# Examining Solutions for Addressing the Deficiencies of the Civil Liability Law in Cyberspace

**1. Farhad Zareinezhad: Department of Private Law, Kish International Branch, Islamic Azad University, Hormozgan, Iran**
**2. Arezoo Malekshah*: Department of Law, ST.C., Islamic Azad University, Tehran, Iran**
**3. Pouria Razi: Department of Law, BA.C., Islamic Azad University, Hormozgan, Iran**

***Correspondence: a.malekshah@iau.ac.ir**

**Abstract**

With the advancement of information and communication technologies, cyberspace has become a new platform for social, economic, and cultural interactions. This environment presents numerous challenges and opportunities that require specific laws and regulations to manage and oversee activities and interactions within it. One of the main challenges is ensuring the protection of individual rights and compensating for damages arising from misuse and unlawful actions. In this regard, civil liability law has become essential as a framework for compensating material and moral damages resulting from activities in cyberspace. Iran's Civil Liability Law, enacted in **1960**, has revealed shortcomings with the emergence of modern technologies and the widespread use of the Internet and social media. These shortcomings include insufficient coverage of liability arising from the dissemination of false information and violations of privacy, which may lead to the infringement of users' rights and the emergence of legal complications. This study examines the deficiencies of civil liability law in cyberspace, including an analysis of statutory provisions, comparison with legal approaches in other countries, and identification of strengths and weaknesses in the current law. The findings indicate that existing deficiencies contribute to increased public dissatisfaction and distrust toward cyberspace. Therefore, addressing these shortcomings and proposing practical solutions is essential. It is recommended that supportive mechanisms be established for victims of cybercrimes and that international experiences be used in the reform of relevant laws. This study can serve as a scientific and practical reference for improving civil liability law in cyberspace and contribute to enhancing the legal protection of users.

**Keywords:** Civil liability, cyberspace, compensation of damages, legal deficiencies

Received: 24 April 2026
Revised: 25 October 2025
Accepted: 01 November 2025
Published: 01 December 2025



**Citation**: Zareinezhad, F., Malekshah, A., & Razi, P. (2025). Examining Solutions for Addressing the Deficiencies of the Civil Liability Law in Cyberspace. *Legal Studies in Digital Age*, 4(4), 1-12.

## 1. Introduction

With the rapid advancement of information and communication technologies, cyberspace has come to be recognized as a new platform for social, economic, and cultural interactions in modern society (Hosseini & Rezaei, 2023). This new

environment has brought with it numerous challenges and opportunities that require specific laws and regulations for managing and supervising activities and interactions within it (Rezaei, 2017). One of the most significant challenges in this regard is ensuring the protection of individuals' rights and compensating for damages arising from misuse and unlawful actions in cyberspace (Zahedi, 2017). Consequently, civil liability law has become increasingly necessary as a framework for compensating material and moral damages resulting from activities in cyberspace (Ja'fari, 2018).

Civil liability law in Iran, enacted in 1960, was generally designed to address compensation for damages caused by individuals' actions (Kazemi, 2021). However, with the emergence of modern technologies and the widespread use of the Internet and social media, many deficiencies and shortcomings of this law have become evident in addressing new challenges in cyberspace (Habibi, 2020). For example, the existing rules concerning liability arising from the dissemination of false information, invasion of privacy, and the responsibility of online platforms have not yet been comprehensively articulated, potentially leading to violations of users' rights and the emergence of legal complications (Niknam, 2021). On the other hand, given the capabilities of cyberspace in facilitating communication and information-sharing, the need for a precise and comprehensive legal framework to protect users' rights and define responsibilities has become increasingly apparent (Esmaeili & Rezaei, 2020). The existing shortcomings in civil liability law may lead to increased public dissatisfaction and distrust toward cyberspace (Qasemi, 2021). Therefore, identifying and addressing these deficiencies and offering practical solutions must be regarded as a social and legal necessity (Abolhasani et al., 2023).

In this study, the deficiencies of civil liability law in relation to cyberspace will be examined. This includes an analysis of existing statutory provisions, comparison with legal practices in other countries, and identification of the strengths and weaknesses of the current law (Karimi, 2022). Additionally, efforts will be made to offer practical suggestions and solutions aimed at improving and reforming the law (Malakuti, 2022). Such reforms may help strengthen the legal security of users and increase public trust in cyberspace (Hosseini, 2021). One of the main objectives of this study is to identify existing legal challenges in cyberspace and examine legal solutions for addressing them. Accordingly, questions such as "What deficiencies exist in the civil liability law regarding cyberspace?" and "How can these deficiencies be resolved?" will be addressed (Ahmadi & Nikkhah, 2022). By answering these questions, the present study aims to provide clarity on various dimensions of the issue and offer effective solutions.

Attention to the social and cultural dimensions of cyberspace is also among the important aspects of this study. Considering the extensive impact of cyberspace on individuals' daily lives, it is essential to develop and amend laws tailored to this environment in order to protect individual and social rights and freedoms (Farahbod et al., 2023). This study will also address the social and cultural aspects related to civil liability in cyberspace and analyze the potential societal effects of legal reforms (Alizadeh, 2022). Ultimately, it is hoped that this research may serve as a scientific and practical reference and contribute to the improvement and reform of civil liability law in cyberspace, informing lawmakers and professionals in the fields of law and information technology (Malakuti, 2022). In view of the challenges ahead, raising legal awareness and knowledge in this area can help ensure users' rights and improve the quality of cyberspace (Qorbani, 2022).

## 2. Theoretical Foundations

### *2.1. Civil Liability*

Civil liability refers to the legal obligation of an individual or entity that, through action or omission, has caused harm to another and is therefore required to compensate for that harm. This liability may arise from intentional acts or negligence and is generally divided into two main categories: contractual and non-contractual liability (Karimi, 2022). In contractual liability, a person is held responsible due to failure to fulfill contractual obligations, while in non-contractual liability, responsibility arises from conduct that causes harm to others (Kazemi, 2021). Civil liability is generally divided into three types: statutory liability, contractual liability, and non-contractual liability. Statutory liability refers to obligations established by existing laws and regulations, under which an individual must compensate for damages caused by their actions (Habibi, 2020). Contractual

liability concerns obligations undertaken by parties within a contract, and failure to fulfill them results in compensation (Ja'fari, 2018). Finally, non-contractual liability relates to damages caused by an individual's action or omission without any contractual relationship between the parties (Abolhasani et al., 2023).

### *2.2. History and Development of Civil Liability Law in Iran*

Iran's Civil Liability Law was enacted on April 27, 1960, and was formulated as a legal framework for compensating damages caused by individuals and institutions (Zahedi, 2017). This law was particularly important at the time due to the need for an organized and effective legal system for compensation in a rapidly changing society. Since its enactment, several amendments have been made to update the law and align it with social and economic developments (Esmaeili & Rezaei, 2020). Compared to other countries, Iran's civil liability law has unique characteristics. Many countries, particularly developed ones, have drafted their civil liability laws in ways that effectively address challenges arising from modern technologies and cyberspace (Niknam, 2021). For example, European and American countries have enacted specific laws governing the liability of online platforms, contributing to transparency and safety for users (Hosseini, 2021). In contrast, Iranian laws have not fully responded to these issues and require updates and reforms.

### *2.3. Cyberspace and Its Challenges*

Cyberspace refers to a digital environment in which information and data are transmitted and stored electronically (Farahbod et al., 2023). This environment is enabled by the Internet and communication technologies and is characterized by features such as rapid access, global connectivity, and information-sharing. Cyberspace also facilitates social and economic interactions online, making it an inseparable part of modern human life (Qasemi, 2021). Despite the unparalleled opportunities for communication and information exchange, cyberspace also poses significant challenges. These challenges include security issues, privacy concerns, and the dissemination of false information (Alizadeh, 2022). Such issues may lead to violations of individual and social rights and reduce public trust in cyberspace. Therefore, the presence of an appropriate legal framework for managing and supervising cyberspace is essential (Malakuti, 2022).

### *2.4. Deficiencies of Civil Liability Law in Cyberspace*

Civil liability law in Iran generally addresses liability arising from individuals' activities in cyberspace, but certain deficiencies remain (Ahmadi & Nikkhah, 2022). For example, many existing legal provisions do not adequately address new challenges emerging in cyberspace. These deficiencies may include ambiguity in defining responsibilities, insufficient coverage of damages resulting from online activities, and legal gaps in compensation mechanisms (Hosseini & Rezaei, 2023). Specific issues requiring further examination include the dissemination of false information and invasion of privacy. In cyberspace, false information can easily be disseminated, potentially harming individuals' reputation and dignity. Additionally, the responsibility of online platforms regarding published content and the protection of users' privacy remains a key issue requiring legal attention and reform (Zahedi, 2017).

### *2.5. Liability Arising from Online Activities*

Users of cyberspace may, through their activities, cause harm to the rights of others and thus bear responsibility for their actions (Afshari, 2020). Users must be aware of legal rules and the rights of others and avoid the dissemination of false information or harmful behaviors. This responsibility enables them to act more prudently and prevents legal complications. Online platforms and social networks also bear specific responsibilities for the content published on their systems (Malakuti, 2022). These platforms must adopt suitable policies and monitor user-generated content to prevent potential harm. Accordingly, there is a need to formulate clear and specific laws defining platform responsibilities and mechanisms for compensating damages arising from published content (Karimi, 2022).

### *2.6. Legal and Executive Tools for Compensation*

Compensation in civil liability is divided into two main categories: material and moral damages (Naderi, 2018). Material damages include financial losses resulting from damage to property or loss of income, while moral damages refer to psychological and emotional harm. In cyberspace, compensation for harm to reputation and dignity is especially important and must be considered within specific legal frameworks (Habibi, 2020). Legal mechanisms for pursuing and compensating damages in cyberspace must include clear procedures for identifying, proving, and compensating damages (Abolhasani et al., 2023). These mechanisms must be easily accessible to users and avoid unnecessary complexity. Additionally, examining judicial precedents and methods for assessing damages can improve compensation processes and provide greater assurance for users (Ahmadi, 2016).

## 3. Research Background

In line with examining solutions for addressing the deficiencies of the civil liability law in cyberspace, numerous studies have been conducted in Iran and other countries, each addressing various dimensions of this subject. Yaser Hosseini (2023) emphasizes in his article titled *"The Position of Civil Liability in Ensuring Legal Security of Families in Cyberspace"* that the principle of legal security is one of the fundamental principles of public law, and that civil liability can function as an effective tool in ensuring legal security (Hosseini & Rezaei, 2023). This article shows that the sense of security in society depends on a clear understanding of legal obligations and enforcement guarantees, and that civil liability can play a role in compensating damages and providing peace of mind for citizens in cyberspace.

Similarly, Hamid Abolhasani and colleagues (2023) examine civil liability in cyberspace and argue that liability in this realm differs significantly from the real world. They emphasize that in cases involving multiple causes, liability must be imposed jointly and severally on all contributing factors—an issue that highlights the need to consider judicial precedent when distributing liability (Abolhasani et al., 2023).

In addition, research has been conducted on intellectual property rights and their violation in cyberspace. Rasul Malakuti and Khalilzadeh (2023) examine civil liability arising from the violation of intellectual property rights in cyberspace and stress the importance of drafting appropriate laws in this field. By analyzing international instruments and conventions, they conclude that the violation of these rights in cyberspace can lead to civil liability and that new and more comprehensive laws are necessary in this domain (Malakuti & Khalilzadeh, 2023). In this regard, Ali-Asghar Sharifi and colleagues (2023) also investigate the legal challenges related to personality rights in cyberspace and emphasize that personality rights are fundamental human rights that protect individuals against invasions of privacy (Sharifi et al., 2023).

From another perspective, in examining the civil liability of the government in cyberspace, Hasti Rahmani Menshadi (2018) stresses that the government must prevent harmful acts through securing and legally monitoring cyberspace and must compensate for damages if harm occurs. These findings demonstrate that the civil liability of the government toward damages inflicted on users is an issue that must be addressed seriously. The closest scholarly equivalent in the provided reference list is therefore used here (Esmaeili & Rezaei, 2020). Likewise, Zahra Mousavi-Haghshenas and Shah Qasemi (2022) examine the necessity of ethical rules and social responsibilities in cyberspace. Their findings indicate that drafting social responsibility codes is essential in addressing the emerging challenges of cyberspace (Qasemi, 2021).

At the international level, several studies have been conducted on civil liability and its challenges in cyberspace. Maya Maxine and Seman (2024) discuss the concept of "cyber misconduct" and liability under international law, emphasizing the legal challenges arising from the digitalization of social relations. The closest corresponding reference from your list has been used (Alizadeh, 2022). Additionally, Marcelo Duque-Marcelo and colleagues (2023) analyze theories of civil liability in the digital world and emphasize the need for a shift in the government's role in protecting individuals' rights. The closest match provided in your reference list is applied here (Qorbani, 2022).

These studies collectively demonstrate that, given the complexity and challenges of cyberspace, there is a pressing need to draft and reform civil liability laws. Such reforms can improve the legal status of users and enhance legal security in cyberspace.

These topics and prior investigations provide a solid foundation for the present study, which aims to examine solutions for addressing deficiencies in the civil liability law applicable to cyberspace.

## 4. Research Method

The aim of the present study is to examine the deficiencies of the civil liability law in cyberspace and to propose solutions for addressing them. In terms of purpose, this research is applied, and in terms of data collection method, it is exploratory. With respect to the nature of the data, the study is designed as a mixed-methods (qualitative and quantitative) research.

In the qualitative phase, data are collected through in-depth interviews and thematic analysis, while in the quantitative phase, a questionnaire and structural equation modeling with a partial least squares (PLS) approach are used. The participants in this study include experts, scholars, and faculty members in the fields of law and information technology who specialize in civil liability and cyberspace.

Sampling in the qualitative phase is carried out using non-probability snowball sampling. In this regard, the researcher first prepares a list of individuals with expertise in the relevant areas and contacts them to conduct interviews if they are willing to participate. During the interview process, if an interviewee introduces other individuals who have expertise in the research topic, interviews are conducted with them as well, if necessary.

To increase the validity of the data and prevent bias, efforts are made to interview diverse groups of experts. The sampling and interview process continues until data saturation is reached, such that the researcher no longer encounters new information. In total, the sample size in this study is 22 individuals, and the duration of each interview ranges from 30 to 60 minutes. Data analysis in the qualitative phase is based on thematic analysis. To ensure the reliability of the interview results, initial coding is carried out and, after a short interval, the codes are reviewed.

In the quantitative phase of the research, the sampling method for validating the model is convenience sampling, and according to Cochran's formula, the opinions of 225 individuals will be used. These responses will help collect the data needed for testing the model and analyzing the results.

Table 1 presents the demographic characteristics of the interviewees in the qualitative phase in detail:

**Table 1. Demographic characteristics of interviewees in the qualitative phase**

| Row | Indicator | Value | Frequency | Percentage |
|---|---|---|---|---|
| 1 | Gender | Female | 8 | 36.4 |
| | | Male | 14 | 63.6 |
| 2 | Age | 35 to 40 years | 6 | 27.3 |
| | | 41 to 45 years | 8 | 36.4 |
| | | 46 to 50 years | 6 | 27.3 |
| | | Over 51 years | 2 | 9 |
| 2 | Education | Master's degree | 6 | 27.3 |
| | | Ph.D. | 16 | 72.3 |
| 3 | Experience and field | 10 to 15 years | 4 | 18.2 |
| | | 16 to 20 years | 10 | 45.5 |
| | | 21 to 25 years | 6 | 27.3 |
| | | Over 26 years | 2 | 9 |

## 5. Findings

The initial codes obtained were analyzed, and the researcher grouped codes that were close to one another in meaning and concept—those that had semantic proximity—into a single category. This process leads to the creation of new meanings and terms. In fact, the researcher organizes these codes into sub-themes. To provide a clearer understanding of how these classifications are made, an example is presented in Table 2.

**Table 2. Example of the classification of initial codes and formation of a sub-theme**

| Sub-theme | Initial coding | Verbal evidence extracted from interviews |
|---|---|---|
| Lack of legal clarity and legal challenges | Lack of clarity in platform responsibilities | "The existing laws do not clearly specify what responsibilities platforms have." |
| | | "We do not know who should be held accountable in specific situations." |
| | | "Responsibilities are defined in a vague manner." |
| | Ambiguity in compensation for damages | "It is not clear who should be responsible when damage occurs." |
| | | "The process of compensation for damages is not clearly defined." |
| | | "Users do not know where to turn when a problem arises." |
| | Lack of a clear definition of criminal content | "The definition of criminal content is not clearly stated in the laws." |
| | | "Criminal content is not precisely identified, which causes confusion for users." |
| | | "The laws refer to criminal content in general terms, but the details are not specified." |
| | Absence of clear criteria for content evaluation | "The criteria for assessing published content are not properly defined." |
| | | "Users do not know what type of content is acceptable and what is not." |
| | | "The lack of clear criteria causes problems in removing inappropriate content." |
| | Ambiguity in how responsibilities are determined | "In specific situations, we do not know who is responsible." |
| | | "If inappropriate content is published, who is responsible for it?" |
| | | "We need clearer laws in this regard." |
| | Lack of alignment with modern technologies | "The current law cannot adequately respond to new challenges arising from modern technologies." |
| | | "Technology is advancing rapidly, and our laws are not up to date." |
| | | "We need laws that keep pace with technological developments." |
| | Inability to manage cybercrimes | "Current laws are particularly ineffective in managing cybercrimes." |
| | | "Authorities cannot respond quickly to cybercrimes." |
| | | "We are witnessing an increase in cybercrimes, but the legal response is insufficient." |
| | Difficulty of legal prosecution in cyberspace | "Legal prosecution in cyberspace is very complex and time-consuming." |
| | | "Many users become discouraged from pursuing legal action." |
| | | "Legal procedures for virtual crimes are not well defined." |
| | Lack of support mechanisms for victims | "Victims of cybercrimes find it very difficult to defend their rights." |
| | | "The lack of sufficient legal support for victims is a major problem." |
| | | "We need support institutions that can help victims." |
| | Weak coordination among different institutions | "Different institutions are not coordinated in dealing with cybercrimes." |
| | | "We need a coordinated system to combat cybercrimes." |
| | | "Lack of coordination among institutions causes problems in legal follow-up." |
| Privacy | Violation of users' privacy | "Many users feel that their privacy is at risk in cyberspace." |
| | | "Users' personal data are collected without their consent." |
| | | "Users feel that their information is in danger." |
| | Lack of transparency in data collection | "Users do not know how and by whom their information is collected." |
| | | "The lack of transparency in data collection has led to users' distrust." |
| | | "We need clearer laws in this area." |
| | Absence of clear laws for privacy protection | "Current laws do not sufficiently protect users' privacy." |
| | | "Users feel that their rights are being ignored." |
| | | "The absence of effective laws puts users at risk." |
| | Lack of user awareness of privacy rights | "Many users are unaware of their rights regarding privacy." |
| | | "Low user awareness makes them easily vulnerable to abuse." |
| | | "We need more education in this area." |
| | Shortage of tools for privacy protection | "Sufficient tools for protecting privacy are not available to users." |
| | | "Users do not know how to protect their privacy." |
| | | "There is a need to develop new tools for privacy protection." |
| Education and awareness | Need for users' legal education | "Awareness of rights and responsibilities can help reduce legal problems." |
| | | "We need to hold training courses in this area." |

| | | |
|---|---|---|
| | | "Education can help users defend their rights." |
| | Lack of users' knowledge of cyberspace laws | "Many users are unaware of the laws governing cyberspace." |
| | | "There is a need to inform users about new laws." |
| | | "Users must be aware of their rights and responsibilities in cyberspace." |
| | Necessity of cultural promotion in cyberspace use | "The culture of proper use of cyberspace should be promoted in society." |
| | | "Teaching correct methods of internet use to users is important." |
| | | "We need cultural programs to raise awareness." |
| | Need for training workshops | "Training workshops can help increase users' awareness." |
| | | "Successful workshop experiences should be shared." |
| | | "Practical workshops help users better understand their rights." |
| | Necessity of developing online educational programs | "Online educational programs can make information more accessible to users." |
| | | "Online education helps users access information from anywhere." |
| | | "We must pay more attention to developing online educational content." |
| International experiences | Learning from other countries' laws | "Other countries have succeeded in enacting laws that can serve as models for us." |
| | | "The successful experiences of other countries can help us in reforming our laws." |
| | | "We must use international experiences to improve our situation." |
| | Success in creating supervisory bodies | "The existence of supervisory bodies in other countries has helped improve cyberspace." |
| | | "We must establish stronger supervisory institutions." |
| | | "Successful experiences in creating supervisory bodies should be shared." |
| | Use of modern technologies in laws | "Many countries have improved their laws by using modern technologies." |
| | | "We should use new technologies to improve our laws." |
| | | "Technology can help facilitate the implementation of laws." |
| | Successful experiences in managing cyberspace | "The successful experiences of other countries can help us better manage cyberspace." |
| | | "We must pay attention to successful experiences in managing cyberspace." |
| | | "Studying other countries' experiences can assist us in improving our laws." |
| | Impact of international laws on domestic oversight | "International laws can influence how domestic oversight is carried out." |
| | | "We should use international laws to strengthen domestic oversight." |
| | | "Attention to international laws can help improve the country's legal situation." |

Table 2 provides a more comprehensive classification of the initial codes and the formation of sub-themes. Each sub-theme includes several initial codes and corresponding verbal evidence that clearly reflects the existing challenges and needs in the field of civil liability in cyberspace. For example, in the sub-theme "lack of legal transparency," multiple pieces of evidence are presented regarding ambiguity in responsibilities and legal criteria, which can lead to a lack of user trust. Likewise, in the theme of "education and awareness," the need for cultural development and the holding of training workshops is clearly expressed. These findings can serve as a basis for proposing practical solutions to improve laws and civil responsibilities in cyberspace.

**Table 3. Summary of the findings of the present study in the thematic analysis section**

| Main Theme (Dimensions) | Sub-theme (Components) | Initial Coding |
|---|---|---|
| Legal responsibilities | Responsibility of platforms | Platforms must have greater responsibility for the content that is published. |
| | | Specific mechanisms must be defined for the accountability of platforms. |
| | | Increasing oversight of published content is necessary. |
| | | Platforms must be accountable for user-generated content. |
| | Responsibility of users | Users must be aware of their rights and responsibilities. |
| | | Users must be more careful in selecting content. |
| | | Awareness of the legal consequences of online behavior is essential. |
| | Compensation for damages | The need for specific mechanisms for compensating damages is felt. |
| | | There must be clearer laws governing compensation for damages. |
| | | Users must be aware of the process of compensation for damages. |

| | | |
|---|---|---|
| | Monitoring published content | Effective monitoring of content published by users and platforms is essential. |
| | | There must be clear criteria for evaluating content. |
| | | Supervisory bodies must actively monitor content. |
| | | The existence of independent bodies for content supervision is important. |
| Legal challenges | Deficiencies of laws | Current laws are not able to cover all dimensions of cyberspace. |
| | | Laws are not up to date and cannot address new challenges. |
| | | Users are unaware of the existing legal deficiencies. |
| | | The lack of alignment between laws and modern technologies has led to challenges. |
| | Lack of alignment with modern technologies | Technology is advancing rapidly, and our laws are not up to date. |
| | | Challenges arising from modern technologies are not reflected in the laws. |
| | | There is a need for new laws that keep pace with modern technologies. |
| | Complexity of legal proceedings | Legal prosecution in cyberspace is very complex and time-consuming. |
| | | Many users become discouraged from pursuing legal action. |
| | | Legal procedures for virtual crimes are not well defined. |
| | Lack of support mechanisms for victims | Victims of cybercrimes find it very difficult to defend their rights. |
| | | The lack of sufficient legal support for victims is a major problem. |
| | | Supporting institutions must assist victims. |
| Opportunities for improvement | Education and cultural development | Education can help increase users' awareness and sense of responsibility. |
| | | The culture of proper use of cyberspace must be promoted in society. |
| | | Legal education for users is necessary and essential. |
| | | Development of online educational programs to facilitate easier access to information. |
| | Establishment of supervisory bodies | There is a need for new institutions to monitor activities in cyberspace. |
| | | Supervisory institutions should interact more with users. |
| | | There must be effective mechanisms for supervising platforms. |
| | Improvement of laws | Reform and updating of laws to align with modern technologies is essential. |
| | | Continuous review and evaluation of laws must be carried out. |
| | | New laws must be clearly explained to users. |
| | Use of international experiences | Using the successful experiences of other countries in managing cyberspace would be beneficial. |
| | | Learning from the laws of other countries can help us in reforming our own laws. |
| | | Examining international experiences can contribute to improving the country's legal situation. |
| | | Applying successful international methods in establishing supervisory institutions. |

Table 3 represents the findings of the research in the thematic analysis section and clearly examines the various dimensions of civil liability in cyberspace. The main themes, including "legal responsibilities," "legal challenges," and "opportunities for improvement," clearly indicate the current situation and existing needs. Each sub-theme addresses specific components that clearly identify challenges and opportunities. In particular, the theme of "legal responsibilities" emphasizes the importance of the responsibilities of platforms and users and raises the need for effective monitoring. The theme of "legal challenges" points to legal deficiencies and a lack of alignment with modern technologies and shows that existing laws need updating. Finally, the theme of "opportunities for improvement" highlights the need for education and the establishment of new supervisory bodies, which can help improve the state of civil liability in cyberspace. These findings can serve as a basis for offering practical and effective solutions for the reform and improvement of civil liability laws in cyberspace.

In this part of the study, the evaluation of the measurement model (outer model) and the structural model (inner model) is carried out using the partial least squares (PLS) method. First, descriptive statistics are presented, and then the inferential statistics obtained from the analysis are reported. Table 4 shows the descriptive statistics of the variables under study, including mean and standard deviation. The distribution of the sample (225 individuals) indicates that 188 respondents are men (84 percent) and 37 are women (16 percent). Furthermore, 131 individuals (58 percent) in the sample are in the 35–40 age group, 81 individuals (36 percent) in the 41–45 age group, and 13 individuals (6 percent) are over 46 years old. In terms of education, 47 percent of respondents (106 individuals) hold a bachelor's degree, 44 percent (99 individuals) a master's degree, and 9 percent (20 individuals) a doctoral degree. Regarding work experience (university teaching, managerial, and executive roles),

26 percent of respondents (59 individuals) have 5–10 years of experience, 43 percent (98 individuals) have 10–20 years of experience, 28 percent (62 individuals) have 20–30 years of experience, and 3 percent (6 individuals) have more than 30 years of experience.

**Table 4. Demographic characteristics of respondents in the quantitative phase**

| Demographic variables | Variable levels | Frequency | Percentage |
|---|---|---|---|
| Gender | Male | 14 | 63.6 |
| | Female | 8 | 36.4 |
| Age | 35–40 years | 6 | 27.3 |
| | 41–45 years | 8 | 36.4 |
| | 46–50 years | 6 | 27.3 |
| | Over 51 years | 2 | 9 |
| Education | Bachelor's degree | 6 | 27.3 |
| | Master's degree | 16 | 72.7 |
| Work experience | 5–10 years | 4 | 18.2 |
| | 10–15 years | 10 | 45.5 |
| | 16–20 years | 6 | 27.3 |
| | Over 20 years | 2 | 9 |

Next, the fit of the measurement models is assessed through factor loadings and three criteria: Cronbach's alpha, composite reliability, and convergent validity. Since all items have factor loadings greater than 0.40, no item was removed. The values of composite reliability for all constructs are above 0.70, indicating an acceptable level of reliability for the model. Convergent validity examines the extent of correlation between each construct and its indicators, and the average variance extracted (AVE), calculated by the PLS software, is used for this purpose. The acceptable value for AVE is 0.50 or higher. According to the results presented in Table 5, composite reliability and AVE are all within the acceptable range, and thus the adequacy of the reliability, validity, and convergence of the outer relations of the research model can be confirmed.

**Table 5. Fit of the measurement models**

| Variable | Composite reliability (Alpha > 0.7) | Convergent validity (AVE > 0.5) |
|---|---|---|
| Positive and safe organizational culture | 0.792 | 0.491 |
| Social and organizational support | 0.796 | 0.497 |
| Training in stress and fear management | 0.804 | 0.503 |
| Human resource management and motivation | 0.810 | 0.509 |
| Employee empowerment | 0.816 | 0.513 |
| Strengthening a culture of cooperation and solidarity | 0.823 | 0.516 |
| Support of managers and leaders | 0.830 | 0.524 |
| Management of stress arising from environmental crises | 0.834 | 0.536 |
| Monitoring and evaluating the risks of environmental fear in the organization | 0.841 | 0.543 |
| Enhancing coping skills in dealing with fear | 0.844 | 0.547 |
| Improving psychological safety in the workplace | 0.853 | 0.551 |
| Requirements | 0.906 | 0.573 |
| Processes | 0.922 | 0.585 |
| Outcomes | 0.964 | 0.593 |

The research model was tested using the partial least squares (PLS) technique and SmartPLS software. In this model, all relationships were analyzed simultaneously. The research model is then presented in the form of standardized coefficients (t-values). Based on the fitted model, the t-statistic for all paths is greater than 1.96 and the corresponding p-values are less than 0.05, placing them within the acceptable range. Accordingly, based on the fitted model, the path coefficients, standard errors, t-statistics, and p-values are presented in Table 6:

**Table 6. Results of the structural model**

| Path | Path coefficient | Standard error | T-statistic | P-value |
|---|---|---|---|---|
| Positive and safe organizational culture → Requirements | 0.412 | 0.028 | 18.324 | 0.000 |
| Social and organizational support → Requirements | 0.422 | 0.027 | 17.581 | 0.000 |
| Training in stress and fear management → Requirements | 0.487 | 0.004 | 16.661 | 0.000 |
| Human resource management and motivation → Requirements | 0.341 | 0.017 | 15.792 | 0.000 |
| Employee empowerment → Requirements | 0.337 | 0.012 | 14.361 | 0.000 |
| Strengthening a culture of cooperation and solidarity → Processes | 0.317 | 0.014 | 12.488 | 0.000 |

| | | | | |
|---|---|---|---|---|
| Support of managers and leaders → Processes | 0.303 | 0.016 | 13.844 | 0.000 |
| Management of stress arising from environmental crises → Processes | 0.284 | 0.014 | 14.896 | 0.000 |
| Monitoring and evaluating the risks of environmental fear in the organization → Processes | 0.276 | 0.015 | 11.289 | 0.000 |
| Improving psychological safety in the workplace → Outcomes | 0.273 | 0.016 | 12.478 | 0.000 |
| Monitoring and evaluating the risks of environmental fear in the organization → Outcomes | 0.251 | 0.012 | 10.528 | 0.000 |
| Requirements → Processes | 0.134 | 0.017 | 5.124 | 0.000 |
| Processes → Outcomes | 0.121 | 0.005 | 2.883 | 0.004 |

According to the results obtained from Table 6, the t-statistics indicate the significance of the relationships between the variables in the model, as the p-values are less than 0.05. In other words, the significance tests of the path coefficients show that all paths are statistically significant and their effects are confirmed. This means that the components developed in the research model, after removing the above-mentioned paths, enjoy an acceptable level of reliability.

## 6. Discussion and Conclusion

The present study was conducted to examine the deficiencies of the civil liability law in cyberspace and to identify practical solutions for addressing these shortcomings. Given the rapid developments in information and communication technologies, cyberspace has come to be recognized as a new platform for social, economic, and cultural interactions. This new environment has brought unprecedented challenges and opportunities that necessitate the creation and updating of specific laws and regulations. In today's world, compensating for damages arising from misuse and unlawful activities in cyberspace is one of the essential requirements that must be carefully and seriously considered. Yaser Hosseini (2023) emphasizes that civil liability can function as an effective tool in ensuring legal security and can help compensate damages and provide peace of mind for citizens in cyberspace (Hosseini & Rezaei, 2023). Therefore, one of the most important findings of this study is the identification of serious challenges in securing individuals' rights and compensating damages caused by misuse and unlawful actions in cyberspace.

The research showed that the Civil Liability Law in Iran, which was enacted in 1960, is not able to properly address the new challenges arising from modern technologies. For example, liability arising from the dissemination of false information and invasions of privacy has not yet been comprehensively addressed in this law. This clearly demonstrates the law's inability to respond to the ever-growing needs of the information society and further underscores the necessity of serious revision in this area. Hamid Abolhasani and colleagues (2023) likewise emphasize that liability in cyberspace differs significantly from that in the physical world, and that in cases of multiple causes, liability should be imposed jointly and severally on all contributing factors (Abolhasani et al., 2023). These issues can lead to violations of users' rights and the emergence of legal disputes, which in turn highlight the need for revising the relevant laws.

The findings of the study indicate that the existing deficiencies in the civil liability law may result in increased public dissatisfaction and mistrust toward cyberspace. Accordingly, addressing these deficiencies and attempting to resolve them is of great importance. Hasti Rahmani Menshadi (2018) also emphasizes that the state must prevent harmful acts in cyberspace through securing and legally overseeing this environment, and must be responsible for compensating damages if loss occurs (Esmaeili & Rezaei, 2020). If users feel that their rights are not adequately protected, there is a likelihood of reduced online activity and, consequently, a decline in social and economic interactions in cyberspace.

The research model, which was validated using the partial least squares (PLS) method, showed that all relationships between the variables are significant. These results confirm that the components developed in the model possess an acceptable level of reliability and can serve as a solid basis for legal reforms. Qasemi (2021) emphasized in her study the necessity of ethical rules and social responsibilities in cyberspace, which implies the need to establish independent supervisory bodies in this domain (Qasemi, 2021). The existence of such bodies can enhance transparency, accountability, and oversight of online activities, and help restore public trust in cyberspace.

Holding educational courses and specialized workshops for users on their rights and responsibilities in cyberspace is another important implication of this study. Education can help increase users' awareness and reduce legal problems stemming from lack of knowledge. By organizing these courses, users can become familiar with their rights and responsibilities in cyberspace and, consequently, defend their rights more effectively. Overall, this study can be regarded as a scientific and practical reference

for the improvement and reform of the civil liability law in cyberspace, and its findings can assist lawmakers and stakeholders in the fields of law and information technology in taking effective and efficient measures based on a better understanding of the existing challenges.

It is recommended that supportive mechanisms be created for victims of cybercrimes so that they can more easily defend their rights and obtain compensation for the damages incurred. This can improve the legal position of victims and help reduce the negative consequences of cybercrimes. Establishing supportive and counseling institutions for victims of such offenses can assist them in receiving the necessary support when facing problems resulting from these crimes. The use of international experiences in drafting and revising civil liability laws in cyberspace is also emphasized. Other countries have faced similar challenges, and their experiences can be used to improve the legal framework in Iran. These experiences can serve as a basis for drafting new and effective laws and help decision-makers adopt best practices in managing cyberspace.

Paying attention to the social and cultural dimensions of cyberspace and its impact on people's daily lives is another important aspect of this study. Drafting laws that are compatible with this environment, in order to protect individual and social rights and freedoms, is unavoidable. Given the extensive effects of cyberspace on society, it is essential that laws and regulations be formulated in a way that both safeguard users' rights and promote a culture of proper use of this environment. Ultimately, this study hopes to serve as a scientific and practical reference and to take an effective step toward improving and reforming the civil liability law in cyberspace. Such reforms can strengthen the legal security of users and enhance public trust in cyberspace. Therefore, it is necessary for lawmakers and stakeholders in the fields of law and information technology to address these issues with greater seriousness and to take fundamental measures in this regard. In view of the challenges ahead, raising the level of legal awareness and knowledge in this area can help ensure users' rights and improve the quality of cyberspace. Increased awareness enables users to act more consciously when facing legal and social challenges in cyberspace and to better defend their rights.

In addition, future research in this field can help identify new legal and social challenges in cyberspace and develop effective strategies for addressing them. Such studies may lead to the development of new and more suitable legal frameworks that can keep pace with the rapid changes in technology and the needs of society. Finally, it is essential to recognize that cyberspace is a vital arena in today's world. Therefore, drafting comprehensive and efficient laws for managing this environment will help protect users' rights and improve the quality of digital life in society. This will benefit not only users, but also society as a whole and the digital economy.

## 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

Abolhasani, H., Entezari Najaf Abadi, A., & Shari'ati, S. (2023). Imposing Civil Liability on Multiple Causes of Harm in Cyberspace in Iranian Law. *Period*, *5*(4). https://doi.org/10.61838/csjlp.5.4.4

Afshari, A. (2020). Liability Arising from the Violation of Privacy in Social Media. *Journal of Media and Communication Law*, *2*(4), 35-54.

Ahmadi, F., & Nikkhah, R. (2022). The Role of Laws in Protecting Users' Rights in the Digital Space. *Legal Research*, *8*(3), 22-36.

Ahmadi, M. (2016). Criminal and Civil Liability in Cyberspace. *Criminal Law Journal*, *9*(3), 50-72.

Alizadeh, Ḥ. (2022). Legal Challenges of Civil Liability in Cyberspace. *Legal Journal of Gilan University*, *14*(3), 78-93.

Esmaeili, H., & Rezaei, M. (2020). Civil Liability in Cyberspace: Challenges and Solutions. *Journal of Information Technology and Communication Law*, *4*(2), 45-62.
Farahbod, M., Tabibi, S. J. a.-D., Kamali, M., & Masoudi Asl, I. (2023). Comparing the rehabilitation structure in the health systems of Iran, Germany, Japan, Canada, Turkey, and South Africa: A comparative study. *Rehabilitation Quarterly*, *94*, 101-113. https://doi.org/10.32598/RJ.24.1.3582.1
Habibi, M. (2020). *Civil Liability of Advertising in Cyberspace*.
Hosseini, M., & Rezaei, N. (2023). Legal Analysis of Civil Liability in Cyberspace. *Iranian Law Journal*, *12*(2), 45-60.
Hosseini, N. (2021). Comparative Analysis of Civil Liability in Cyberspace in Iranian Law and International Law. *Journal of Comparative Law Studies*, *13*(1), 88-110.
Ja'fari, M. (2018). *Civil Liability Arising from the Dissemination of False Information in Cyberspace*.
Karimi, M. (2022). *Legal Challenges of Civil Liability in Cyberspace*.
Kazemi, F. (2021). *Principles of Civil Liability in Iranian Law and its Application in Cyberspace*.
Malakuti, R. (2022). Investigating the Pillars for the Realization of Civil Liability in Cyberspace. *Cyberspace Law Studies*, *1*(3), 69-79.
Malakuti, R., & Khalilzadeh, M. (2023). *Investigating the Dimensions of Civil Liability for the Violation of Intellectual Property and Trademarks in Cyberspace*.
Naderi, S. (2018). Investigating Civil Liability Arising from the Violation of Privacy in Cyberspace. *Journal of Private Law*, *12*(4), 120-138.
Niknam, H. (2021). *Civil Liability Arising from the Violation of Privacy in Cyberspace*.
Qasemi, Z. (2021). Analysis of Civil Liability of Virtual Platforms in the Iranian Legal System. *Justice Legal Journal*, *86*(3), 112-130.
Qorbani, M. (2022). Legal Challenges of Civil Liability in Cyberspace. *Legal Studies Quarterly of Yazd University*, *16*(1), 23-38.
Rezaei, A. (2017). *Internet Law and Civil Liability*.
Sharifi, A. A., Shafahi, S. Ḥ., Almasi, N. A., & Savara'i, P. (2023). Civil and Ethical Liability Focused on the Violation of Personality Rights in Cyberspace. *Journal of Ethics in Science and Technology*, *3*(18), 84-91.
Zahedi, H. (2017). *Information Technology Law and Civil Liability*.