Civil Liability of Content Producers and Providers in Cyberspace

1. Mohammad Sadeq Borzou: Department of Private Law, Shi.C., Islamic Azad University, Shiraz, Iran
2. Hekmatollah Askari*: Department of Law, Shi.C., Islamic Azad University, Shiraz, Iran
3. Zohreh Farrokhi: Department of Law, Shi.C., Islamic Azad University, Shiraz, Iran

*Correspondence: hekmat_askari@iaushiraz.ac.ir

Abstract

Technological advancement has rendered the influence of cyberspace on human life undeniable, and its significance continues to increase daily. Content is the central element of cyberspace. The growing use of cyberspace, on one hand, and the potential ability of content to cause harm to individuals, on the other, have heightened the necessity for legislative attention to this domain. Given that the actors in cyberspace can be broadly categorized into two main groups—content producers and providers, and ordinary users—civil liability arising from the production and dissemination of defective content pertains primarily to the first group (i.e., producers and distributors of content). This is because ordinary users generally play no role in causing damage. However, in situations where an ordinary user could prevent the occurrence or expansion of damage but fails to do so, the resulting harm will not be compensable due to the absence of customary attribution of the damage to the producer or provider of content, as well as in light of the legal maxim of "act of intervention". Furthermore, in cases where multiple producers and providers contribute to the production and distribution of defective content, liability for damages must be apportioned among them in accordance with the extent of their individual contributions.

Keywords: Civil liability, content, cyberspace, content producers and providers

Received: 20 January 2025
Revised: 01 April 2025
Accepted: 08 April 2025
Published: 17 June 2025

Citation: Borzou, M. S., Askari, H., & Farrokhi, Z. (2024). Civil Liability of Content Producers and Providers in Cyberspace. *Legal Studies in Digital Age,* 4(2), 1-10.

1. Introduction

The growing use of cyberspace and the dominance of technology over daily human life have led many characteristics of traditional society to migrate into the digital domain. Despite its numerous benefits, cyberspace also presents significant challenges. One of the most critical issues in this realm is civil liability. Civil liability in cyberspace is particularly important because the cyber environment differs fundamentally from the real world, and its actors are generally categorized into two broad groups: internet intermediaries (in the broad sense) and users (Bert, 2012; Malekouti & Saurabi, 2016).

Internet intermediaries typically facilitate access to the Internet for others and may also provide ancillary services such as website management or content production. It is important to note, however, that content producers or providers are not always intermediaries; rather, users themselves may also, in certain circumstances, generate and disseminate content in cyberspace (Cutlip et al., 2006; Elkin Koren, 2006).

One of the key challenges regarding civil liability in cyberspace relates to the legal consequences of disseminated content. Specifically, if a piece of data is defective and causes harm due to its defect, how should compensation be administered, and how should fault be established? Furthermore, if one person produces defective data and another distributes it, who bears responsibility? Additionally, if another individual plays a role in promoting it, but only within a very short timeframe, how should civil liability be calculated for these actors? This article addresses these pressing questions (Rahpeyk, 2011; Zabarjad & Khorsandian, 2023).

2. The Concept of Content Producers and Providers

“Content” has recently been examined from various disciplinary perspectives and has garnered attention across multiple scientific fields. Legal studies are no exception; legal scholarship has increasingly explored both the definition and different dimensions of content (Boiko, 2005). According to the Oxford Dictionary, content is, in a literal sense, "something that is contained within something else." From a terminological standpoint, content is defined as information made available by a website or other electronic medium ("Oxford Dictionary, Content," 2016).

Various scholars in different disciplines have also offered definitions of content. For instance, in the field of communication, content is understood as a message that holds meaning and relevance for its recipient. Another definition describes content as data and functionalities that are structured and organized for specific purposes (Boiko, 2005).

In Iranian law, Clause (a) of Article 1 of the "Bylaw for Organizing and Developing Digital Cultural Media" (No. 172412T41255H) defines content as "visual, audio, written, or a combination of these in any form or format." Based on this definition, news, commercial advertisements, games, entertainment, and similar items can all be categorized as digital content. However, this definition merely addresses the form of content and makes no attempt to explain its nature. It seems more appropriate to define content as anything that conveys a message, news, emotion, or similar information to others through visual, auditory, written, or mixed forms and in any format. Accordingly, content can be transmitted via a variety of media, including text, images, audio, video, the Internet, television, or even a live theater performance (Boiko, 2005; Cutlip et al., 2006).

Given this conceptualization of content, content producers and providers are those individuals or entities that engage in creating and distributing content. Accordingly, a content provider is someone who produces and stores information in digital space. Content creation may be undertaken by individual users or institutional providers. Clause 1 of Article 2 of the "Bylaw on Information Service and ISP Units" defines a service provider as follows: “The activities of ISP (Information Service Provider) companies and institutions are carried out under the specific regulations and laws in force in the country and may operate independently or in conjunction with the internet network to offer information technology services to users” (Alsan, 2014; Smith, 2002).

3. Objectives of Civil Liability for Content Producers and Providers in Cyberspace

One of the shared goals across liability systems is deterrence. In the domain of civil liability as well, deterrence is recognized as a central objective. Accordingly, another purpose of civil liability is realized through the punishment and private sanctioning of the liable party by the injured party through the imposition of liability. This is because the perpetrator, through their harmful act, has infringed upon the legitimate interests of the injured party. Imposing liability not only compels the wrongdoer to bear the consequences of their harmful actions but also encourages more cautious behavior and discourages the repetition of such actions in the future (Katouzian, 2005; Rahpeyk, 2011).

In addition to deterrence, which is a shared and significant goal of civil liability, the primary and most essential aim is compensation for damages. However, as noted, compensation is not the sole objective of civil liability, nor is the requirement that the wrongdoer pay a sum of money to the injured party always sufficient to restore the loss incurred.

Compensation in civil liability plays not only a key role in preventing the wrongdoer from repeating harmful conduct but also in deterring others in society from engaging in similar harmful behavior. A critical issue in this regard is the determination of appropriate criteria for assessing the amount of damage and identifying the recoverable harm (Badini, 2015).

From an economic standpoint, lower compensation incentivizes more careless behavior, thereby increasing the recurrence of harm in society. Raising the compensable amount—for example, through recognizing indirect damages—can reduce the frequency of negligent acts and even mitigate the very occurrence of harm. Thus, the level of compensation becomes a variable that influences the degree of harm generated by individuals. The impact of potential compensation on the extent of harm also depends on their substitutability (Zabarjad & Khorsandian, 2023).

For instance, if a producer becomes aware of a defect in their product after its release but takes no steps to rectify it, and if the potential damages awarded are less than the cost of recalling and repairing the defective products, a court ruling for compensation will likely have little effect on deterring such violations. In this case, the demand for such misconduct is inelastic. Conversely, if potential damages exceed the cost of recall and repair, the judgment will likely discourage future violations, making demand for such misconduct elastic. This leads us to the concept of rational negligence in consumer law (Posner, 1998).

To explain the role of rational negligence, it must be stated that the effectiveness of legal remedies depends on the expected compensation available to the victim. If the victim, due to the low potential for recovery, decides not to pursue legal action, the legal sanction against the offender becomes ineffective. This often occurs in cases of minor damages resulting from product defects, where the overall harm suffered by the individual is negligible compared to the total possible harm. Rational negligence is also prevalent in civil liability cases involving cyberspace, particularly in relation to data repositories (Zabarjad & Khorsandian, 2023).

Accordingly, in assessing compensable harm in cyberspace, a distinction must be made between an ordinary user and a content producer. If a defective or false dataset is created by either a user or a data platform, their differing purposes must be taken seriously. Although both are liable to compensate for damages, the platform typically operates for profit and derives financial gain, whereas the ordinary user lacks such intent or gain. Therefore, applying identical legal consequences to both groups may fail to achieve the goals of civil liability (Malekouti & Saurabi, 2016).

To ensure and preserve the deterrent function of civil liability, both parties should be obliged to compensate for the damages inflicted. However, any financial gain obtained by the platform through the dissemination of defective content should be reclaimed as either damages or as unjust enrichment. This approach eliminates the incentive to infringe on others' rights through harmful content distribution. Otherwise, the platform may view civil liability as a mere cost of doing business, and the compensation awarded may be negligible compared to the profits gained (Alsan, 2014).

In other words, civil liability laws applicable to cyberspace require critical analysis and, if necessary, revision. One of the defining features of any law in the modern world is effectiveness. As Immanuel Kant, the Western philosopher and founder of modern legal thought, asserts: “It is not important that the best law be enacted; what matters is that the law be aligned with the nature of the people. In reality, the best law is the most efficient and applicable one.” Based on this perspective, efficiency is more vital than any other element in modern legal systems, and lawmakers must draft effective laws based on the public’s intellectual and social maturity, since it is the people who ultimately enforce the law (Rousseau, 1962; Taylor, 2006).

Efficiency, in this context, means performing tasks in the best possible manner with optimal outcomes, minimizing waste of time, energy, and resources. Economics defines efficiency as producing the highest output from minimal inputs. Similarly, effectiveness is defined as the degree to which predetermined goals are achieved.

From an economic perspective, legal rules function as instruments for “behavior modification” and “policy-making.” Therefore, the prevailing attitude in economic analysis of law emphasizes the use of economic principles—especially efficiency—in legal decision-making (Zabarjad & Khorsandian, 2023).

In an effort to align legal frameworks with the cyber environment, various foreign legal systems and international instruments have reoriented their approaches to enhance compatibility and efficiency. For example, in civil liability, causality has always been a prerequisite. Thus, if an employee discloses confidential information without a clear agreement of confidentiality with the employer, civil liability may not be imposed. However, if such disclosure constitutes a criminal offense based on customary expectations, then civil liability becomes easier to prove. Moreover, losses such as data deletion may be either unquantifiable or severely undervalued in civil liability terms. In such cases, recognizing criminal liability serves as an effective means to minimize intrusions upon legitimate rights and assets (Elkin Koren, 2006; Smith, 2002).

In the 1980s and 1990s, many countries refused to recognize data as a form of property, largely on the grounds of its intangible nature. However, with the emergence of virtual goods such as online games and virtual worlds, which clearly hold monetary value, the classification of data as property has re-emerged. The Dutch Supreme Court has recently ruled that, under certain conditions, stealing such virtual goods may constitute theft ("Dutch Supreme Court [Hoge Raad] 31 January 2012, LJN BQ9251," 2012).

Moreover, the Council of Europe's Convention on Cybercrime (Budapest Convention), in Article 2 of Chapter II titled *"Illegal Access,"* defines unauthorized access—such as hacking or cracking—as a criminal offense. While Iranian law also recognizes unauthorized access as a crime under Article 1 of the Computer Crimes Act, it imposes additional conditions not found in the European Convention. One such condition is the existence of protected security measures for safeguarding data. Article 1 stipulates: "Anyone who unlawfully accesses computer or telecommunications systems or data protected by security measures shall be sentenced to imprisonment for a term of 91 days to one year, or a fine of 5,000,000 to 20,000,000 Rials, or both." By contrast, the Budapest Convention does not require such a condition; mere unauthorized access to a system or its data constitutes a criminal offense ("Convention on Cybercrime, Budapest, 23 November 2001, CETS 185," 2001).

4. Elements of Civil Liability for Content Producers and Providers in Cyberspace

The elements of civil liability for content producers and providers in cyberspace parallel those of traditional civil liability. In the context of cyberspace, four essential elements must be satisfied to establish civil liability: (1) the existence of a duty or obligation, (2) breach of that duty, (3) the occurrence of harm, and (4) a causal relationship between the breach and the resulting harm. However, given that in tort law the existence of an explicit obligation is not as central as in contractual liability, these elements may be condensed into the following three core components:

1. A wrongful (harmful) act
2. Compensable damage
3. A causal link, as recognized by social norms, between the wrongful act and the harm

On this basis, if defective or dangerous content causes harm to a buyer or third party, and the above elements are present, the resulting damages are eligible for compensation (Katouzian, 2005; Rahpeyk, 2011).

A noteworthy consideration in establishing liability for defective content is the role of the injured party in the occurrence of the harm. That is, while in some cases defective content directly targets the reputation of the injured party and causes significant harm, in many other instances the content merely sets the stage for damage, without a causal connection between the harmful act and the damage.

Therefore, civil liability is not established in every instance where harm occurs. Rather, the harmful conduct must be considered socially objectionable, and public morality must recognize the harm as wrongful. Furthermore, a reasonable and customary link must exist between the production or dissemination of defective content and the harm incurred (Badini, 2015).

According to the principle of innocence and the maxim *"al-bayyina 'ala al-mudda'i"* (the burden of proof is on the claimant), the plaintiff bears the burden of proving causation. As there is no fixed standard for attributing harm to the producer or distributor of defective content, the judge may rely on surrounding circumstances and available evidence to ascertain the truth (Khorsandian & Sharai, 2016; Zabarjad & Khorsandian, 2023).

5. Basis of Liability for Content Producers and Providers

Although there is relatively little debate regarding the liability of actors in the digital currency sphere—such as ISPs and website administrators—owing to the provisions of Clause 4-3-5 of the 2001 Bylaw on Internet Information Service Providers (ratified by the Supreme Council of the Cultural Revolution), and given the absence of supervisory roles for administrators regarding approval or correction of online content, their liability is typically grounded in fault-based theory. However, determining the basis of liability for content producers and providers is more complex (Alsan, 2014; Malekouti & Saurabi, 2016).

This complexity arises from the fact that these actors merely make defective, incomplete, or illegal content publicly available. Liability does not arise unless users actually download the content. Based on this nuance, some scholars argue that the act of uploading the content alone is sufficient to incur civil liability for content producers and providers. In other words, their liability stems from the very act of making the content accessible to the public, regardless of whether it is ever downloaded. Accordingly, their liability may be characterized as strict or absolute liability (Elkin Koren, 2006).

Even though users do not receive defective or illegal content unless they voluntarily download it, this does not exempt the producer or provider from liability. This interpretation also appears to be endorsed by the Iranian legal system. Supporting this view, Clause 5-3-1 of the same 2001 bylaw explicitly states: "Institutions and companies offering ISP services and users are responsible and accountable under this bylaw for the content they publish on the network." A similar rationale is observable in Article 74 of the Electronic Commerce Law, which treats the publication and distribution of another's work in cyberspace as equivalent acts, using both terms interchangeably (Smith, 2002).

Some legal scholars who have examined civil liability in cyberspace consider the liability of content producers and providers to be a form of strict liability, asserting that:

"…regarding the basis of liability for this group, one must adopt a strict liability regime for content providers in cyberspace, as the nature of their conduct inherently results in harm. The mere act of making content available in cyberspace enables millions of users across the world to access it, and the possibility of removal or restricting access is nearly impossible. Subsequent actions by users typically do not contribute significantly to the harm. According to custom and technological realities of cyberspace, merely posting harmful content is considered equivalent to causing harm, and the act of posting is viewed as a form of publication in and of itself." (Bert, 2012; Zabarjad & Khorsandian, 2023).

6. The Scope of Civil Liability for Content Producers and Providers in Cyberspace

Another major challenge in the field of civil liability in cyberspace is clarifying the scope of liability for content producers and providers, as well as the extent of compensable damages.

Consider a case where a person suffers harm as a result of defective data generated by another party in cyberspace. If the injuring party had the ability to control or mitigate the damage but deliberately refrained from doing so, can the principle of "voluntary assumption of risk" (qāʿidah-ye eqdām) be invoked to limit liability? Put differently, when a content producer is found liable for damages caused by defective content, should the compensation be full or limited? An example of this issue appears in Iranian law in Note 3 of Article 8 of the 2016 Third Party Liability Insurance Act, which explicitly recognizes the concept of limited compensation.

Prior to the enactment of this 2016 statute, only minor exceptions to the principle of full compensation were recognized. However, with its ratification, the notion of full and unrestricted compensation encountered a significant legal exception. According to Note 3 of Article 8: "Financial damages resulting from traffic accidents shall only be compensable up to the amount corresponding to the damage inflicted on the most expensive conventional vehicle, either through third-party insurance or by the at-fault party." This provision, when read in conjunction with Note 4—which defines the term "conventional vehicle"—places a substantive and formal limitation on the principle of full compensation (Rahpeyk, 2011; Zabarjad & Khorsandian, 2023).

Given the precedent of limiting full compensation in Iranian civil law, based on considerations such as equity and public interest—notably found in Article 4 of the 1960 Civil Liability Act—it appears that the foundation for such limitation in the Third Party Insurance Act may also rest on the principle of voluntary assumption of risk or public order (naẓm-e ʿomūmī). The latter is particularly relevant because public order is widely understood in both civil law and comparative legal systems to

prioritize the collective interests of society. Where individual interests conflict with communal welfare, public order dictates that collective interests prevail. However, since the concept of public interest is not absolute and varies by time and context, what constitutes public order in one legal era or jurisdiction may not apply identically in another (Khorsandian & Sharai, 2016; Rousseau, 1962).

As can be seen from the 2016 Third Party Insurance Act, the rationale for limiting full compensation is grounded in the principle of assumption of risk. But this raises the question: in cases of civil liability involving content producers in cyberspace, does the injured party bear any duty? For example, could the victim have reduced or prevented the damage by conducting further investigation into the content, issuing a disclaimer, or exercising reasonable caution—especially if the falsity of the information was discernible upon further examination?

It appears that the principle of assumption of risk could indeed be applicable—particularly in situations where the injured party relied on a news item and suffered harm. Therefore, by analogy with Note 3 of Article 8 of the Third Party Insurance Act, one might argue that a portion of the loss should be attributed to the victim, as a means of preventing negligence or imprudence. In fact, such a limitation on full compensation may be even more justified in the context of cyberspace liability, since it serves a deterrent function that is not explicitly present in the insurance law itself (Posner, 1998; Zabarjad & Khorsandian, 2023).

7. Conclusion

Although the foundational basis of civil liability in cyberspace remains largely aligned with traditional legal doctrines, the unique nature of the digital environment necessitates revisiting and updating certain principles. While maintaining the theoretical underpinnings of civil liability, the legal framework must be adapted to the realities and complexities of cyberspace.

In cases where the mere act of producing defective content causes harm (such as creating faulty software), the producer will bear liability. However, if the production alone does not directly cause harm (e.g., reputational loss), then not only the producer of the defective or false content but also the party that disseminated it may be held liable.

If an individual is involved in the dissemination of defective or false content during a specific time frame, their liability will depend on both the duration and scope of their involvement—especially considering whether the actor is an ordinary user or a professional operating on a broader scale.

If the injured party had the capacity to prevent or mitigate the damage, then based on the principle of assumption of risk and by analogy to Note 3 of Article 8 of the 2016 Third Party Insurance Law, a portion of the damage may reasonably be borne by the injured party to deter imprudent behavior.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Ethical Considerations

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

Acknowledgments

Authors thank all individuals who helped us do 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

Alsan, M. (2014). *Cyber Space Law*. Shahr-e-Danesh Publishing.
Badini, H. (2015). *Philosophy of Civil Liability*. Sherkat Sahami Enteshar.
Bert, J. K. (2012). Criminal law and Cyberspace as a Challenge for Legal Research. *SCRIPTed*, *9*(3). https://doi.org/10.2966/scrip.090312.354
Boiko. (2005). *Content management bible*. Wiley.
Convention on Cybercrime, Budapest, 23 November 2001, CETS 185. (2001).
Cutlip, S. M., Allen, H. C., & Glen, M. B. (2006). *Effective public relations*. Pearson Prentice Hall.
Dutch Supreme Court [Hoge Raad] 31 January 2012, LJN BQ9251, (2012).
Elkin Koren, N. (2006). Making technology Visible: liability of Internet Service Providers for Peer to Peer Traffic. *New York University Journal of Legislation and Public Policy*, *9*.
Katouzian, N. (2005). *Non-Contractual Obligations: Tort Liability* (Vol. 1). University of Tehran Press.
Khorsandian, M. A., & Sharai, E. (2016). *The Rule of Non-Interference in the Scope of Islamic Private Law*. Gostaresh Rayaneh.
Malekouti, R., & Saurabi, P. (2016). An Introduction to Civil Liability in Cyberspace. *Quarterly Journal of Private Law Research*, *4*(15).
Oxford Dictionary, Content. (2016). http://www.oxforddictionaries.com/definition/english/ content?q=content
Posner, E. A. (1998). Standards, Rules, and Social Norms. *Harv. J. L. & Pub. Pol'y*, *21*.
Rahpeyk, H. (2011). *Civil Liability Law and Remedies*. Khorsandi Publishing.
Rousseau, J.-J. (1962). *The Social Contract*. University of Tehran Press.
Smith, G. J. H. (2002). *Internet Law and Regulation*. Sweet and Maxwell.
Taylor, M. (2006). *International Competition Law: A new pimension for the wto?* university press. https://doi.org/10.1017/CBO9780511494574
Zabarjad, S. F., & Khorsandian, M. A. (2023). A New Perspective on Economic Analysis of Law in Light of the Islamic Jurisprudential Rule of Non-Interference. *Islamic Jurisprudence and Law Studies*, *14*(28).