal data protection over the last few years, and one of the latest efforts is the Personal Data Protection Plan. Although this plan has not yet been approved and implemented, it represents a significant change in Iran's legal system in terms of protecting personal data, modelled after GDPR. It is expected that the approval of the personal data protection plan will overcome the lack of explicit regulations and specific instructions.

References

Abhari, H., & Miri, H. (2012). A comparative study of the responsibility of Internet service providers with an emphasis on American and European Union law. *Private Law Research, 1*(1), 20.

Aghababaie, H., & Ahmadinatur, Z. (2016). The comparative study of crimes against privacy in cyberspace in Iran and Germany. *Interdisciplinary Studies in Media and Culture, 11*(6), 12.

Ansari, B., & Attar, S. (2021). Protection of rights in China with a comparative study of America and Europe. *Comparative Law Studies, 25*(13), 110.

Ansari, M. (2002). *Civil responsibility of mass media*. Tehran: Deputy Research and Development of Regulations.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of things: A survey. *Computer Networks, 54*(15). https://doi.org/10.1016/j.comnet.2010.05.010

Charter of Citizenship Rights 2016.

Civil Liability Law 1960.

Custers, B., Van der Hof, S., Schermer, B., Appleby-Arnold, S., & Brockdorff, N. (2013). Informed consent in social media use – The gap between user expectations and EU personal data protection law. *Journal of Law, Technology & Society, 10*(4), 441. https://doi.org/10.2966/scrip.100413.435

Electronic Commerce Law 2002.

Etooii, I. (2021) Initiation of crime in absolute crime. *International Journal of Judicial Research, 3*(2), 556.

Finck, M. (2018). Blockchains and data protection in the European Union. *European Data Protection Law Review, 4*(1), 29. https://doi.org/10.21552/edpl/2018/1/6

General Data Protection Regulation 2016.

Ghannad, F., & Aligholi, A. (2022). The concept and importance of privacy and the types of its protection in cyberspace. *Journal of Modern Laws and Contracts, 1*(1), 317.

Giurgiu, A., & A Larsen, T. (2016). Roles and powers of national data protection authorities. *European Data Protection Law Review, 7*(2), 342. https://doi.org/10.21552/EDPL/2016/3/9

Habibi, H. (2016). The right to privacy in social media. *Legal Research Quarterly,* 75(19), 58.

Jashim, A. U. (2010). Documentary research method: New dimensions. *Indus Journal of Management & Social Science (IJMSS), 4*(1), 2.

Kaminski, M. (2020). *Understanding transparency in algorithmic accountability*. UK: Cambridge University Press. https://doi.org/10.1017/9781108680844.006

Katouzian, A. N. (1997). *Civil law: General rules of contracts*. Tehran: Enteshar Company.

Kubben, P., & Dumontier, M. (2019). *Fundamentals of clinical data science*. https://doi.org/10.1007/978-3-319-99713-1

Mehrpour, H. (2006). Law approval process in Iran's legal system. *Strategy Quarterly, 27*(7), 416.

Mohseni, F. (2010). *Information privacy: A comparative study of the laws of Iran, the United States of America and Imami jurisprudence*. Tehran: Imam Sadegh University Press.

Montazeri, H. (1988). *Lessons from the lslamic state* (2nd ed.). QOM: Thinking Publications.

Naraghi, A. (1996). *The return of days*. QOM: School of Islamic Media.

Pernot-Leplay, E. (2020). China’s approach on data privacy law: A third way between the U.S. and the E.U.? *Penn*

State Journal of Law & International Affairs, 8(1), 104.

Personal Data Protection Plan 2022.

Pod, I. (2013). *Exclusive criminal law*. Tehran: Roham Publications.

Raisi, L., & Ghassemzadehliyasi, F. (2020). The Challenges of the Iranian legal system in violating the personal data and privacy in cyber space. *Judiciarys Law Journal, 110*(30),183.

Tadaion, A. (2009). Respecting the private rights of individuals during evidence collection under the laws of Iran, France and the judicial procedure of the European Court of Human Rights. *Mofid letter, 16*(9), 103.

The internet of things Act 2018.

Vaezi, M., & Alipour, A. (2012). Study of legal rules of privacy and its protect in Iranian legal system. *Private law, 17*(7), 143.

Velai, I. (2008). *Legal terms*. Tehran: Ney Publishing.

Voigt, P., & Von Dem Bussche, A. (2017). *The EU general data protection regulation (GDPR)*. USA: Springer International Publishing. https://doi.org/10.1017/9781108680844.006

Yaghobi, M., & Soltanifar. M. (2020). Explain the challenges of the law of dissemination and free access to information from the perspective of communication and media professors. *New Media Studies, 21*(6), 47.