Legal Challenges of User Rights in Cyberspace in the Context of Personal Data Protection

1. Mohsen Mastery Farahani: PhD Student, Department of Private Law, Sari Branch, Islamic Azad University, Mazandaran, Iran

***Correspondence: e-mail:**

Abstract

Cyberspace, like other communication platforms, has specific characteristics and a set of regulations that govern it, subjecting individuals to international laws in certain cases and potentially leading to the violation of user rights. Given the significance of this issue, the present study aims to examine user rights in cyberspace and analyze the legal challenges and requirements related to the protection of users' personal data. The research follows a descriptive-analytical method. According to the findings, data protection regulations, emphasizing the necessity of safeguarding the privacy of data subjects, have established a set of mandatory rules for software owners and personal data processors. If an individual or an organization intentionally or unintentionally violates a user's rights, they must accept liability for compensating the damages. Regarding online messaging applications, civil liability may encompass responsibility for the content published by users, breaches of privacy, or non-compliance with data protection regulations. However, due to the lack of updates, ambiguity, lack of specificity, insufficiency of related laws, and disproportionate treatment compared to traditional offenses, legal regulations gradually lose their effectiveness. In many cases, such as the protection of privacy rights concerning users' personal data—which holds substantial importance—these regulations appear inadequate.

Keywords: User rights, cyberspace, legal requirements, data protection, privacy.

Received: 12 May 2024
Revised: 06 June 2024
Accepted: 18 June 2024
Published: 01 July 2024

Citation: Mastery Farahani, M. (2024). Legal Challenges of User Rights in Cyberspace in the Context of Personal Data Protection. *Legal Studies in Digital Age*, 3(3), 38-45.

1. Introduction

With the advent of the Information Age in the late twentieth century and the advancement of modern technologies, virtual messaging applications emerged as a communication platform between service providers and consumers, experiencing significant expansion. Virtual messaging applications provide a range of services to end-users free of charge; in return, they collect users' data, including personal data, after obtaining their consent and utilize and process such data for predefined purposes (Safarzadeh Roodsari, 2017).

The use of virtual messaging applications necessitates the dominance of software owners over a considerable portion of users' personal data. Under the European Union's personal data protection regulations, every messaging application presents a privacy policy agreement to users upon registration, and upon acceptance, an adhesion contract is formed. This contract is considered an adhesion contract because the user, in order to benefit from the messaging application's services, must accept its terms without making significant modifications to the agreement's provisions. In this process, the user voluntarily provides

some personal information, such as their first and last name, mobile number, email address, username, and password, to the messaging applications. Additionally, certain personal data is recorded and stored through observation, such as the user's location data during phone calls. Other data is inferred or extracted from existing data, such as a person's creditworthiness determined by analyzing financial history. For example, Google's privacy policy illustratively mentions some of the data collected, including the language used, visited pages, posted comments, liked content, emails, shared content, as well as the device's operating system, active software, software updates, device IP address, Wi-Fi access points, active Bluetooth devices, mobile network operator, telecommunications provider, browsing history, and location (Attarzadeh & Ansari, 2020).

Information security pertains to the protection of users' personal data, which includes private information, commercial transactions, financial transactions, personal communications, place of residence, and physical conditions of individuals. Cyberspace conceals the identity and location of actors, enabling them to use fake names and proxies that are difficult to penetrate and reveal. Furthermore, cyberspace has significantly increased the speed, volume, and scope of communications not only for powerful countries and organizations but also for ordinary citizens. Cyberspace is vast and boundless, legally ambiguous, concise in language, and generally complex and elusive. It should be regarded as the fifth domain alongside traditional domains of land, air, sea, and space (Peltier, 2016).

Like other fundamental aspects of life, cyberspace and information technology have always aimed to facilitate better interaction and communication. Cyberspace, like other communication platforms, possesses specific characteristics and regulations. However, it is crucial to recognize that entering cyberspace equates to entering an international environment, where individuals may be subject to international laws, potentially facing liability or harm. The subject of internet rights emerged with the widespread use of the internet, expanding as the number of users grew (Ghamami et al., 2022, p. 88). Given the significance of this issue, the present study seeks to analyze user rights in cyberspace by examining the legal challenges and requirements necessary for protecting users' personal data.

2. Cyberspace

To better understand cyberspace, it is first necessary to define the concept of cyber space. Geographically, cyberspace is an unlimited and non-physical space that facilitates communication between humans and computers regardless of time and place. Accordingly, the unique feature of cyberspace is the inability to pinpoint a specific time or location where an activity occurs or a communication is established. Using cyberspace in this broad sense encompasses all activities performed through computers (Naeini Badi, 2022).

Linguistically, in different cultures, the term "cyber" refers to something virtual and intangible, synonymous with the English word "virtual." The term "cyberspace" originated from the word "cybernetics," which was coined by Norbert Wiener in 1948. Cybernetics is the science of control theory and is used in the study of complex systems.

When cyberspace is mentioned, people often think of a computer connected to the internet, whereas this represents only a small fraction of cyberspace. Cyberspace is not merely a collection of hardware but also a set of symbolic definitions that facilitate an exchange of ideas and beliefs in the form of binary data transactions. In essence, cyberspace is a term that encompasses numerous modern applications of communication technologies. The term "virtual" was coined by science fiction writer William Gibson to describe a vast range of informational resources accessible through computer networks and presented via digital data (Abbasi Darreh Bidi et al., 2016).

Cyberspace, also referred to as cyber space or computer space, is an environment that includes platforms such as the internet, where individuals interact without physical presence, using computers or other communication devices. Across all definitions, the use of internet-connected tools and engagement in cyberspace remain consistent. Given the extensive scope of cyber-related activities and their applicability to a broad range of actions and events occurring within international networks, including the internet, leading experts and scholars in this field advise against translating the term "cyber" into other languages. Due to the linguistic and conceptual nuances of this term in the global context, any attempt to translate it might limit its breadth of application. Therefore, the Persian translation of "cyber" remains somewhat ambiguous. Cyber refers to the science of command, artificial intelligence, and, from a technical perspective, the world of binary code (Farajiha & Alamdari, 2017).

Legal scholars suggest that to avoid legal ambiguities resulting from the vague definition of cyber, the term should be used uniformly across languages, much like the term "telephone," which has a universally consistent meaning. Using a common

international term for cyberspace would ensure a widely accepted and operational definition. Consequently, cyberspace encompasses the rapid transmission of digital information across the world. The mechanism of cyberspace is relatively simple: any data that can be converted into a computer-recognizable format can be transmitted through cyberspace. From a technical perspective, cyberspace refers to the information space created by computer systems and digital networks, which ultimately connect to the internet, the central hub of all networks (Shokrollahi-Far, 2019).

3. Protection of User Rights

Monitoring messaging applications is essential to protect user rights and prevent potential misuse. Given the high volume of personal information exchanged through these messaging applications, oversight can help safeguard users' privacy. Supervision of virtual messaging applications can protect user rights through various mechanisms, one of which is "data protection." For instance, the provisions of the General Data Protection Regulation (GDPR), enacted by the European Union in 2016, ensure that messaging applications implement robust data protection measures and safeguard users' personal information against unauthorized access and misuse.

Another mechanism is the enforcement of user rights. Users of messaging applications have certain rights, including the right to access, rectify, and delete their data, which allows them to control how their information is managed. Another significant mechanism is content moderation, which requires messaging applications to monitor content for illegal activities. This oversight helps prevent harassment, hate speech, and misinformation, thereby creating a safer online environment. Overall, these and other measures enhance user trust, increase the accountability of messaging applications, and ultimately serve to protect user rights (Attarzadeh & Ansari, 2020).

Section Three – Regulations Governing Private Data

A coherent definition of privacy encompasses the sphere of an individual's information that, according to social norms or the individual's explicit declaration, is expected to remain free from any access or intrusion by others. Any interference by individuals or the state within this private domain is prohibited and illegitimate. Privacy constitutes a reasonable boundary within which a person expects to be shielded from external access. The term "others" in this context can refer to both the state and other natural or legal persons (Guangxu, 2021).

From a human rights perspective, the analysis of personal data and its connection to data subjects and messaging applications is significant. The right to personal data is recognized as a fundamental right in international instruments, such as Article 12 of the Universal Declaration of Human Rights and Paragraph 1 of Article 17 of the International Covenant on Civil and Political Rights. This legal approach does not treat personal data as property but rather establishes regulations solely for the protection of the data subject's privacy. Under these conditions, the fate of personal data in the event of a messaging application's inactivity must balance the individual data subject's rights with the broader interests of future generations.

In Iranian law, the Electronic Commerce Law defines personal data messages. However, this law primarily addresses sensitive personal data, and some scholars argue that it lacks a comprehensive provision for the protection of all personal data (Aghaei Togh & Naser, 2020). Nonetheless, Article 59 of this law appears to provide absolute protection for personal data, not limited to sensitive data alone. This article grants individuals the right to access, rectify, and delete their personal data.

Additionally, the Citizens' Rights Charter, issued by the Presidency of Iran but lacking legislative authority, acknowledges the right to personal data in Article 31. This provision guarantees citizens the right to be informed about their personal data, the right to rectify their data, and the right to decide whether their data should be shared with others.

The most recent legal effort in Iran to regulate the governance of personal data is the Draft Law on the Protection of Personal Data and Information. Similar to earlier legal instruments, this draft law outlines specific rights for data subjects, from which an ownership-based interpretation of personal data rights can be inferred. Article 4 of this law stipulates that processing personal data related to non-public situations or conditions requires the data subject's consent. Additionally, Article 6 grants the data subject the right to request the processing or non-processing of all or part of their data at any time. Article 8 provides the right of access to personal data, while Article 33 ensures the right to be informed and to access details such as the type and manner of data processing, processing purposes, sources of data collection, characteristics of the processing, the data subject’s rights, and the means of exercising those rights.

Article 11 of this draft law explicitly recognizes the proprietary rights of data subjects over their personal data. Under this provision, the exploitation of personal data without the data subject's consent is prohibited. Therefore, the data subject themselves retains proprietary rights, a characteristic inherent to ownership. Consequently, no other party has the right to exploit personal data unless they have obtained explicit consent through an agreement transferring such rights. However, according to this article, if the anonymity of the data subject is preserved, if they do not suffer material or moral harm under customary standards, and if obtaining their consent is impossible, proprietary exploitation of personal data without consent is permitted.

Nevertheless, this provision appears incompatible with property law principles in Iranian law. If data were considered property, then any exploitation of such data by non-owners would require a legal mechanism transferring ownership, usufruct rights, or beneficial interest in the data. In the present scenario, the only justification for non-consensual exploitation is the impossibility of obtaining consent. However, since there is no definitive renunciation by the data subject that would render the data legally unclaimed, and since the data does not qualify as lost property under unknown ownership (Mafqood al-Malik) or found property (Luqatah), it remains legally attributable to a specific data subject. Therefore, allowing proprietary exploitation and, consequently, commercial use and profit generation from personal data without consent would constitute unjust enrichment and is legally impermissible (Razavi Asl, 2019).

4. Enhancing Transparency and Accountability

Monitoring the operations of messaging applications is of paramount importance, as these applications serve as intermediaries between users and service providers. Messaging applications must be accountable and transparent to their users. Oversight in this domain contributes to increasing transparency in privacy policies, data collection practices, and content management. Effective supervision fosters transparency and accountability in several areas:

1. Prevention of Misuse: Proper oversight facilitates the detection and prevention of unethical behavior or potential abuses. Strict monitoring can help reduce misconduct and wrongful actions.
2. Enhancing User Trust: When users are aware that monitoring is in place and that their rights are protected, they feel more secure. This trust leads to an increase in user engagement, ultimately improving the performance and quality of services provided by messaging applications.
3. Improving Operational Transparency: Oversight ensures that information regarding the operations and quality of services is readily accessible, enabling users to make better decisions. This transparency can also contribute to service improvement and foster healthy competition.
4. Ensuring Accountability: Regulatory authorities can require service providers to be accountable for their decisions and actions. This ensures that providers cannot easily evade their responsibilities. Consequently, oversight not only protects user rights but also enhances service quality and the efficiency of messaging applications.

5. Criminal Liability for Violating User Rights in Cyberspace

The processing of users' personal information by online messaging applications may, under certain conditions, result in the liability of messaging service providers. Unlike the European Electronic Commerce Directive, which grants a form of initial immunity to messaging applications, the Data Protection Directive imposes specific obligations on them. Failure to comply with these obligations may result in liability for privacy violations against users.

Pursuant to Article 17 of the Directive, online messaging applications must implement appropriate technical and organizational measures to protect private information from accidental or unlawful destruction, accidental damage, alteration, disclosure, or unauthorized access, especially when processing involves transmitting information across networks. Additionally, under Article 23 of the same Directive, any act or omission that violates these regulations and results in harm shall render messaging applications liable. In such cases, the actions of both the user and the messaging application contribute to the violation of privacy rights, rendering both the user and the online messaging application jointly liable to the injured party (Udrea & Smith, 2021; Van der Sloot, 2015).

The rules of civil liability in Iranian law, based on Imamiyyah jurisprudence, distinguish between direct causation (Itlaf) and indirect causation (Tasbib). In direct causation, fault is not required, and merely establishing causation suffices to prove liability. Conversely, liability arising from indirect causation generally requires proof of fault.

The nature of damages caused by users of messaging applications suggests the applicability of indirect causation principles to the liability of messaging applications. For instance, when a person is exploited through a messaging application such as Divar, Snapp, or Digikala by another user, the offending user is considered the direct cause of the harm, while the messaging application is regarded as the indirect cause. Therefore, unless the messaging application demonstrates a lack of negligence, it may be held liable. However, this reasoning applies only when causation alone is sufficient for liability. Otherwise, when a user inflicts harm through a messaging application, the rule governing concurrent direct and indirect causation applies. The prevailing legal principle, derived from authoritative opinions and consensus in Imamiyyah jurisprudence, is that direct causation takes precedence unless indirect causation is stronger. This principle explains why the liability outlined in these regulations reflects general principles of civil liability in Iranian law.

The 1998 Regulations on Computer Information Networks, adopted by Iran's Supreme Council of the Cultural Revolution, emphasize the legal and civil liability of individuals for their online activities. The emphasis on individual liability in cyberspace demonstrates the council's adherence to fundamental principles of civil liability in Iran, including the principle of personal responsibility (Najafi & Madani, 2020).

Furthermore, various provisions of these regulations emphasize the non-liability of online service providers for user violations. According to Article 5-3-1 of the regulations, media outlets and users are responsible for the content they publish online.

Additionally, under Article 5-3-4 of the Regulations on Information Service Providers (ISP), the liability of ISPs regarding access to third-party content is limited to facilitating access and implementing content filtering mechanisms.

If, due to an ISP's negligence, a user violates another individual's privacy, can the ISP be held civilly liable for the privacy violation?

In this scenario, the user is the direct violator, while the ISP is the indirect cause of the violation, thus constituting a case of concurrent direct and indirect causation. The general rule in Iranian law attributes liability to the direct violator unless the indirect cause is stronger. Despite the ISP's failure to filter content properly, if a user deliberately commits a privacy violation, the user's action is stronger in causation, making their liability more justifiable.

Nonetheless, it may be argued that since the violation would not have occurred without the ISP's platform, the ISP should also be held liable alongside the direct violator. This argument could be justified based on Article 526 of the 2013 Islamic Penal Code, which states:

"When multiple actors contribute to a crime—some through direct commission and others through indirect causation—the one to whom the crime is primarily attributed is liable. If the crime is attributed to all involved, liability is shared equally unless the impact of their actions varies, in which case each is responsible in proportion to their contribution. If the direct actor is involuntary, ignorant, a minor, or insane, only the indirect cause is liable."

If a user commits a privacy violation due to the ISP's negligence, common legal reasoning could attribute harm to both the user and the ISP, resulting in shared liability (Norouzi & Rabbani Mousavian, 2021).

However, since the provision in Article 526 contradicts the prevailing view in Imamiyyah jurisprudence and Iranian law, it must be interpreted restrictively and only applied to cases of concurrent direct causation. The present case falls under concurrent indirect causation, which means the prevailing rule remains that the direct violator is liable.

Adherence to civil liability principles is also evident in certain legislative bills. For example, in the Comprehensive Public Media Bill, Article 11, Note 3 states:

"If media content is published under the author's real or pseudonymous name, liability rests with the author; otherwise, liability rests with the media outlet."

Under this provision, the principle of personal liability applies in public media, including online messaging applications. If a messaging service functions as a news platform and a user commits a privacy violation, the user bears sole responsibility.

The User Rights and Essential Digital Services Protection Bill, recently reviewed in the Iranian Parliament under Article 85 of the Constitution, contains provisions that, if ratified, may introduce civil liability for online messaging applications.

However, a close examination of this bill reveals that its drafters adhered to the general principles of civil liability. The bill imposes specific obligations on online messaging applications.

According to Article 2, Note 5 of the bill,

"All domestic social messaging applications and the official representatives of influential foreign messaging services (in accordance with formal negotiations) must comply with the regulations set forth by the Cybercrime Determination Committee and the directives issued by its secretariat regarding the filtering of criminal content."

The responsibility of social messaging services under this provision is limited to filtering criminal content. Similarly, Article 2, Note 6 states:

"All social messaging applications covered by this law are subject to the obligations and responsibilities of access and hosting service providers, as stipulated in the Cybercrime Law and Chapter Ten of the Criminal Procedure Code."

Reviewing these laws and regulations demonstrates no explicit recognition of civil liability for messaging applications. The enforcement provisions only entail fines, imprisonment, or platform termination, with no reference to civil liability. Thus, the general rules of civil liability remain applicable, as previously explained.

6. Challenges Related to the General Data Protection Regulation (GDPR)

One of the main challenges facing this law today is the lack of resources and regulatory institutions, including cybersecurity experts and data protection officers. Governments and technology companies must invest in further cybersecurity training and workforce development in this field. Regulatory authorities in various countries may lack the necessary human resources and expertise to effectively monitor the implementation of data protection laws, which can lead to insufficient oversight and ineffective enforcement of the law (Rahbari, 2022).

Another issue concerning the enforcement of data protection regulations is the variation in implementation across different countries. The penalties imposed on organizations for violations may differ from one country to another. In summary, one of the primary challenges in enforcing data protection laws is the discrepancy in interpretation and implementation across jurisdictions, which can result in inconsistencies in enforcement and regulatory deficiencies. The absence of centralized, independent regulatory bodies and divergences in enforcement mechanisms can create coordination problems regarding exemptions and effective oversight. If messaging applications are uncertain whether exemptions might be revoked easily or interpreted differently based on varying conditions, they may avoid applying for exemptions altogether, leading to distrust in the effective implementation of the law (Farahani et al., 2023).

Another issue in data protection laws is the complexity of the complaint process. The process of filing a complaint and addressing legal violations can be complex and time-consuming, potentially discouraging users from pursuing their rights and negatively impacting their motivation to report breaches. Despite efforts to create a robust framework for personal data protection, weaknesses in the enforcement mechanisms of this law remain a significant challenge in safeguarding user rights and ensuring effective implementation. These shortcomings necessitate review and procedural reforms to ensure that the laws are enforced properly and effectively (Attarzadeh & Ansari, 2020).

7. Conclusion

The managers of virtual messaging applications handle a vast amount of users' personal data. The dominance of software owners over personal data is inevitable; as long as users benefit from messaging applications, their personal data will be accessible to the owners of these platforms. The collection and processing of personal data by software owners, as well as its subsequent use in various domains, is contingent upon user consent.

As long as messaging applications remain in use, the relationship between users and software owners is largely governed by an agreement referred to as a privacy policy. However, if a messaging application ceases its operations for any reason, the existing agreement may not comprehensively address all legal challenges. The question of what happens to personal data when messaging services are discontinued depends on the legal analysis of personal data ownership, the connection between the data and the individual it pertains to, and the contractual relationship between the user, the data controller, and other stakeholders.

If the governing system for personal data follows property law principles, then data should be treated as property belonging to individuals. In this perspective, data must align with the legal attributes of property and ownership. If so, the fate of personal data before and after the discontinuation of messaging applications would remain under the control of the data owner.

The current legal framework governing personal data is contractual, incorporating human rights principles. As a result, the contractual consent agreement between the user and the messaging application serves as the governing contract, determining the collection, transfer, processing, and usage of personal data. Data protection regulations, with their emphasis on privacy protection for data subjects, impose mandatory legal requirements on software owners and personal data processors.

The existing system is criticized for not treating personal data as traditional assets despite its financial value and ownership attributes. Under the current legal order, users do not fully recognize the financial worth of the data they provide to messaging applications. Most users rely on multiple messaging applications daily, and their consent to data processing is often granted without thorough examination of the terms and conditions. Many users prioritize quick access to services over carefully reviewing privacy agreements, leading them to consent unknowingly.

One of the primary legal challenges in cyberspace is the security of user data and information. With the extensive use of the internet and online services, personal, financial, and social data are increasingly at risk of cyberattacks, hacking, viruses, and malware. The Computer Crimes Law explicitly addresses issues such as unauthorized access to data, illegal surveillance, system intrusions, and data theft. This law also covers cybercrimes such as online fraud, defamation, threats, and the spread of viruses.

Another key challenge is protecting user confidentiality. Many users entrust online services with their personal data, and if this data is disclosed without authorization or misused, their rights are violated. Confidentiality is a fundamental user right, ensuring that personal data is not used or disclosed without consent. This principle is often reflected in privacy policies on websites and applications. If these principles are not upheld, users may seek legal action to enforce their rights.

In the legislative sphere, the legal framework for protecting personal data has yet to fully address the property rights aspects of personal data. The primary reason for this gap is the dominant focus on privacy protection as a human rights issue, which has influenced legislators and legal drafters. Consequently, laws developed under this approach do not provide a comprehensive legal framework for data ownership.

Based on the research findings, there is no unified and comprehensive law governing messaging applications in cyberspace. Instead, fragmented laws, particularly the Computer Crimes Law and the Electronic Commerce Law, are applied. However, due to the lack of updates, insufficient clarity, and incompatibility with traditional legal frameworks, these laws are gradually losing their effectiveness. In many critical areas, particularly in protecting privacy rights, the existing legal framework appears inadequate.

Civil liability in cyberspace entails the responsibility of individuals and organizations for damages resulting from the misuse or unauthorized use of online data or services. This liability may be civil or criminal, depending on the applicable laws. If an individual or organization violates a user’s rights, either intentionally or unintentionally, they must compensate for the damages. In the case of online messaging applications, civil liability may include responsibility for user-generated content, privacy violations, or failure to comply with data protection regulations.

Due to the lack of explicit regulations in Iranian law concerning the civil and criminal liability of internet intermediaries, some Iranian courts have refrained from holding these service providers liable. To address this issue, the broad interpretation of Article 1 of the Civil Liability Law in civil lawsuits and the provisions of the Islamic Penal Code on computer crimes in criminal cases could provide legal solutions to this deficiency.

While the regulatory obligations imposed under digital services laws provide several benefits, they can also be problematic, leading to imbalances between security, user rights, and the operational freedom of messaging applications. These regulations may negatively impact diversity, innovation, and competition in cyberspace because instead of focusing on developing better services, messaging applications prioritize regulatory compliance. Excessive legal burdens may hinder service providers' ability to conduct business.

To overcome these challenges, appropriate legal and technical measures should be adopted, including:

- Establishing and updating specific laws on cyberspace, including comprehensive legislation for data protection and user rights.
- Continuous monitoring of online activities and strict enforcement against privacy violations, data security breaches, and user rights violations.
- Educational programs for users to enhance awareness of their rights and safe usage of online services.

- Encouraging messaging applications and technology companies to comply with security standards and provide privacy control tools for users.
- International cooperation in addressing global threats, such as cyberattacks and privacy breaches, recognizing the borderless nature of cyberspace.

Ethical Considerations

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

Acknowledgments

Authors thank all participants who participate in 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

Abbasi Darreh Bidi, A., Yousefi, S., & Mahmoudi, F. (2016). Virtual Space Technology and Progress. In *Selected Articles from the 10th Pioneers of Progress Congress*.

Aghaei Togh, M., & Naser, M. (2020). Challenges of Protecting Private Data in the Internet of Things: A Comparative Study of Iranian and EU Law. *Administrative Law Quarterly*, *7*(23), 33-55.

Attarzadeh, S., & Ansari, J. (2020). *Special Criminal Law on Cybercrimes*. Mizan Legal Foundation.

Farahani, M. S., Kadkhodaei, A. A., & Rostami, V. (2023). Competition Law in Digital Platforms: The Need to Revise Traditional Rules. *Public Law Research*, *25*(79), 7-40.

Farajiha, M., & Alamdari, A. (2017). A Comparative Study of Criminalization Criteria in Cyberspace in Iranian and German Legal Systems. *Comparative Law Studies*, *8*(2).

Guangxu, Y. (2021). Research on computer network information security based on improved machine learning. *Journal of Intelligent & Fuzzy Systems*, *40*(4), 6889-6900. https://doi.org/10.3233/JIFS-189520

Naeini Badi, M. (2022). *The Role of Virtual Space in Life*. Aftab Giti.

Najafi, H., & Madani, M. (2020). *Participation in Intellectual Property Violations in Iranian and U.S. Law*. Mizan.

Norouzi, M., & Rabbani Mousavian, S. A. (2021). Civil Liability for Violating Privacy Rights in Cyberspace from a Jurisprudential and Legal Perspective. *Islamic Jurisprudence and Legal Principles*, *14*(1), 221-240.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC press. https://doi.org/10.1201/9780849390326

Rahbari, E. (2022). An Analysis of Competitive Law Challenges in Big Data. *Legal Research Quarterly*, *98*, 302-307.

Razavi Asl, S. M. (2019). *Internet Theft (Nature, Elements, Punishments, and Prevention)*. Islamic Research Foundation.

Safarzadeh Roodsari, M. (2017). *Cybercrimes: Emergence, Prevalence, and Increase*. Aftab Giti.

Shokrollahi-Far, N. (2019). *Examining the Impact of Virtual Space*. Sanjesh and Danesh.

Udrea, A., & Smith, D. (2021). Minority protection and kin-state engagement: Karta Polaka in comparative perspective. In *Poland's Kin-State Policies* (pp. 67-82). Routledge. https://doi.org/10.4324/9781003190288

Van der Sloot, B. (2015). Welcome to the Jungle: The liability of Internet intermediaries for privacy violations in Europe. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *6*, 211.