

# Validity and Effects of Restrictive Clauses on the Use of User Data in Digital Services Contracts

1. Nasim Parastegari \*: Department of Private Law, Isf.C., Islamic Azad University, Isfahan, Iran

\*Correspondence: nasim.parastegarii1983@gmail.com

## Abstract

Digital transformation has turned digital services contracts into one of the most prevalent legal instruments governing relationships between service providers and users. In these contracts, users typically provide their personal data as consideration to service providers. One of the fundamental challenges in this field is the inclusion of restrictive clauses that limit users' rights with respect to the use, access, transfer, or deletion of personal data. Employing a descriptive-analytical and comparative methodology, this study examines the validity and effects of such clauses in Iranian law and compares them with the approaches adopted in the European Union and the United States. The findings indicate that, despite users' apparent acceptance, restrictive clauses face serious challenges to their validity, as information asymmetry, the complexity of legal language, and the absence of genuine opportunities for negotiation undermine the realization of informed consent. Moreover, these clauses have extensive effects on users' rights, including restrictions on data access and portability, and may lead to reduced competition in digital markets. The results further show that Iran lacks a comprehensive framework for personal data protection, making it necessary to enact comprehensive legislation in this area, amend consumer protection law, and establish transparency requirements in terms of use.

**Keywords:** digital services contracts, restrictive clauses, personal data, consumer rights, privacy

Received: 06 November 2025

Revised: 11 February 2026

Accepted: 18 February 2026

Initial Publication 20 February 2026

Final Publication 01 October 2026



**Copyright:** © 2026 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

**Citation:** Parastegari, N. (2026). Validity and Effects of Restrictive Clauses on the Use of User Data in Digital Services Contracts. *Legal Studies in Digital Age*, 5(4), 1-9.

## 1. Introduction

Digital transformation over recent decades has fundamentally reshaped the landscape of economic and social interactions and has turned digital services contracts into one of the most prevalent legal instruments governing relationships between service providers and users. In these contracts, users typically provide their personal data as consideration instead of monetary payment and, in return, gain access to digital services or content. This new model, grounded in a data-driven economy, raises complex legal questions regarding the nature of this exchange, the validity of contractual clauses, and the protection of user rights. Janmohammadi et al. (2024, p. 231) emphasize that digital content and service supply contracts possess distinctive characteristics that differentiate them from traditional contracts and require a novel legal approach (Janmohammadi et al., 2024). One of the fundamental challenges in this domain is the presence of restrictive clauses that limit users' rights to use, access, transfer, or delete their personal data. These clauses, typically presented in the form of terms of service or privacy

policies, are generally drafted unilaterally by providers and accepted by users without genuine negotiation. Pishnamaz and Rokni (2023, p. 473) have demonstrated that personal data possess significant economic value and that restrictions imposed upon them may inflict irreparable harm on users (Pishnamaz et al., 2023). Mizrahi (2021, p. 490), in his analysis of mobile application user agreements, concludes that many such clauses are designed in ways that deprive users of fundamental rights without providing adequate awareness of the consequences of acceptance (Mizrahi, 2021). Despite the importance of this issue, legal scholarship in Iran has not yet comprehensively and systematically examined the validity and effects of restrictive clauses in digital services contracts. Abulqasem (2023, p. 52) points to legislative gaps in data protection within Iran and argues that the absence of comprehensive and integrated regulations enables service providers to exercise extensive control over user data through contractual clauses (Abulqasem, 2023). Simbar and Nabidoust (2023, p. 138) have also analyzed the criteria for identifying unfairness in contract terms; however, the application of these criteria in the digital environment requires closer scrutiny (Simbar & Nabidoust, 2023). While advanced legal systems, including the European Union, have adopted comprehensive frameworks to protect users through instruments such as the Digital Content Directive and the Digital Markets Act (Nakhjavani, 2023; Wiśniewska & Pałka, 2023), the Iranian legal system still lacks appropriate regulatory mechanisms in this field.

This study seeks to fill this scholarly gap by analyzing the validity and effects of restrictive clauses concerning the use of user data in digital services contracts. The principal research questions are as follows: First, what is the validity of restrictive clauses in digital services contracts under the general rules of contract law and consumer protection law in Iran? Second, what legal effects do such clauses have on users' rights and freedoms? Third, what approaches have different legal systems adopted to protect users against restrictive clauses, and which of these approaches are adaptable to the Iranian legal system? To answer these questions, this research employs a descriptive-analytical and comparative method to examine theoretical foundations, review the relevant literature, and compare the legal approaches of Iran, the European Union, and the United States. The findings contribute not only to the theoretical enrichment of digital contract law but also provide practical recommendations for legislators, judges, and other stakeholders.

## 2. Literature Review

### 2.1. Domestic Scholarship on Digital Contracts and Consumer Protection

Within domestic scholarship, several studies have examined various aspects of digital contracts and consumer rights protection. Janmohammadi et al. (2024), in their article titled "Analysis of the Legal Dimensions of Content and Digital Service Supply Contracts with an Emphasis on Consumer Rights Protection," provide a comprehensive examination of the characteristics of these contracts, their essential elements, conditions of validity, and protective challenges. Their research indicates that existing Iranian laws require revision and supplementation to adequately protect digital consumers and particularly emphasize the importance of transparency in contractual terms and balance in the rights and obligations of the parties (Janmohammadi et al., 2024).

Khanjani (2025), in his study entitled "Civil Liability of Digital Service Providers in Electronic Contracts," analyzes the foundations of contractual and tort liability of digital service providers. He demonstrates that limitation-of-liability clauses commonly incorporated into such contracts cannot override mandatory civil liability rules and that users retain the right to seek remedies in cases of damage (Khanjani, 2025). This research bears direct relevance to the present article, as it shows that the mere inclusion of restrictive clauses cannot entirely absolve providers from liability.

Sajjadi et al. (2025), in their research titled "Concept, Validity, and General Conditions for the Validity of Electronic Contracts in Iranian and UAE Law; A Reflection on Islamic Schools of Jurisprudence," comparatively analyze legal and jurisprudential approaches to the validity of electronic contracts. They demonstrate that although the principle of freedom of contract is recognized, such freedom must not result in the violation of fundamental rights, and clauses contrary to law, public order, or good morals are invalid (Sajjadi et al., 2025). This analysis provides a crucial foundation for assessing the validity of restrictive clauses in digital contracts.

Bahrami and Parvin (2023), in their article on electronic commerce law, examine broader legal challenges and opportunities within electronic commerce and emphasize the necessity of establishing modern legal frameworks to regulate digital relationships (Bahrami & Parvin, 2023). Although their study does not directly address restrictive clauses, it offers a general contextual framework for understanding challenges within electronic commerce law.

### 2.2. Domestic Scholarship on Personal Data and Privacy

Pishnamaz and Rokni (2023), in their study titled “Closure of Virtual Platforms: The Necessity of Analyzing the Regime Governing Personal Data from a Property Law Perspective,” examine the legal nature of personal data and the necessity of recognizing them as protectable property interests. They demonstrate that sudden shutdowns of virtual platforms may result in the loss of valuable user data and severe infringement of user rights. Their research underscores the importance of the rights of access, portability, and erasure and indicates that restrictive clauses limiting these rights may have destructive consequences (Pishnamaz et al., 2023).

Rahbari et al. (2025), in the article “The Status and Application of the Right to Personal Data Portability in the Competition Law of Digital Platforms,” analyze the role of data portability in enhancing competition and reducing the monopolistic power of platforms. They argue that clauses preventing easy data transfer can lead to user lock-in and diminished competition (Rahbari et al., 2025). This research demonstrates that restrictive clauses affect not only individual user rights but also the competitive structure of digital markets.

Farahzadi (2021), in the article “The Right to Exchange Private Data and Solutions to Address Its Challenges in the Mechanism of Internet of Things Devices,” addresses the particular complexities of data collection and processing within the Internet of Things. He demonstrates that in IoT environments, vast amounts of personal data are automatically and continuously collected, while users typically exercise limited control over such processes (Farahzadi, 2021). Restrictive clauses in this context may effectively deprive users of meaningful control over their data.

Abulqasem (2023), in the series “Identifying Legal Gaps in Data Protection within the Data Value Chain: A Comparison of Iranian and US Laws,” provides a comprehensive analysis of existing regulations and legislative gaps in the field of data protection. He demonstrates that Iran lacks a comprehensive and integrated framework for personal data protection, thereby enabling service providers to exert extensive control over data through contractual clauses (Abulqasem, 2023).

Mohsen (2020), in the article “Internet of Things (2): IoT Regulations and Comparison of Laws in the European Union, United States, and China,” offers a comparative analysis of regulatory approaches to IoT and emphasizes the necessity of establishing appropriate protective frameworks for users of such technologies (Mohsen, 2020).

### 2.3. Domestic Scholarship on Unfair Terms and Cloud Computing

Simbar and Nabidoust (2023), in their study titled “Criteria for Identifying Unfairness in Contract Terms,” provide a comprehensive analysis of the standards for identifying unfair clauses in contracts. They propose criteria such as a significant imbalance between the rights and obligations of the parties, inconsistency with the principle of good faith, and the imposition of abnormal or excessive harm as benchmarks for determining unfairness. This research establishes an important theoretical framework for evaluating restrictive clauses in digital contracts and demonstrates that even where there is apparent consent, unfair terms may be subject to invalidation (Simbar & Nabidoust, 2023).

Ansari and Kateb Damghani (2022), in their research entitled “The Legal Regime of Cloud Computing Contracts,” analyze the distinctive characteristics of such contracts and their associated legal challenges. They demonstrate that cloud computing contracts commonly contain standardized, non-negotiable terms that limit providers’ liability and reduce user rights. Their study emphasizes the necessity of balancing the commercial interests of providers with the protection of user rights (Ansari & Kateb Damghani, 2022).

Nakhjavani (2023), in the article “Limitations of Digital Platforms under the EU Digital Markets Act (DMA),” examines the European Union’s regulatory approach to limiting the power of large digital platforms. He demonstrates that the Digital

Markets Act imposes specific restrictions on gatekeeper platforms, which may serve as a model for Iranian lawmakers. This research highlights the importance of regulatory oversight over platform contractual terms (Nakhjavani, 2023).

#### 2.4. *Foreign Scholarship on Digital Contracts and Consumer Protection*

Wiśniewska and Pałka (2023), in their article “The Impact of the Digital Content Directive on Online Platforms’ Terms of Service,” provide a comprehensive analysis of the EU Digital Content Directive and its influence on the modification of major platforms’ terms of service. They demonstrate that the Directive establishes specific requirements regarding transparency, quality, and conformity of digital services and limits the use of unfair terms. Their findings indicate that although platforms have attempted to adjust their conditions to comply with the new requirements, challenges remain in the full implementation of these regulations (Wiśniewska & Pałka, 2023).

de Elizalde (2025), in the article “Fragmenting Consumer Law through Data Protection and Digital Market Regulations,” analyzes the interaction—and at times tension—between various EU instruments, including the GDPR, the DMA, the DSA, and consumer law. She argues that although these legal regimes all aim to protect users, their differing and sometimes inconsistent approaches may generate confusion and regulatory fragmentation. The study underscores the necessity of greater coordination and integration among overlapping regulatory frameworks (de Elizalde, 2025).

Kar and Yu (2024), in their comprehensive article “The Contractual Death and Rebirth of Privacy,” provide a historical and forward-looking analysis of the role of contracts in privacy protection. They argue that the traditional model, which relies exclusively on user consent, has failed in the digital era and must be replaced by a hybrid approach in which contractual mechanisms operate alongside protective regulation. They propose that personal data should be recognized as negotiable assets and that users should be empowered to determine the conditions governing their use (Kar & Yu, 2024).

#### 2.5. *Foreign Scholarship on Privacy and Data Protection Law*

Davis and Marotta-Wurgler (2024), in their twin studies titled “Filling the Void: How EU Privacy Law Spills Over to the US,” examine the extraterritorial effects of the GDPR on the privacy policies of US companies. Through empirical analysis, they demonstrate that many US firms not formally subject to the GDPR have nevertheless adopted similar privacy policies due to market pressures and competitive dynamics. Their research indicates that strong data protection laws can elevate global privacy standards (Davis & Marotta-Wurgler, 2024; Marotta-Wurgler & Davis, 2024).

Slate et al. (2025), in their innovative research “Iterative Contextual Consent: AI-enabled Data Privacy Contracts,” propose a new model for obtaining user consent through artificial intelligence technologies. Rather than relying on a one-time, blanket consent at the outset of the contract, they suggest that AI systems can request consent in real time and in context, thereby enhancing user awareness and meaningful control over personal data (Slate et al., 2025).

Mizrahi (2021), in the article “Risky Fine Print: A Novel Typology of Ethical Risks in Mobile App User Agreements,” provides a comprehensive analysis of risks embedded in mobile application terms of service. He introduces a new typology of ethical risks, including privacy violations, unfair restrictions, unilateral disclaimers, and imbalanced clauses. His research demonstrates that many user agreements contain provisions that effectively deprive users of fundamental rights (Mizrahi, 2021).

These strands of scholarship demonstrate that restrictive clauses in digital services contracts have been examined from multiple perspectives. Nevertheless, the present article, by focusing specifically on the validity and legal effects of such clauses under Iranian law and adopting a comparative approach, seeks to fill the existing gap in this field and to offer practical solutions for enhancing the protection of user rights.

### 3. **Research Methodology**

The research method adopted in this article is descriptive–analytical and comparative, employing a legal approach to examine the validity and effects of restrictive clauses concerning the use of user data in digital services contracts. In terms of its nature, this study may be classified as fundamental–applied research, as it aims to achieve a deeper understanding of

theoretical foundations while also proposing practical solutions for protecting user rights. Data collection has been conducted through library-based and documentary research. The primary sources include scholarly articles published in reputable domestic journals as well as leading international journals, including the *Yearbook of European Law*, the *Journal of Consumer Policy*, and the *Harvard Journal of Law & Technology*. Persian-language sources address the most recent findings concerning the legal status of digital contracts within the Iranian legal system, while English-language sources focus on the analysis of European Union regulations and legal approaches in the United States, thereby enabling a comprehensive comparative assessment.

## 4. Findings

### 4.1. *Concept and Nature of Digital Services Contracts*

Digital services contracts, as one of the most significant legal instruments in the era of digital transformation, provide a framework through which service providers and users exchange economic and informational value. These contracts constitute agreements whereby one party undertakes to provide digital services or content, and the other party, in return, typically provides personal data or pays monetary consideration. Digital content and service supply contracts possess distinctive characteristics that differentiate them from traditional contracts, including the intangible nature of the subject matter, the unlimited reproducibility of digital content, and the central importance of user data within providers' business models (Jannohammadi et al., 2024).

Within the Iranian legal framework, the nature of these contracts remains subject to debate. Electronic contracts must satisfy the general conditions of contractual validity, including intention, capacity, a determinate and lawful subject matter, and a lawful purpose. However, adapting these traditional elements to the digital environment presents particular challenges. Especially where the contractual subject matter consists of personal data, significant questions arise concerning ownership, transferability, and valuation of such data (Sajjadi et al., 2025).

Electronic commerce law, due to the complexities arising from the digital nature of transactions, requires a novel legal approach that fully accounts for these characteristics. In this context, one of the fundamental prerequisites for analyzing electronic contracts is recognizing data as valuable and tradable assets (Bahrami & Parvin, 2023). Moreover, within the European Union, the Digital Content Directive has significantly influenced the terms of service of online platforms and has emphasized the importance of transparency and clarity in defining the rights and obligations of the parties (Wiśniewska & Pałka, 2023).

### 4.2. *Personal Data as Consideration in Digital Contracts*

One of the foundational issues in analyzing digital services contracts concerns the status of users' personal data as contractual consideration. In many digital business models, users provide personal data instead of monetary payment. This model, often described as the "data-driven economy," raises profound questions regarding the legal nature of such exchanges. In examining the closure of virtual platforms and the necessity of analyzing the legal regime governing personal data from a property law perspective, personal data are shown to possess significant economic value, and their deletion or loss may cause irreparable harm to users (Pishnamaz et al., 2023).

Recognizing the right to data portability as a fundamental user right may contribute to increasing competition in digital markets and reducing the monopolistic power of dominant platforms. This approach illustrates that data are not only economically valuable but also function as instruments for strengthening user autonomy and independence (Rahbari et al., 2025).

Various EU instruments, including the GDPR, the DMA, and the DSA, have adopted differing approaches toward personal data, which at times may result in tension or lack of coordination (de Elizalde, 2025). By contrast, personal data should be recognized as negotiable assets over which users may determine the conditions of use, rather than being protected solely through mandatory statutory safeguards (Kar & Yu, 2024).

#### 4.3. *Restrictive Clauses and Their Legal Nature*

Restrictive clauses in digital services contracts refer to provisions that limit users' rights to use, access, transfer, or delete their personal data. These clauses are typically presented in the form of terms of service or privacy policies and are often accepted by users without any genuine opportunity for negotiation. A clause is considered unfair when, without justified reason, it disrupts the reasonable balance between the rights and obligations of the parties and conflicts with the principle of good faith (Simbar & Nabidoust, 2023).

Limitation-of-liability clauses unilaterally drafted by service providers cannot preclude the application of mandatory civil liability rules. This argument demonstrates that even where users have apparently accepted such terms, certain inherent limitations exist regarding their validity (Khanjani, 2025).

In the analysis of mobile application user agreements, many clauses are structured in a manner that deprives users of their fundamental rights without ensuring that they possess adequate awareness of the consequences of acceptance (Mizrahi, 2021). Moreover, the European legislator has attempted to prevent the imposition of imbalanced and unfair terms by introducing regulatory constraints on powerful digital platforms (Nakhjavani, 2023).

#### 4.4. *Validity of Restrictive Clauses in the Iranian Legal System*

The validity of restrictive clauses under Iranian law must be evaluated in light of the general principles of contract law and the governing rules applicable to consumer–service provider relationships. Iranian civil law emphasizes freedom of contract and the binding force of agreements; however, this freedom is not absolute. Where a contractual term contradicts statutory law, public order, or good morals, it is deemed invalid. In the analysis of the general validity conditions of electronic contracts, a clause must be lawful and cannot result in the deprivation of fundamental individual rights (Sajjadi et al., 2025).

The Consumer Protection Law of 2009 and its subsequent amendments provide mechanisms for supervising unfair contractual terms. Under this framework, clauses that create a significant imbalance between the rights and obligations of the parties may be annulled. Nevertheless, applying these rules within the digital environment requires more precise interpretation and contextual adaptation (Janmohammadi et al., 2024).

Standard terms in cloud computing contracts, typically drafted by large providers, often contain extensive limitations that minimize provider liability. Assessing the validity of such clauses necessitates a case-by-case evaluation and careful consideration of the specific circumstances of each contract (Ansari & Kateb Damghani, 2022).

#### 4.5. *Legal Effects of Restrictive Clauses on User Rights*

Restrictive clauses concerning the use of user data produce wide-ranging effects on individual rights and freedoms. One of the most significant consequences is the restriction of the right of access to data. Users may be unable to easily access, download, or transfer their data to other services. This not only reduces individual control over personal information but may also result in user lock-in and diminished competition within the market. The inability to transfer data constitutes one of the principal barriers to competition in digital markets (Rahbari et al., 2025).

In the context of the right to exchange private data and the challenges associated with Internet of Things mechanisms, the complexities arising from the automatic and continuous collection of data by smart devices are particularly significant. Within such environments, restrictive clauses may be designed in ways that effectively deprive users of meaningful control over the data generated by their own devices (Farahzadi, 2021). The necessity of establishing clear legal frameworks to safeguard user rights in this domain is undeniable (Mohsen, 2020).

One of the most critical challenges is the absence of a comprehensive and integrated regulatory framework governing the data lifecycle from collection to deletion. In the absence of such a framework, service providers may, through restrictive clauses, obtain complete control over data and deprive users of their fundamental rights (Abulqasem, 2023).

Even in the absence of comprehensive federal legislation, US companies have altered their privacy policies under the influence of the GDPR. This demonstrates that strong data protection laws can produce extraterritorial effects and elevate global standards (Davis & Marotta-Wurgler, 2024; Marotta-Wurgler & Davis, 2024).

#### 4.6. *User Consent and the Problem of Information Asymmetry*

One of the central issues in evaluating the validity of restrictive clauses concerns the authenticity of user consent. In many cases, users accept terms by clicking “I agree” without fully reading the conditions. This phenomenon, commonly referred to as “clickwrap agreements,” raises serious concerns regarding the validity of consent. The use of artificial intelligence technologies may facilitate the creation of dynamic and contextual consent systems, in which users are prompted in real time and in context to make more informed decisions (Slate et al., 2025).

Information asymmetry between service providers and users constitutes another fundamental challenge. Users typically lack sufficient awareness of the technical complexities of data processing, the extent of data collection, and the manner of its use. This asymmetry means that even where users read the terms, they may not fully comprehend the practical implications of their acceptance (Janmohammadi et al., 2024). Under such circumstances, user consent alone cannot serve as a sufficient criterion for validating restrictive clauses, and more objective standards for assessing fairness are required (Simbar & Nabidoust, 2023).

Excessive length of user agreements, complex legal language, and lack of transparency regarding consequences all impede informed consent. Accordingly, legal requirements should be introduced to mandate the summarization of terms in plain language and the highlighting of key provisions (Mizrahi, 2021).

#### 4.7. *Protective Approaches in Comparative Law*

Different legal systems have adopted varying approaches to protecting users against restrictive clauses. The European Union, through the adoption of the Digital Content Directive, the Digital Markets Act, and the Digital Services Act, has established a comprehensive framework governing these relationships. The Digital Content Directive imposes requirements regarding transparency, quality, and conformity of services and restricts unfair terms. Notably, it explicitly recognizes personal data as consideration in digital contracts (Wiśniewska & Pałka, 2023).

The EU Digital Markets Act imposes specific limitations on gatekeeper platforms, including prohibitions on combining personal data without explicit consent, obligations to ensure data portability, and prohibitions against user lock-in (Nakhjavani, 2023). Although this multi-layered EU approach increases regulatory complexity, it provides more comprehensive protection for users (de Elizalde, 2025).

In the United States, a sectoral and state-based approach predominates. State privacy laws such as the CCPA and CPRA in California provide rights similar to those under the GDPR for residents of those states; however, at the national level, the absence of a comprehensive federal law remains a significant challenge (Davis & Marotta-Wurgler, 2024; Marotta-Wurgler & Davis, 2024). The future of privacy protection in the United States depends on achieving a balance between contractual mechanisms and regulatory safeguards (Kar & Yu, 2024).

A comparison between Iranian and US law reveals gaps within both systems, and Iran requires the enactment of comprehensive personal data protection legislation capable of addressing the challenges of the digital era (Abulqasem, 2023).

## 5. **Conclusion**

This study was conducted with the objective of analyzing the validity and legal effects of restrictive clauses governing the use of user data in digital services contracts, addressing complex legal challenges situated at the intersection of contract law, consumer protection, and data privacy. The findings demonstrate that, despite their apparent acceptance by users, restrictive clauses in digital services contracts face serious challenges concerning their legal validity and exert extensive effects on users’ rights and freedoms.

The theoretical analysis revealed that digital services contracts possess a nature distinct from that of traditional contracts. As emphasized by Janmohammadi et al. (2024) and Sajjadi et al. (2025), adapting the general elements of contractual validity to the digital environment presents particular difficulties, especially with respect to the subject matter of the contract, which often consists of users' personal data (Janmohammadi et al., 2024; Sajjadi et al., 2025). Recognizing personal data as economically valuable and tradable assets constitutes one of the central findings of this research, a conclusion likewise supported by Pishnamaz and Rokni (2023) and Rahbari et al. (2025) (Pishnamaz et al., 2023; Rahbari et al., 2025).

With respect to the validity of restrictive clauses, the research indicates that such provisions cannot enjoy absolute and unrestricted validity under Iranian law. According to general principles of contract law, clauses that contravene statutory law, public order, or good morals are invalid. Furthermore, as Simbar and Nabidoust (2023) argue, clauses that, without justified reason, disrupt the reasonable balance between the parties' rights and obligations and conflict with good faith are considered unfair and subject to annulment (Simbar & Nabidoust, 2023). This issue is particularly significant in digital contracts, where users lack genuine bargaining power and meaningful opportunities to negotiate contractual terms.

One of the most significant findings of this research concerns the issue of genuine user consent. The analysis demonstrates that apparent consent obtained through clickwrap agreements cannot serve as a sufficient basis for validating restrictive clauses. Information asymmetry between service providers and users, the complexity of legal language, and the excessive length of terms of service collectively undermine the possibility of informed consent. Mizrahi (2021) and Slate et al. (2025) propose measures such as simplifying contractual language and implementing AI-based contextual consent systems to mitigate these challenges (Mizrahi, 2021; Slate et al., 2025).

The legal effects of restrictive clauses on user rights are broad and multidimensional. Limitations on the right of access to data, the inability to easily transfer data to competing services, and unilateral provider control over user data constitute some of the most significant consequences. Rahbari et al. (2025) demonstrate that such limitations not only impair individual user rights but also negatively affect market competition by facilitating user lock-in and reducing competitive dynamics (Rahbari et al., 2025). This finding underscores the importance of adopting an approach that extends beyond individual protection and takes into account broader competitive and macroeconomic dimensions.

The comparative analysis of different legal approaches reveals that the European Union has established a comprehensive and advanced regulatory framework through instruments such as the Digital Content Directive, the Digital Markets Act, and the Digital Services Act. Wiśniewska and Pałka (2023) and Nakhjavani (2023) show that these regulations impose specific obligations regarding transparency, limitations on unfair terms, and the safeguarding of fundamental user rights, including data portability (Nakhjavani, 2023; Wiśniewska & Pałka, 2023). By contrast, Iran lacks a comprehensive and integrated framework for personal data protection, a gap identified as one of the most significant legislative deficiencies by Abulqasem (2023) (Abulqasem, 2023).

Based on the findings of this study, several recommendations may be proposed to improve the legal framework in Iran. First, the enactment of a comprehensive personal data protection law that explicitly recognizes and guarantees fundamental user rights, including the rights of access, rectification, erasure, and data portability. Second, the amendment of consumer protection legislation to explicitly address digital services contracts and to clearly define unfair terms in this context. Third, the introduction of statutory transparency requirements in terms of use, including obligations to provide concise and plain-language summaries of key contractual provisions. Fourth, strengthening the role of regulatory and judicial bodies in reviewing and invalidating unfair contractual clauses.

This study was subject to certain limitations that should be considered when interpreting its findings. The analysis was conducted solely on the basis of documentary sources and did not include empirical field research. Moreover, given the rapid pace of technological developments in the digital domain, some findings may require periodic updating. Future research may focus on empirical studies of user and provider behavior, analysis of judicial practice in disputes arising from digital contracts, and evaluation of the practical effectiveness of European Union regulations.

Ultimately, this research demonstrates that effective protection of user rights against restrictive clauses requires a multidimensional approach combining legislative reform, strengthened regulatory oversight, enhanced public awareness, and the responsible deployment of emerging technologies. Achieving a balance between the commercial interests of service providers and the fundamental rights of users remains the key to sustainable and equitable governance in the digital era.

## Ethical Considerations

All procedures performed in this study were under the ethical standards.

## Acknowledgments

Authors thank all who helped us through this study.

## Conflict of Interest

The authors report no conflict of interest.

## Funding/Financial Support

According to the authors, this article has no financial support.

## References

- Abulqasem, R. (2023). *Identifying legal gaps in data protection within the data value chain: A comparison of Iranian and US laws (No. 2): Constitution, federal, and state laws.*
- Ansari, B., & Kateb Damghani, M. M. (2022). *The legal regime of cloud computing contracts.*
- Bahrami, & Parvin. (2023). Electronic commerce law. 8th International and National Conference on Management, Accounting, and Law Studies,
- Davis, K. E., & Marotta-Wurgler, F. (2024). Filling the Void: How EU Privacy Law Spills Over to the US. *Journal of Law & Empirical Analysis*, 1(1), 77-97. <https://doi.org/10.2139/ssrn.4733036>
- de Elizalde, F. (2025). Fragmenting consumer law through data protection and digital market regulations: The DMA, the DSA, the GDPR, and EU Consumer Law. *Journal of Consumer Policy*, 1-35. <https://doi.org/10.1007/s10603-025-09584-3>
- Farahzadi. (2021). The right to exchange private data and solutions to address its challenges in the mechanism of Internet of Things (IoT) devices. *Business Reviews*, 19(109), 115-129.
- Janmohammadi, J., Janmohammadi, & Hosseini. (2024). Analysis of the legal dimensions of content and digital service supply contracts with an emphasis on consumer rights protection. *Majlis and Rahbord*, 31(118), 229-258.
- Kar, R. B., & Yu, X. (2024). The Contractual Death and Rebirth of Privacy. *Harvard Journal of Law & Technology*, 38. <https://doi.org/10.2139/ssrn.4939708>
- Khanjani, M. K. (2025). *Civil liability of digital service providers in electronic contracts.*
- Marotta-Wurgler, F., & Davis, K. E. (2024). Filling the Void: How EU Privacy Law Spills Over to the US. *NYU Law and Economics Research Paper*, 24-15. <https://doi.org/10.2139/ssrn.4733036>
- Mizrahi, B. F. (2021). Risky fine print: A novel typology of ethical risks in mobile app user agreements. *Villanova Law Review*, 66, 483.
- Mohsen, B. (2020). *Internet of Things (2): IoT regulations and comparison of laws in the European Union, United States, and China.*
- Nakhjavani. (2023). Limitations of digital platforms in the EU Digital Markets Act (DMA). *Legal Research*(e164158).
- Pishnamaz, S. A., Rokni, & Amir, A. (2023). Closure of virtual platforms: The necessity of analyzing the regime governing personal data from a property law perspective. *Legal Research*, 22(53), 469-506.
- Rahbari, Masoudi, T., & Arian. (2025). The status and application of the right to personal data portability in the competition law of digital platforms. *Legal Studies*.
- Sajjadi, K., Khoieini, Ghafour, & Salehifar. (2025). Concept, validity, and general conditions for the validity of electronic contracts in Iranian and UAE law; A reflection on Islamic schools of jurisprudence. *Journal of Islamic Law Research*.
- Simbar, & Nabidoust, D. (2023). Criteria for identifying unfairness in contract terms. *Legal Research Quarterly*, 26(103), 135-156.
- Slate, D. D., Chen, C., Yao, Y., & Li, T. J. J. (2025). Iterative Contextual Consent: AI-enabled Data Privacy Contracts. Proceedings of the 2025 Workshop on Human-Centered AI Privacy and Security,
- Wiśniewska, K., & Pałka, P. (2023). The impact of the Digital Content Directive on online platforms' Terms of Service. *Yearbook of European Law*, 42, 388-406. <https://doi.org/10.1093/yel/yead004>