LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S5(2025)

THE JURIDICAL NATURE OF CONTRACTS FOR THE EXCHANGE OF PERSONAL DATA

Saja Alabboodi[1], Mohammad Bagher Parsapour[2], Morteza shahbazinia[3]

[1]PhD. Student, Department of Private Law, Faculty of Law, Tarbiat Modares University,Tehran, Iran,
[2]Associate Professor; Department of Private Law; Faculty of Law; university of Tarbiat Modares, Tehran; Iran,
[3]Associate Professor; Department of Private Law; Faculty of Law; university of Tarbiat Modares, Tehran; Iran,

saja_laith@modares.ac.ir[1]
parsapour@modares.ac.ir[2]
shahbazinia@modares.ac.ir[3]

Abstract
Personal data such as IP addresses, geolocation details, email accounts, and social media profiles has increasingly come to represent a valuable asset within the global data economy, serving as a driver of innovation and shaping new commercial practices. Businesses often engage in the circulation and commercial use of such data, while individuals frequently provide their information in return for complimentary services, discounts, or reduced costs. This study, conducted through doctrinal legal research and a descriptive–analytical approach, explores the contractual dimension of these practices and their legal implications. Identifying the nature of agreements between data subjects and data controllers is essential for clarifying the scope of rights, duties, and liabilities arising from them. Despite the centrality of this issue, the European Union has not fully articulated a coherent position on the commodification of personal data; although the GDPR safeguards personal data as a fundamental right, many European jurists oppose its treatment as a tradable commodity. In contrast, Iranian law contains no specific statutory provisions on contractual exchange or exploitation of personal data, and legal reasoning must instead rely on general principles of contract law. This divergence underscores the need for a more systematic understanding of personal data contracts and for frameworks that balance the protection of privacy with the facilitation of legitimate economic interests.

Keywords: Personal Data; Sensitive Data; Freedom of Contract; Public Policy; Onerous Contract

Introduction

Today, data is widely recognized as a source of wealth (Gates, 2014, pp. 105–106). Given such significance, any definition of data must be approached with caution, particularly in distinguishing it from related concepts such as information. Various perspectives exist concerning the relationship between data and information. The common element across these views is that data represents the raw material from which information is generated. In other words, data consists of uninterpreted symbols; information is data enriched with meaning; and "knowledge" refers to the ability to ascribe meaning to data in order to derive information (Stepanov, 2020, p. 67).

Different categorizations of data have been proposed (for a comparative overview, see Praveen, 2017, pp. 68–69). From a legal perspective, data may be classified into five distinct categories: **public data[1], personal data[2], metadata[3], mixed data[4], big data[5], and open data[6]**.

[1]. Public data
[2]. Personal data
[3]. Big data
[4]. Mixed data
[5]. Big data
[6]. Open data

In line with the purpose of this research, the **General Data Protection Regulation (GDPR)** of the European Union, in Article 4(1), defines *personal data* as follows:
"Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person."
A similar definition may also be found in the **Electronic Commerce Act of Iran (1382), Definitions section**.
Given that this type of data is today recognized as an economic reality, from a legal perspective it is also possible to inquire into the contractual nature of such relationships. More precisely, the question arises as to what kind of contract we are confronted with in this form of data exchange. However, before addressing this question, jurists have been divided in their opinions regarding the legal nature of personal data itself. In general, two main theories have been advanced. Some scholars are, in absolute terms, in favor of the exploitation of personal data; this group explains their position through a property rights model, considering personal data as part of assets and property (Purtova, 2009, p. 507). Conversely, many others reject the legitimacy of exploiting personal data on the grounds that such data form part of personal rights rather than property rights (see: Scholz, 2016, pp. 1113–1142).
In light of these two theories, the adoption of either approach may lead to different outcomes. Embracing the first approach could render contracts such as sale agreements conceivable, whereas adopting the second approach would make certain types of contracts concerning personal data impossible. In this study, after examining the nature of such data, we will focus more closely on the contractual nature of agreements between data subjects and data controllers an issue that has rarely attracted the attention of legal scholars.

1- Legal Grounds for Processing Personal Data and Their Contractual Basis
In data protection law, a data processor must rely on at least one valid legal ground for the processing of personal data, a requirement commonly referred to as the principle of *lawfulness of processing* (see, generally, Latifzadeh et al., 2023, pp. 157–199). The necessity of having a valid legal basis is established under the principle of lawfulness set forth in Article 5 of the GDPR. Accordingly, if no such legal ground exists, the processing will be unlawful and the principle of lawfulness of personal data will be violated. Among the recognized legal bases are: contractual necessity (Article 6(1)(b) GDPR); processing pursuant to the controller's legal obligation, the performance of a task carried out in the public interest, or the exercise of official authority vested in the controller (Articles 6(1)(c) and (e) GDPR); the protection of vital interests of individuals (Article 6(1)(d) GDPR); and the legitimate interests pursued by the controller or a third party (Article 6(1)(f) GDPR) (see: Latifzadeh et al., 2023, pp. 157–199).
Nevertheless, among these bases, only *consent* may serve as the foundation for the formation of a contract through the concurrence of wills. In the other grounds, since the will of the data subject plays no role in authorizing the processing, no contractual relationship can be said to exist. Article 6(1)(a) GDPR, which requires "the data subject's consent to the processing of his or her personal data for one or more specific purposes," together with Articles 58 and 59 of the Iranian Electronic Commerce Act (2003), expressly addresses this matter.

2. The Legal Nature of Personal Data

In general, property rights and the human rights approach are the two recognized perspectives in contemporary debates on personal data rights. As noted, the adoption of either approach entails specific consequences, particularly with respect to the contractual nature of personal data exchanges. The following sections will address these approaches in turn.

2.1. Approaches to the Legal Nature of Personal Data

2.1.1. The Property Rights Approach to Personal Data

In the United States, it has been argued that the right established over personal data constitutes a form of property right. This approach is grounded on several arguments. One of its main claims is that, by recognizing property rights, individuals would have the opportunity to retain control over their personal data while enjoying various benefits. First, companies that process personal data would be obliged to bear the costs associated with its collection and processing. This would compel companies to be more selective in their collection and processing practices, thereby automatically enhancing the overall level of personal data protection (Prins, 2006, p. 279). Nevertheless, it may also be argued that the opposite effect could occur: recognizing a proprietary right in personal data may increase its economic value, which could in turn encourage companies to process personal data more extensively than before (Id., p. 296).

This approach is not without criticism. One objection is that the economic value of personal data only materializes when such data is assessed in combination with other data. Therefore, determining the precise value of personal data in isolation-solely for the purpose of grounding ownership claims-poses a significant difficulty. At present, it cannot be said that the property rights approach provides a convincing solution to this issue (Zech, 2016, p. 6). Another point that follows from this analysis is that the economic value of personal data is often created by the companies that process it. In other words, in the data economy, the party actively engaged in the use of data is not the individual who provides it. Unlike traditional transactions, where the person supplying the good invests effort in producing it and the other party merely benefits from the result, here it is the data-processing companies that generate value by developing new products or providing targeted advertising to users. Thus, rather than trading in raw personal data, such companies generate income through its processing. Without these activities, personal data cannot be said to possess inherent value. When an individual attempts to sell raw personal data independently, the expected benefits may not materialize, since the actual value is derived through the analytical processes of corporate algorithms. This situation resembles cases in which a person performs operations on another's property or transforms it: if the added value of such labor exceeds the value of the original thing, ownership of the new product belongs to the operator; otherwise, it remains with the original owner. Applying this reasoning to personal data suggests that, although one might initially attribute ownership to the data subject, the functioning of the market may effectively shift ownership to data-processing companies. Clearly, such a conclusion is not what proponents of the property rights approach intended; rather, their aim was to frame personal data rights within the scope of property law (Rochfeld, 2015, pp. 228–229).

To avoid these difficulties, some scholars have sought a middle ground, maintaining a property-based view while avoiding the pitfalls of classical property law. According to this position, the right created over personal data should be regarded as a form of intellectual property right rather than as traditional property. The advantage of this approach is that it recognizes a right over intangible, non-physical assets in the economic sphere while removing the inherent limitations of classical property rights (see: Van Erp, 2019, p. 83).

Nevertheless, criticism has also been directed at drawing analogies between personal data and "works" protected under intellectual property law. The fundamental distinction lies in the qualitative nature of each. Works protected by intellectual property rights arise from the conscious and deliberate creative activity of an author, who is fully aware of the potential consequences of such creation (Cherpillod, 1985, p. 125). By contrast, personal data is not produced through deliberate creative effort; rather, it is often generated passively, without specific intent or substantial effort on the part of the data subject, and frequently without the subject even being aware of its creation (Ibid).

2.1.2. The Personality Rights Approach to the Protection of Personal Data

According to the prevailing view, particularly in European law, an individual's right over his or her data is classified as a *personality right*. Consequently, some scholars argue that the right holder does not possess a corresponding right to economically exploit personal data, as such exploitation would be inconsistent with the very purpose of personality rights. Since the protection of personal data is deemed essential for safeguarding human dignity (Floridi, 2016, pp. 307–312), the possibility of deriving economic benefit from the disclosure of one's personal information is legally precluded.

All rights attributed to the individual are directed toward the preservation of human dignity and the guarantee of material and spiritual development. The high levels of dissatisfaction resulting from technological practices that disregard human dignity underscore the importance of personal data protection. Political history itself bears witness to the suffering inflicted during turbulent periods, when the absence of safeguards for personal data led to profiling, stigmatization, and grave harm to individuals. It is evident that the processing of sensitive categories of data-such as race, religious beliefs, political opinions, philosophical thought, sexual orientation, or health information-without the knowledge of the data subject, without a legal basis, and without granting the individual rights of control and protection, gives rise to discrimination and related harms. Accordingly, the creation of a supervisory society grounded in respect for human dignity becomes a legal and ethical necessity (Floridi, 2016, p. 307). A society in which personal data is left unprotected can only become one of surveillance and oppression.

Viewing personal data primarily as an economic asset leads to practices that erode human dignity (Bormida, 2021, pp. 71–91). Individuals must be protected against both private corporations and public authorities that control vast pools of global data-such as Facebook, Google, and Amazon-especially at a time when data has emerged as the "new capital." Recent scandals concerning massive data breaches by such corporations highlight the urgency of robust personal data protection.

2.2. Comparative Assessment of the Two Approaches

One cannot easily dismiss the criticisms directed at both property rights and intellectual property rights approaches. First and foremost, since our legal system is fundamentally different from the Anglo-American common law tradition, conceiving of personal data merely as a product or commodity is inconsistent with the philosophy of our legal framework. Within the scope of these critiques, it is correct to conclude that personal data should not be viewed exclusively through a "property rights" lens. While elements of this approach may inform part of our analysis, the question of whether the right to personal data protection should instead be characterized as a *fundamental right* or even a *human right* requires further evaluation an approach that is frequently grounded in Article 8 of the Charter of Fundamental Rights of the European Union (Kuner et al., 2020, Forward).

The protection of personal data is enshrined in Article 8 of the Charter, placed alongside Article 7 on "Respect for private and family life." The inclusion of two separate provisions is noteworthy. Given that Article 7 covers a wide range of issues-from private and family life to the inviolability of the home and the confidentiality of communications—the drafters of the Charter sought to ensure that personal data protection would not be subsumed under the broader, and potentially diluted, right to privacy. By explicitly dedicating a separate article to data protection, they intended to establish it as an autonomous fundamental right. Indeed, under EU law, the right to the protection of personal data has been recognized as an independent fundamental right alongside the right to privacy (Ibid., p. 50).

In Iranian law, this approach is also defensible, particularly given the criminal provisions enacted in this area (see the following section). Specific regulations further reflect the legislator's sensitivity towards personal data. Consequently, given that the first approach to the nature of personal data (i.e., property rights) is hardly defensible under current legal frameworks, we adopt here the personality rights approach.

Nevertheless, at this stage, an important point must not be overlooked: although the right to personal data protection has been recognized as a fundamental right, contemporary developments suggest that its protection has, in practice, drifted away from its human rights foundation. Following September 11, a significant shift occurred towards a security- and control-oriented perspective. The private sector has also capitalized on this shift. Moreover, surveillance, control, and tracking of individuals have become inevitable with the constant evolution of new technologies. For these reasons, since the concept of personal data first appeared in the legal framework, many of the original tools and functions have changed, and the foundational principles of data protection have begun to erode. Not only states and their institutions, but also private legal entities now engage extensively in data processing.

Therefore, despite such transformations, personal data must continue to be protected under fundamental rights and freedoms. The importance of such protection becomes evident when considering categories of personal data that may not neatly fall within the scope of human rights yet nevertheless make individuals identifiable. Thus, there exist forms of personal data that may not reach the normative strength of human rights, but still require legal protection.

Finally, based on the foregoing discussion, it should be clear that the right to personal data protection encompasses both public law and private law dimensions. Viewing the right exclusively through a human rights lens as a constitutional entitlement does not preclude its private law dimension. The element of *consent*, explicitly recognized in data protection legislation, illustrates that personal data may also be subject to contractual arrangements. The implications of this point will be elaborated upon in the following section.

3. The Nature of Contracts Concerning the Disposal of Personal Data

3.1. Review of the Literature on the Nature of the Contract

3.1.1. Sale

The first possibility is sale, or a purchase and sale contract. In European law, authors have not explicitly justified considering such contracts as sales, but there are indications of this approach, suggesting that they are regarded as a form of reciprocal or commutative contract, with the contract of sale being the complete example of such contracts. According to jurists, "a commutative contract is an agreement under which one of the parties gives property to the other in return for receiving property. In a commutative contract, there are two counter-performances, each facing

the other. In other words, in such a contract the exchange of property for property is intended, and the exchanges are reciprocal, regardless of whether the property received in exchange is delivered simultaneously or later." By contrast, a gratuitous contract is one under which one party transfers property to the other without receiving anything in return. In other words, what one party gives to the other is given without consideration (Safai, 2018, vol. 2, pp. 40–41).

In fact, as discussed in the general rules of contracts, the first condition for the formation of a contract regarding personal data as mutual obligations is an offer or proposal to enter into such a contract (Civil Code, Article 339). Today, it is widely accepted that an average user of a data-based internet service understands the proposal of "free use" as an offer to exchange their personal data in return for the service or benefit provided. Acceptance of such offers may be explicit or implicit, for example, through the mere use of the service. In Iranian law, it can reasonably be justified that, given the services that process user data, the use of such services may be interpreted as acceptance of the contractual offer to use the service under the applicable terms and conditions. Accordingly, personal data is placed as the "price" in exchange for the service as the "object of sale" - or conversely, which is a less disputed formulation. (This conclusion, however, is premature and will be contested later on.)

In European law, while such an understanding is accepted, it has been contested under the General Data Protection Regulation (GDPR). A specific concern arises with contracts involving personal data as mutual obligations, as stated in Article 7(4) GDPR: "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

At first glance, this rule seems to prohibit contracts that link the consent of the data subject to the provision of a service. According to Article 3(8) of the DSDC Directive, "without prejudice to the protection of individuals with regard to the processing of personal data." Therefore, the DSDC cannot replace the GDPR. The question then arises: is it that no mutual obligations exist in such cases, or can the regulation be interpreted differently?

In interpreting this, one may consider that the wording of Article 7(4) GDPR leaves room for flexibility. The expression "utmost account shall be taken" does not explicitly mean that personal data cannot fall under reciprocal obligations typical of commutative contracts. Rather, this provision may serve as a criterion to assess whether the data subject's consent to join the contract is truly voluntary. In other words, when consent is granted in the framework of a contractual relationship and later disputed, special consideration must be given to whether this consent was given freely or under pressure and compulsion. Different methods can be used to assess whether consumer consent was voluntary. For example, if other providers exist offering similar services, or if the service in question is not essential but recreational, this may help establish voluntariness. Clearly, it would be strange to interpret, for instance, membership in a social network as meaning that the consumer had no choice in joining the contract (Kosta, 2020, pp. 351–352).

This understanding of European law can also be applied to Islamic jurisprudence and Iranian law. The Iranian Civil Code, following Islamic jurisprudence, defines a contract of sale as the transfer of a specific object of legal value in return for something of equivalent value (the price). Thus, the concept of sale in Islamic law also includes exchange - the exchange of one item for another of equal value. A sales contract, after a series of negotiations in which no binding agreement yet exists, comes into being when concluded. At that point, ownership of the goods passes to the buyer, and the seller receives something in return (see Katouzian, 2018, pp. 29–30, 36–37, discussing the

transfer-of-ownership nature of the contract of sale and the two reciprocal performances). If we place services and data opposite each other, we reach the same result: one may be considered the price, the other the object of sale.

But is it really correct to interpret such contracts as sales? The truth is that one cannot so easily equate such contracts with sales contracts as originally defined. On the one hand, the main effect of a sale namely, the transfer of ownership at the time of contract conclusion does not materialize, since the element of alienation from the object of sale or the price after the contract is not fully realized for one of the parties. As discussed regarding the rights of the parties, the rights of the "data subject" persist even after the contract is concluded and over time. For example, the data subject may even request the deletion of their data from the controller's systems. This makes the distinction from a sale contract clear. Therefore, it is necessary to identify another more appropriate contractual category for this situation.

3.1.2. Deposit

Some authors, with a degree of doubt and hesitation, have also raised the possibility of classifying certain instances of data processing as a **deposit**. These writers argue that such a contract, in its nature and in absolute terms, cannot be fully aligned with any of the nominate contracts that create a fiduciary relationship (whether contracts such as deposit, whose primary and inherent purpose is "delegation for safekeeping," or contracts such as lease, where the aspect of protection is merely incidental). Immediately thereafter, however, they introduce a distinction. In their view, one must differentiate between **gratuitous** and **non-gratuitous** processing in cases where the data subject has granted consent. In the latter case (non-gratuitous), the controller's possession of the data is considered a **non-felonious strict liability possession** (Latifzadeh et al., 2023 [Obligations]: 269). In the former case, however-that is, where processing is gratuitous it may be assimilated to a contract of deposit (ibid.: 267).

If we wish to analyze the latter assumption namely, "gratuitousness in the case of consent" it requires an examination of certain preliminaries and their application to the present subject. As this view presupposes, such a conclusion depends upon an analysis that can be drawn from the elements of the **contract of deposit** Accordingly, for an individual's possession of something not to be a liability-bearing possession, certain conditions must be satisfied. In the definition of fiduciary possession , it has been stated:

"Whenever property is delivered by the owner or his legal and lawful representative to another, and authorization is given for him to take possession, without any consideration being envisaged in return, the possessor's holding is considered fiduciary possession. In case of loss without negligence or abuse, he will not be liable." (Mohakek Dammad, 1987, vol. 1, p. 93).

From this definition, it follows that for an individual to be regarded as a trustee (*amīn*) in relation to a subject, two conditions must be observed: (1) authorization of the owner or his legal/lawful representative, and (2) gratuitousness (Khoei, n.d., vol. 30, p. 220; Mohakek Dammad, 1987, vol. 1, p. 94). Therefore, in the absence of either of these two conditions, the individual will not be considered a trustee (ibid., p. 94). For example, the contract of partnership can be cited, in which the recipient is both authorized and the contract is gratuitous.

The fiduciary character and fiduciary possession of the processor may also be inferred from Article 82 GDPR. According to this article:

"…2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing

only where it has not complied with obligations of this Regulation specifically directed to processors, or where it has acted outside or contrary to lawful instructions of the controller. 3. The controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage."

In summary, the processor is not liable so long as he has not committed a fault recognized and defined by law.

Regardless of the objections that may be raised against drawing conclusions from the concept of fiduciary possession, at least in the case of deposit such an inference is valid. According to jurists, Wadi'ah is a contract whereby the owner appoints another person as his agent in safeguarding a specified property (Al-Sistani, 1995, vol. 2, p. 192). In light of this definition, Article 607 of the Iranian Civil Code, in addition to indicating authorization, also explicitly requires gratuitousness of deposit. The fact that the realization of the Wadi'ah contract is dependent on the absence of compensation means that if the trustee imposes a cost upon the owner for protection, he will in fact be the owner's hireling for protection and not a depositary. This implies that the distinguishing line between the contract of deposit and the contract of hire is precisely this-gratuitous safekeeping in the former and compensated protection in the latter.

Although the distinction between deposit and loan for use (Article 635 Civil Code) lies in the permissibility of use and the lack thereof, and thus if the safekeeping of property is combined with the right of use it is in reality a loan for use and not a deposit, it may nevertheless be the case that occasional permission to benefit from the property after the conclusion of the contract does not harm its realization (for example, banks' use of deposit accounts). Article 617 of the Civil Code also points to this: "The trustee may not dispose of the deposit for purposes other than safekeeping, or benefit from it in any way, unless expressly or implicitly authorized by the depositor; otherwise he is liable."

Therefore, it seems that the first assumption advanced by these authors is valid. From their perspective:

"…If processing is gratuitous (such as the processing of personal data by media, social networks, or search engines), the relationship between the data subject and the data processors is fiduciary; because in such cases, authorization by the data subject and gratuitousness for the flow of the fiduciary relationship are present. Furthermore, where data processing takes place by contract, there exists contractual fiduciary possession, and in other cases, where processing is authorized by law, there may exist legal fiduciary possession for example, the processing of personal data for the protection of the vital interests of the data subject or others, or processing for public interest." (Latifzadeh et al., 2023: 266).

The authors ultimately conclude, with hesitation, that the fiduciary nature of data processing cannot be fully assimilated to any specific nominate fiduciary contract, though analogies may be drawn with **deposit**. They argue that if the processor gratuitously safeguards personal data, the relationship resembles that of depositor and trustee. However, this analogy is problematic: processing by social networks or search engines is not truly gratuitous but serves economic purposes, and deposit traditionally applies to property with financial value. Thus, personal data can only be treated as a deposit when it carries clear financial significance for the processor. Consequently, each case must be assessed against the privacy rules set by the processor, and the mere existence of GDPR obligations does not suffice. For a deposit analogy to hold, the platform's core purpose would need to be **gratuitous safekeeping**, which in most modern contexts is unlikely.

3.2. Final Analysis of the Nature of the Contract

As stated, recent attempts to explain and determine the nature of contracts relating to personal data have not been successful. For this purpose, in order to determine the nature of such a contract, the elements and components of such a contract must first be carefully reviewed in light of legal regulations, and then within the framework of these elements its nature may be determined.

3.2.1. Fundamental Elements in the Contract for Processing Personal Data

3.2.1.1. Is this contract binding or non-binding?

The importance of this issue lies in the fact that it determines whether binding or non-binding contracts are excluded, thereby facilitating the identification of the contract's nature. Within the framework of the General Data Protection Regulation (GDPR), as mentioned, under Article 17 GDPR individuals have the right to erase their personal data. However, this right is not absolute and applies only in specific circumstances. For an organization processing personal data, it is necessary to be prepared for the possibility that the data subject may invoke this right. The controller is obliged to respond appropriately to such requests within 30 days (see Recital 59 GDPR).

The cases in which the data subject may invoke the right to erasure, according to Article 17, include: "the disappearance of the purpose of processing, withdrawal of consent and absence of an alternative legal basis for processing, objection to processing, unlawful processing, existence of a legal obligation to erase, data relating to a person who has reached majority."

Under the GDPR, the right to erasure is subject to exceptions where the controller may be required or allowed to retain data. These include: protecting freedom of expression and information, compliance with legal obligations (e.g., company record retention for seven years), public health interests, archiving in the public interest, scientific or historical research or statistical purposes, and the establishment or defense of legal claims.

Therefore, within the GDPR framework, the right to withdraw consent and consequently terminate such an agreement, although provided for, is subject to certain obstacles as mentioned, and these conditions set out in paragraph 3 of that article apply regardless of the basis provided in paragraph 1 (the right to withdraw consent) (Kranenborg, 2020: 483). It is clear that this right may be described as a "conditional right of termination." However, in Iranian law, this right appears to be absolute. According to paragraph (h) of Article 57 of the Electronic Commerce Act (ECA), "the data subject must be able at any time, in compliance with relevant regulations, to request the complete deletion of the computer file containing his or her personal data messages." From this perspective, such a contract, considering Article 5 of the same law ("any change in the production, sending, receipt, storage, or processing of data messages with the specific agreement of the parties shall be valid"), is a non-binding contract for the data subject, who under Article 186 of the Civil Code may revoke it at any time.

Certain nominate contracts that are non-binding are specified in the Civil Code, including the contract of loan for use (A **Loan for Use**, Article 638 Civil Code), the contract of deposit (**Deposit**, Article 611), the contract of agency (***Agency***, Article 678), Profit-Sharing Contract (Article 550), the contract of partnership (Articles 578, 586, and 588), and the contract of *juʿālah* (Article 565). We have previously discussed the contract of deposit. Now, in order to clarify the nature of this contract, such types of contracts may be compared with contracts relating to personal data. For this purpose, in the following section, we provide an analysis based on purpose.

3.2.1.2. Commutative Contract; Exploitation of Data in Return for a Service

Although this issue was raised earlier, here, with a few notes, we conclude the discussion. The second point: exploitation of personal data, in the sense intended here, becomes significant. This exploitation is well known through what we call exchanges, namely the operators of digital platforms that extract value from "user interaction with these platforms." In such a context, data is mainly processed with the aim of targeting individuals in order to provide customized commercial offers or to make consumer profiles available to others. This is particularly the source of income for certain well-known social networks. However, since such a contract is commutative, it differs from similar contracts such as loan for use (Article 635 Civil Code), which presupposes permission to benefit from the property free of charge.

The third point: when such an aspect is emphasized, it should not be assumed that the financial aspect of personal data prevails over their personal aspect. From a legal point of view, the nature of the act of "economic exploitation of personality rights" differs from the "ordinary economic exploitation of property." (Sanhuri, the Egyptian jurist, also proposes such a distinction with respect to intellectual phenomena: Sanhuri, n.d.: 280).

Here too, although the general regime of rules for legal transactions is more or less applicable, such an analysis must conform to the regime of revocability explicitly provided in the Electronic Commerce Act. As we have seen, the Iranian Civil Code allows for the partial and temporary limitation of personality rights, yet the Electronic Commerce Act makes this limitation even narrower, meaning that any voluntary restriction imposed by the data subject is always revocable. Issues such as the non-binding nature of such a contract under the Electronic Commerce Act are analyzed with this personal dimension in mind. As previously discussed regarding Article 975 of the Civil Code, fundamental human rights, while they may be partially restricted by contract, can also be economically exploited; there is in fact no conflict between the two (see, for a similar view: Mirshkari, 2018: 149-174). However, since such a contract always carries a personal dimension, it cannot be entirely assimilated to the traditional financial contracts, and this is precisely why it remains subject to unilateral adjustment by the data subject over time. It is the right of the data subject to require the controller, whenever deemed appropriate, to rectify, restrict, or erase their data from the controller's systems, irrespective of the legal obligations imposed on controllers both by the GDPR and by similar Iranian laws.

This distinctive character of personality rights, as compared with similar financial contracts under the Civil Code, merits stronger emphasis. Reaching conclusions without such emphasis risks overlooking essential realities. What is particularly noteworthy here is the role of **public order** and **mandatory legal rules**. Contracts relating to personal data are also unique in another respect. Contracts that involve matters of public order, mandatory norms, or fundamental freedoms are special because they extend across a very broad field; they are inherently indeterminate, and their scope is defined in practice, case by case, through the claims asserted by the rights-holder.

The most striking examples of these limitations on contractual arrangements concerning personal data are found in relation to **genetic data** and **criminal convictions**. These examples explain why legislators do not approach personal data merely from an economic or financial perspective, and why legislation such as the **Electronic Crimes Act** explicitly criminalizes unauthorized access to personal data. Ultimately, this also means that such contracts cannot be classified under purely financial agreements such as **contracts of sale** or **loan-for-use contracts**, without the need for further elaboration. In reality, the essence and internal structure of personality rights is fundamentally at odds with purely financial contracts.

3.2.2. Personal Data Contracts: Contracts with a Special Nature

In this respect, given the fundamental differences between contracts relating to personal data and the fact that under Iranian law such contracts have not been classified by the legislator within the framework of nominate contracts, they may therefore fall under Article 10 of the Civil Code (Latifzadeh et al., 2023: 267) and be subject to conditions determined both by the parties and, to some extent, by the legislator (such as the GDPR and the Electronic Commerce Act). Clearly, the core principle underlying Article 10 of the Civil Code is the principle of **freedom of will**. On the basis of legal autonomy, which flows from the freedom of will and encompasses the freedom of contract, new contractual frameworks may be created. Within this scope, although subject to the general limits of contractual freedom, the parties may enter into agreements that differ from the nominate contracts codified in the special part of the law of obligations or in specific legislation. Pursuant to the principle of party autonomy, the will of the parties governs both the formation of the contract and the legal relations and effects arising therefrom (Safai, 2018, vol. 2, pp. 55–57). In light of this principle, as derived from Article 10 of the Civil Code, innominate contracts are the product of the concurrence of two independent wills, and their legal effects are precisely those intended by the parties.

This view appears correct insofar as it concerns the validity of the contract, yet it remains open to critique. It must be emphasized that while the content of such contracts is determined by the mutual consent of the parties, the legislator sometimes prescribes special conditions for their validity; for instance, specific obligations imposed on controllers, or restrictions on the rights of data subjects, as seen in the case of genetic data. The domain of personal data has been subject to intense and continuous regulation by legislators and is regarded as a matter of public governance.

Accordingly, contractual freedom in this field is severely restricted. The contracts under consideration acquire a special nature as a result of legislative intervention, and this special nature is deliberately emphasized by the legislator. It is an established fact that the continuation of all daily and social activities, and the realization of common goals, is achieved through contracts; nevertheless, new needs demand new contractual relations. The absence of express provisions in the law covering such new contractual forms has necessitated the creation of **unnamed contracts**, both on a personal and social basis, as a consequence of welfare demands and technological advances. These emerging needs quickly gave rise to new forms of consent, and in this context, innominate contractual relations began to take shape. Over time, the proliferation of such relations led to the emergence of specific innominate contracts and a multitude of unnamed agreements. The examination and regulation of this development led legislators to focus on the functioning of contracts and the balance of underlying interests. A well-known example in this regard is the **insurance contract**.

However, contracts such as insurance are today no longer regarded as unnamed but as nominate contracts that have gradually been recognized by legislators. Nominate contracts are not necessarily limited to those explicitly enumerated in the Civil Code (ibid., p. 45). It is clear that, in most cases, platforms must regularly and systematically communicate their privacy policies to the data subject, who then expresses consent after reading them. Nevertheless, this process is not left entirely to the absolute will of the parties within the framework of Article 10 of the Civil Code, as the legislator prescribes specific conditions for its validity. In this way, both social needs and practical realities are addressed, while ensuring a fair balance between the parties.

Thus, it may be concluded that a new era has emerged in the law of contracts, one in which contracts regulated by legislation, with specific characteristics, prevail.

Conclusion

In conclusion, the proposition that personal data may be subsumed under rights comparable to property ownership is of considerable importance, as it clarifies the standards and requirements that must be met for personal data to be treated as a proprietary right. The resolution of this issue directly affects their tradability. While property law enables goods to be transferred into the ownership of different individuals, there is no comprehensive and exclusive right over personal data that grants the full spectrum of legal uses in the same manner as tangible property. Consequently, any legal analysis must carefully consider the unique characteristics of personal data in order to avoid negative consequences that may result from equating them with ordinary assets.

Accordingly, the personal dimension inherent in personal data must not be overlooked. Both the economic and personal functions of data should be understood holistically, ensuring that neither aspect is sacrificed at the expense of the other. As long as it remains possible to reconcile these two dimensions, there is no justification for abandoning such a balanced approach.

Given that contracts concerning personal data, within the framework of applicable regulations, cannot be reduced to mere property transactions, they cannot be categorized under traditional nominate contracts designed for tangible assets. Instead, such contracts should be recognized as a distinct contractual category governed by their own specific rules and regulatory framework. As long as these conditions remain in force, personal data contracts cannot be forcefully assimilated into classical contractual models.

References:

Persian and Arabic References:

Books:

Mohakek Damad, S. M. (1406 AH). [Jurisprudential Rules] (12th ed., Vol. Tehran: Markaz Nashr ʿUlum-e Islami Publishing.

Khoei, A. M. (n.d.).[Commentary on al-ʿUrwa al-wuthqa] (Vol. 30). Qom: Muʾassasat Ihyaʾ Athar al-Imam al-Khoei.

Al-Sistani, A. (1415 AH). [Path of the Righteous] (Vol. 2). Qom: al-Sistani Publishing Office

Sanhuri, A. A. (n.d.). *The Comprehensive Commentary on Civil Law* (Vol. 8). Beirut.

Safaei, S. H. (2018/1397 SH) [Civil Law: General Rules of Contracts] (30th ed., Vol. 2). Tehran Mizan Publishing.

Articles

Latifzadeh, M., Ghabooli Derafshan, S. M., Mohseni, S., & Abedi, M. (2023). *Obligations of personal data processors in the European Union and the feasibility of their acceptance in Iranian law.***[Teachings of Civil Jurisprudence]**, 15(27), 245–286.

Mirshkari, A. (2018). *The right to image*. **[Private Law Journal]**, 15(1), 149–174.

Laws

Electronic Commerce Act ,(2003/1382 SH). Law adopted by the Islamic Consultative Assembly (Iran).

Civil Code of Iran, (1928/1307 SH, with later amendments)

English References

Books:

Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

Lohsse, S., Schulze, R., & Staudenmayer, D. (2020). Data as counterperformance contract law 2.0? An introduction. In S. Lohsse, R. Schulze, & D. Staudenmayer (Eds.), *Data as counter-performance – Contract law 2.0?* (pp. 9–21). Oxford; Baden-Baden: Hart Publishing; Nomos.

Articles:

Purtova, Nadezhda (2010). "Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation", *European Journal of Legal Studies*, 2(3).

Bormida, M.D. (2021), "The Big Data World: Benefits, Threats and Ethical Challenges", Iphofen, R. and O'Mathúna, D. (Ed.) Ethical Issues in Covert, Security and Surveillance Research (Advances in Research Ethics and Integrity, Vol. 8), Emerald Publishing Limited, Leeds, pp. 71-91.

Metzger, Axel (2017). "Data as Counter-Performance: What Rights and Duties do Parties Have", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8(2).

Purtova, Nadezhda (2009). "Property Rights in Personal Data: Learning from the American Discourse", *Computer Law & Security Review*, 25(6), pp. 507-521.

Gates, Carrie; Matthews, Peter (2014). "Data Is the New Currency", *NSPW: New Security Paradigms and Workshop*, pp. 105-116.

Stepanov, Ivan, (2019). "Introducing a property right over data in the EU: the data producer's right – an evaluation", *International Review of Law, Computers & Technology*, 34(1), pp. 65–86.

Praveen, Shagufta; Chandra, Umesh (2020). "Influence of structured, semi- structured, unstructured data on various data models", *International Journal of Scientific & Engineering Research*, 8(12), pp. 67-69.

Hu, Ying (2021). "Private And Common Property Rights In Personal Data", *Singapore Academy of Law Journal*, pp. 173-201.

Scholz, Lauren Henry (2016). "Privacy as Quasi-Property", *Iowa Law Review*, 101(3), 1113-1141.

Prins, Corien (2006). "Property and Privacy: European Perspectives and the Commodification of our Identity", *Information Law Series*, 16, pp. 229-255.

Zech, Herbert (2016). "A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data", *Journal of Intellectual Property Law & Practice*, 11, pp. 460-470.

Rochfeld, Mme Judith (2015). "Contre l'hypothèse de la qualification des données en tant que biens, in Les biens numériques", *Presses universitaires de France*, pp. 214-228.

Cherpillod, Ivan (1985). L'objet du droit d'auteur, Lausanne: CEDIDAC.

Floridi, Luciano (2016). "On Human Dignity as a Foundation for the Right to Privacy", *Philosophy & Technology*, 29, pp. 307–312.

Laws:

General Data Protection Regulation (GDPR)