

# Foundations of Civil Liability for the Violation of Privacy in Cyberspace in Imamiyyah Jurisprudence and Iranian Law

1. Jamshid Ebrahimi Ramandi<sup>1</sup>: PhD Student, Department of Private Law, Emirates Branch, Islamic Azad University, Dubai, United Arab Emirates

2. Tayeb Afsharnia<sup>2</sup>: Department of Private Law, WT.C., Islamic Azad University, Tehran, Iran

3. Ebrahim Yaqoti<sup>3</sup>: Department of Islamic Jurisprudence and Law, CT.C., Islamic Azad University, Tehran, Iran

\*Correspondence: Afsharnia59@gmail.com

## Abstract

Privacy, as one of the fundamental rights of individuals, is protected both in legal systems and in Islamic jurisprudence. Violation of this right may lead to civil liability, the foundations of which can be examined within jurisprudence and law. In the jurisprudential system, principles such as the rule of no harm (*qā'idat lā ḍarar*), the principle of respect for the believer's privacy, the principle of respect for human dignity, the principle of correctness (*aṣālat al-ṣiḥḥa*), the principle of generality of permission (*'umūm al-idhn*), and the rule of causation (*qā'idat al-tasabbub*) emphasize the necessity of observing privacy and compensating for damages resulting from its violation. These rules demonstrate that any unauthorized intrusion into individuals' private space is prohibited in jurisprudential terms and entails liability. In the legal system, three main theories have been proposed to explain civil liability arising from the violation of privacy. The fault-based liability theory considers the establishment of liability contingent upon proving the fault of the offending party. The risk-based liability theory deems the mere occurrence of damage sufficient to establish liability without the need to prove fault. Finally, the theory of right-guarantee treats privacy as a fundamental right and regards its violation, without the need to prove fault or risk, as sufficient grounds for civil liability. The examination of these foundations, based on a descriptive and analytical research method, shows that in both Islamic jurisprudence and positive law, the violation of privacy is deemed unacceptable, and necessary safeguards for compensating damages have been foreseen. This reflects the significance of protecting this fundamental right and the necessity of adopting effective legal and religious measures to prevent its violation and to compensate for the resulting harm.

**Keywords:** civil liability, violation of privacy, rule of no harm, principle of respect for the believer's privacy, fault theory, risk theory, right-guarantee theory.

Received: 12 August 2024

Revised: 01 September 2024

Accepted: 13 September 2024

Published: 19 October 2024



**Copyright:** © 2024 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

**Citation:** Ebrahimi Ramandi, J., Afsharnia, T., & Yaqoti, E.. (2024). Foundations of Civil Liability for the Violation of Privacy in Cyberspace in Imamiyyah Jurisprudence and Iranian Law. *Legal Studies in Digital Age*, 3(4), 148-158.

## 1. Introduction

The development of cyberspace, like all other advancements in human life, has been accompanied by both positive and negative consequences. One of the negative consequences is the endangerment of individuals' privacy, while one of the positive outcomes is the facilitation and acceleration of communication and information exchange. Privacy is of such importance that

respect for it has gone beyond the traditional boundaries of religion and ethics and has found legal guarantees in most countries around the world. However, with the expansion of the web, this right has been subjected to serious and transnational threats. On the other hand, a new platform has emerged for the creation of cyber public and private environments and their appropriate utilization.

Privacy is one of the significant topics in the realm of individual and social rights, which, with the expansion of modern life and the development of information technologies, has acquired more complex dimensions. While the protection of this right has been emphasized in legal and jurisprudential systems, multiple challenges persist regarding its definition, boundaries, and the determination of its legal guarantees. One of the most crucial issues in this field is identifying the foundations of civil liability for the violation of privacy, which can be analyzed based on various jurisprudential principles and legal theories.

In Iranian law, privacy is recognized as one of the fundamental rights of individuals, and the legislator has attempted to protect this right through the enactment of various regulations and laws. However, due to the complexities of cyberspace and its rapid developments, existing laws may be insufficient in some cases. In Imamiyyah jurisprudence, privacy also holds significant ethical and religious value, and discussions have been raised regarding the scope and conditions of its protection. In contrast, the legal system of the United Kingdom, by drawing on its extensive experience in common law and human rights law, has developed specific frameworks for the protection of privacy in cyberspace.

The key questions that the authors aim to address are as follows: What are the boundaries and instances of privacy violation from the perspectives of jurisprudence and law? What jurisprudential and legal foundations exist for civil liability in this field? And to what extent can these foundations meet the needs of contemporary societies? Exploring these questions can contribute to a better understanding of the position of privacy in legal and jurisprudential systems and the manner in which legal guarantees are implemented to protect this right.

## 2. Jurisprudential Foundations

In the Islamic legal system, civil liability resulting from the violation of privacy is based on solid jurisprudential principles and rules, each of which addresses different dimensions of protecting individuals' rights against unjust intrusions. Given the importance of safeguarding privacy in human societies, the jurisprudential foundations of this liability can be found in principles and rules such as the rule of no harm (*qā'idat lā ḍarar*), the principle of respect for the believer's privacy, the principle of respect for human dignity, the principle of correctness (*aṣālat al-ṣiḥḥa*), the principle of general permission (*'umūm al-idhn*), and the rule of causation (*qā'idat al-tasabbub*). Accordingly, this collection of principles and rules provides a robust framework for establishing civil liability in the face of privacy violations and demonstrates that, in Islamic jurisprudence, protecting privacy is not only an individual right but also a religious and social obligation.

### 2.1. The Rule of No Harm (*Qā'idat Lā Ḍarar*)

The rule of "*lā ḍarar*" is one of the important jurisprudential rules that serves as the basis for civil liability and compensation in Islamic jurisprudence. According to this rule, causing harm or damage to others without legitimate religious authorization is unlawful, and compensation for the damage is obligatory. This rule originates from the Prophetic hadith "*lā ḍarar wa lā ḍirār fī al-Islām*," meaning that Islam does not permit one to harm or cause harm to another, and in the case of such harm, compensation must be provided.

The Qur'an contains several verses that confirm the rule of no harm: "And do not harm them [your divorced wives] so as to oppress them" (Qur'an, Surah Al-Talaq, Verse 6), which forbids men from harming divorced women during their waiting period. "After fulfilling the bequest he may have made or a debt, provided that no harm is done [to the heirs]" (Qur'an, Surah Al-Nisa, Verse 12), which prohibits wills or debts that harm heirs. "No scribe should be harmed, nor any witness" (Qur'an, Surah Al-Baqarah, Verse 282). These verses collectively establish that causing harm to others is forbidden and illegitimate.

The intended meaning of "*lā ḍarar wa lā ḍirār*" is that there is no injurious ruling from the legislator. As Behrami Ahmadi (2011) states, "In the wisdom of Islamic law, just as it is obligatory for the legislator to negate injurious rulings, it is also obligatory to legislate rulings whose absence would cause harm." (Behrami Ahmadi, 2011). Therefore, any legal ruling from the legislator that results in harm to the people must be negated based on the rule of no harm—for instance, the obligation of ablution (*wudu*) for someone for whom the use of water is harmful (Mohammadi, 2020).

Thus, the illegitimacy of harm must be considered both at the legislative and implementation stages. The general negation of harm is included within the scope of this rule. Undoubtedly, the rational consensus in all legal systems confirms the necessity of avoiding harm in social relations and considers the one causing harm to be liable for compensating the victim.

With the expansion of cyberspace, new issues have arisen concerning privacy and the security of personal information. The violation of individuals' privacy in this realm can occur in various forms, such as unauthorized access to personal data, disclosure of sensitive information, or the use of data for commercial purposes. The rule of no harm clarifies the civil liability of those who violate privacy and mandates compensation for the harm caused.

Based on the rule of no harm, if the government, through the implementation of filtering policies, causes unjustified harm to citizens, it may bear civil liability for compensating such damages. For instance, if filtering is carried out without valid justification or based on vague and unfair laws, and businesses or individuals suffer losses, the government would be obligated to compensate such damages under this rule. However, if the government can prove that filtering was intended to prevent greater harm and protect public safety and interests, it may be exempted from civil liability. In this regard, a precise analysis of the circumstances and the extent of harm caused to citizens, as well as the purpose and necessity of content filtering, plays a decisive role in determining the government's responsibility (Mohammadi Nia & Karamati Moaz, 2024).

This rule can serve as the basis for legislation aimed at protecting privacy in cyberspace and determining the civil liability of individuals and institutions that access or disclose personal data without authorization. Accordingly, rules developed based on the principle of no harm can prevent violations of individuals' privacy and, in case of infringement, provide a legal path for damage compensation.

Therefore, the rule of no harm provides a jurisprudential and legal framework through which the civil liability of privacy violators in cyberspace is recognized, and compensation for damages becomes a necessity. This rule not only serves as a tool for protecting the personal rights of cyberspace users but also plays a crucial role in the formulation and enforcement of privacy protection laws and can contribute to improving information security in the digital space.

## 2.2. *The Principle of Respect for the Believer's Privacy*

Although privacy is recognized in the modern world as an individual and human right, it had already been considered in many societies and cultures. Certain Qur'anic verses also reflect attention to this concept, even if the term "privacy" is not explicitly mentioned. For example, Surah Al-Hujurat, verse 12, prohibits spying and inquisitiveness; Surah Al-Nisa, verse 29, refers to the prohibition of eavesdropping and encroachment upon personal property; and Surah Al-Nur, verse 27, as well as Surah Al-Baqarah, verse 189, address the prohibition of entering homes without permission. These meanings have also been strongly emphasized in various narrations by the Prophet and the Imams.

The principle of respect for the believer's privacy in Islamic jurisprudence is based on the idea that Muslims are obligated to preserve and respect each other's sanctity in both personal and social domains. This principle particularly emphasizes the protection of dignity, character, and private rights, and regards intrusion into personal privacy as an improper and unjust act. It is one of the fundamental jurisprudential principles underpinning civil liability for the violation of privacy and holds unique relevance in cyberspace.

In the sight of God, the sanctity of a believer is as significant as the sanctity of the Prophet, his family, the Qur'an, and the Kaaba (Kulayni, 2008). A Muslim's life is sacred in Islam; thus, no one may inflict harm, such as physical injury, food poisoning, or any act endangering a person's health. In Islamic jurisprudence, a rule known as *ḥurmat dam al-muslim wa mālihi wa 'irdihi*—the inviolability of the blood, property, and honor of a Muslim—emphasizes the sanctity of life, wealth, and dignity (Mousavi Khalkhali, 1997). A Muslim's property is considered as sacred as their life and blood (Tusi, 2008).

The honor and dignity of individuals in Islam enjoy a high level of immunity and sanctity, falling under *ḥaqq al-nās* (the rights of people). This categorization extends the protection of privacy beyond believers, making it applicable to all individuals. Consequently, the reputation of all people is respected in Islam, establishing a barrier against encroachments on their honor and dignity. Thus, the principle of respect for individuals forms the first foundation of privacy in Islam. Given the broad meaning and instances of this principle, the respect for a believer also encompasses both personal privacy in real life and the privacy and information of individuals in cyberspace (Seyyed Saadati, 2013).

The foundation of respect covers both the material aspects of privacy and those related to moral and spiritual dignity. In addition to views that justify privacy based on human dignity, theories in foreign legal systems that try to ground privacy in property rights and material ownership (assuming their validity) are also justifiable under this principle. Since the principle of respect is one of Islam's *imḍāʾī* (endorsed) rules and is based on rational consensus, it can serve as a universal and non-religious principle and support various views in comparative legal systems (Badini et al., 2020).

Beyond protection and preservation of privacy, the foundation of respect implies, by either explicit or implicit meaning, the necessity of compensating for damages. Exceptions and permissible breaches of user rights in cyberspace can also be justified on the basis of respect. Accordingly, certain instances such as public sinfulness or consent (in matters of right) are excluded *specifically*, while others, like overriding public interest or judicial orders, are excluded *particularly*, depending on the case. When respect pertains to the financial aspects of privacy, it is generally considered a “right,” while in cases involving dignity or human honor, it is treated as a “rule” (Qanavati & Javar, 2011).

The principle of respect for the believer's privacy can serve as an important foundation for legislating privacy protection laws in cyberspace. It can be used as a standard to prevent unauthorized access or disclosure of personal information and provide a pathway for civil liability and compensation in cases of violation.

As one of the moral and jurisprudential principles, the principle of respect for the believer's privacy offers a strong framework for civil liability regarding the violation of privacy, especially in cyberspace. This principle not only mandates protection of individuals' privacy and honor but also places the burden of compensation on the violator in case of infringement. Thus, considering this principle in drafting cyberspace regulations can contribute to better protection of private rights and enhance data security.

### 2.3. The Principle of Respect for Human Dignity

The concept of dignity is one of the most prominent values in human life as it defines the status of human beings, and the safeguarding of all human possessions is contingent upon honoring their dignity. This respect entails honoring all human attributes. The principle of intrinsic and ontological dignity of human beings is widely accepted, at least in essence, by the majority of scholars regardless of its scope (Mowhidd, 2002).

Various opinions exist regarding the rationale behind human dignity, stemming from differing views on the essence and nature of humanity. Among Muslim scholars, the most prominent justification for human dignity is that man is God's vicegerent and possesses a comprehensive existential nature (Badini et al., 2020). God has attributed dignity to humans and honored the Children of Adam since creation, elevating them above other beings: “Indeed, We have honored the Children of Adam, carried them on land and sea, provided them with good things, and preferred them above many of those whom We created” (Qur'an, Surah Al-Isra, Verse 70). Also, despite being created from clay, man was made worthy of angelic prostration due to possessing a divine spirit: “And I breathed into him from My spirit” (Qur'an, Surah Al-Hijr, Verse 29).

The principle of respect for human dignity is a fundamental norm in Islamic jurisprudence and ethics, emphasizing the inherent value and sanctity of every human being. In the context of civil liability for privacy violations in cyberspace, this principle can provide a strong foundation for the protection of individuals' rights and the assurance of compensation for resulting harms. According to this principle, human beings, as honored creations of God, possess inherent dignity, and preserving this sanctity is obligatory in all areas of life, including cyberspace. Therefore, any violation of privacy in this realm is considered a breach of human dignity and honor.

In cyberspace, human dignity and status must be observed, and any action that endangers intrinsic human morals is deemed forbidden. Respect for human dignity demands that personal privacy be respected and that any intrusion—whether communicational, spatial, informational, or physical—contradicts this principle. This obligation is also backed by rational consensus, which is not confined to early Islam or the time of the Prophet but remains valid today and can be invoked in novel legal issues (Khoyini, 2018).

In the Islamic legal system, the protection of privacy and the prohibition of its violation is not merely a right but a rule (*ḥukm*). Unlike rights, rules cannot be waived. This demonstrates that human dignity in Islamic thought is not considered a

personal or private right but a general principle. In legal terms, human dignity and, consequently, the right to privacy are *jus cogens* norms and cannot be waived by agreement or consent (Seyyed Saadati, 2013).

Based on the principle of respect for human dignity, civil liability applies to individuals who infringe upon others' privacy in cyberspace and thus damage their dignity. This liability includes compensation for psychological and emotional damages suffered by victims since privacy violations affect not only material interests but also mental peace and social reputation.

Islamic jurisprudence insists on the sanctity of individuals and avoiding actions that harm their dignity. Therefore, privacy violations are condemned due to their conflict with the principle of human dignity. Since this principle also applies to individuals in cyberspace, violators of such privacy must bear the responsibility for their actions.

#### 2.4. The Principle of Validity (*Asalat al-Sihha*)

*Asalat al-Sihha* (the principle of validity) is one of the fundamental jurisprudential rules that has significant implications in Islamic jurisprudence. This principle is discussed in two dimensions: *taklifi* (duty-related) and *wad'i* (legal status). In its *taklifi* meaning, the action of a Muslim is presumed valid unless there is certainty of its invalidity or corruption, and the application of this principle does not imply that others are deemed unfit or unworthy. In its *wad'i* meaning, the principle carries legal and devotional consequences and removes any doubts or presumptions concerning the invalidity of a legal or religious act performed by a Muslim (Mohaghegh Damad, 2020).

The principle of validity is a practical rule in Islamic jurisprudence, which presumes the actions and behavior of others to be valid and lawful until proven otherwise. Designed to foster order and mutual trust in social interactions and to prevent suspicion and distrust, this principle can serve as a significant foundation for establishing civil liability concerning privacy violations in cyberspace.

The principle of permissibility (*Asalat al-Ibahah*) also supports this notion by presuming people's actions to be permissible in the absence of any legal prohibition. This principle prevents suspicion and intrusive investigations into individuals' behavior, thus safeguarding privacy as a fundamental right for users in cyberspace. Furthermore, given that the Qur'an and numerous narrations strictly prohibit unauthorized intrusion into individuals' private domains, any such interference is also deemed impermissible under *Asalat al-Ibahah* (Foroughi et al., 2014).

Applying this principle, which is based on the presumption of the validity of people's actions, prohibits investigation and spying into their lives. Consequently, individuals' privacy, as a fundamental right in cyberspace, is protected from unwarranted scrutiny. Therefore, the principle of validity can be regarded as one of the jurisprudential foundations for the prohibition of violating the right to privacy and the resulting civil liability for its breach (Foroughi et al., 2014). Additionally, the acceptance of the principle imposes a deterrent effect on the state regarding the monitoring and access to users' digital activities and shifts the burden of proof onto the state to demonstrate any violations.

According to the principle of validity, both users and service providers in cyberspace must conduct their actions based on legality and correctness, refraining from activities that infringe on others' rights and privacy. Hence, if a user unlawfully intrudes upon another individual's privacy—such as accessing, publishing, or manipulating their personal data without justification or legal authorization—this act constitutes a violation of the principle of validity. In such cases, the violator cannot escape civil liability by assuming their actions were valid, as privacy infringement is inherently contradictory to this principle and harmful to the rights of others.

Therefore, under the principle of validity, civil liability is assigned to the individual or institution that, by violating privacy, has caused damage to others in cyberspace. In other words, individuals must operate within a sound and secure framework that respects the private rights of others; otherwise, they are obligated to compensate for both material and immaterial damages resulting from the breach. This principle establishes a foundational safeguard for individual rights in cyberspace and acts as a barrier against undue invasions of privacy.

#### 2.5. The Principle of Generality of Consent

This principle is derived from the Holy Qur'an. *Idhn* (consent) refers to obtaining permission to enter another's private domain. In any context where entering another's privacy holds vital or decisive importance, the Qur'an advises that explicit



permission must be sought. Such consent benefits both the one who seeks and the one who grants it (Qur'an, Surah Al-Nur: Verses 27–30).

The principle of generality of consent is a jurisprudential rule emphasizing the necessity of acquiring explicit consent before using another person's property or rights. According to this principle, any use or interference with others' assets or rights without their clear and voluntary permission is impermissible, and civil liability is imposed on the unauthorized actor. This principle is especially critical in domains involving privacy and personal information.

With the growth of cyberspace and increased digital interactions, this principle has become even more significant. An individual's privacy in cyberspace includes their personal data, such as images, videos, messages, and other digital content. Under this principle, any access, processing, distribution, or utilization of such information without the explicit consent of the data owner constitutes a privacy violation and may result in civil liability.

Governments, under this principle, must exercise caution when implementing content filtering and restrictions in cyberspace to avoid infringing on public rights. If a government imposes broad filtering without clear religious or legal justification, causing harm to citizens' rights, it bears civil liability for such damages. For example, if individuals or businesses suffer losses due to unjustified restrictions on access to social networks, the government is responsible for compensating those losses (Mohammadi Nia & Karamati Moaz, 2024).

If this principle is violated in cyberspace, any individual or entity that discloses or uses someone else's private information without authorization is deemed a violator and is held liable for compensating the harmed party. This principle ensures that individual privacy rights in digital environments are respected and that potential abuses are prevented. In other words, civil liability for privacy violations based on the principle of generality of consent functions as a legal guarantee for protecting individual rights against unauthorized intrusions.

In Islamic jurisprudence, the principle of generality of consent provides a rational and principled foundation for civil liability concerning privacy protection in cyberspace. As such, any action or use of individuals' data in this environment requires their consent, and any transgression of this principle entails civil liability and necessitates compensating the resultant damages.

## 2.6. The Rule of Causation (*Qa'idat al-Tasabbub*)

The rule of *tasabbub* (causation) is one of the core jurisprudential principles that serves as a basis for civil liability when a person, through action or omission, causes harm to another. Under this rule, if a person performs an act that creates the conditions for damage or loss to occur, they are responsible for compensating the resulting harm, even if they did not directly cause it.

According to some jurists, the existence of fault is essential for the realization of civil liability under the rule of causation. Without fault, civil liability based on *tasabbub* cannot be established. This contrasts with the rule of *itlaf* (direct destruction), where liability does not require the presence of fault (Katouzyan, 2016).

It appears that certain harmful actions in cyberspace—such as copyright infringement and trademark violations—may fall under the scope of *itlaf*. The objection that direct causation is impossible in cyberspace is unfounded because the key difference between *itlaf* and *tasabbub* lies in whether the agent played a direct or indirect role in causing the harm. Direct or indirect causation must be evaluated within the specific characteristics of the digital environment. Given the unique conditions of cyberspace, direct causation can indeed be established in that context (Mohammadi Kordkhili, 2022).

In cyberspace, privacy violations often occur indirectly through behaviors such as unauthorized disclosure of personal data, hacking, or facilitating unauthorized access to information. Although such actions may not involve direct contact with the victim, they nevertheless create conditions for privacy violations and result in damage. Thus, the rule of causation can serve as a basis for civil liability of individuals or institutions responsible for such harm.

Accordingly, the rule of causation plays a vital role as a foundation for civil liability concerning privacy violations in cyberspace, especially when the violator contributes indirectly to the harm. In the digital realm, this rule is broadly applicable in supporting individuals' rights and deterring irresponsible behaviors that lead to privacy breaches.

### 3. Legal Foundations

In contemporary Iranian law, there are multiple foundations for civil liability. However, there is no consensus among jurists regarding a unified basis for civil liability. Naturally, this divergence has also extended to the domain of cyberspace, particularly because the nature of cyberspace differs significantly from traditional legal contexts and lends itself to such challenges. Although a detailed discussion of classical theories of civil liability is beyond the scope of this study, a brief introduction to traditional foundations is necessary to properly analyze the issue and to evaluate the applicability of such foundations to the cyberspace context. Several theories have been proposed in Iranian law as the basis of civil liability, each with its own proponents and critics. Among these, the fault-based liability theory, the risk-based liability theory, and the theory of right-guarantee are considered the most important legal foundations, each contributing in its own way to the protection of individual rights against privacy violations.

#### 3.1. Fault-Based Liability Theory

The fault theory in civil liability is a classical and traditional approach that prevailed in Western legal systems until the late 19th century. According to this theory, civil liability is based on fault (whether intentional or unintentional), and only a person who commits a fault can be held liable, with the burden of proof generally resting on the injured party. Proponents of this theory—which remains the dominant theory in the West and likely in most countries—justify it using moral concepts: civil liability is seen as a specific form of moral responsibility, and therefore, without fault, liability is not acceptable. Condemning a person without proven fault is tantamount to condemning the innocent, which morality cannot accept (Safaei & Rahimi, 2017).

This theory, rooted in specific philosophical foundations, holds that a person is obligated to compensate for damages only if they have committed a fault. In other words, for the injured party to seek compensation, they must prove that the damage was caused by the wrongdoer's fault. This approach brings civil liability closer to moral responsibility, and in certain definitions of fault (personal fault), the distinction between the two becomes blurred. Therefore, the concept of fault occupies a central place in civil liability, and differing interpretations of it significantly affect the scope of liability (Qasemzadeh, 2008).

In the past, fault was regarded as a personal concept. Under this interpretation, individual freedom allowed a person to engage in various activities, with little consideration for the potential dangers resulting from their actions. Accordingly, a person would only be held liable if they committed a blameworthy act that caused harm to another and that harm could have been anticipated or avoided. This interpretation created numerous challenges, excluding minors and the legally incompetent, and opened the door for many individuals to evade responsibility, since personal fault was difficult to prove in most cases (Barikloo, 2017).

In the English legal system, there is no debate among jurists about fault being the primary basis for tort liability. However, in the Iranian legal system, there is disagreement on this point. Legal sources such as *damān yad* (liability for usurpation and its equivalents), *itlāf* (destruction), and the enactment of the Islamic Penal Code of 2013—which appears to emphasize customary causal relationships for establishing civil liability—have raised doubts about whether fault is indeed the principal basis. Nevertheless, most Iranian jurists emphasize the adoption of fault as the main foundation of civil liability, and judicial practice has largely upheld this position (Safaei & Rahimi, 2017).

As one of the legal foundations of civil liability, the fault-based theory is also applicable to privacy violations in cyberspace. According to this theory, a person is held civilly liable if their act or omission, due to negligence or failure to meet legal or professional standards, causes harm to another. Therefore, if a person breaches another's privacy due to carelessness, negligence, or violation of laws, they are responsible for compensating the resulting damages.

The development of the fault theory has been influenced by two main currents:

- a. The unification of criminal and civil liability—just as a person is only criminally liable when they have committed a fault, in civil liability, too, responsibility is premised on the existence of fault. This view was prevalent in Roman law as well.
- b. Moralism—the fault theory has also been shaped by Christian moral teachings, where liability arises from actions that cause the conscience to feel shame. Therefore, proponents of this theory believe that adhering to it helps achieve the ethical ideals of justice within the legal system (Rostami & Bahadori Jahromi, 2009).

In modern theories, fault is defined as deviation from standard conduct and has thus acquired a social character. According to the fault theory, the only justification for imposing liability is the causal relationship between the fault and the damage (Mir Dadashi, 2014).

Some legal scholars believe that the liability of internet service providers can be explained based on the presumption of fault. This has two advantages: first, assuming fault facilitates the filing of lawsuits against intermediaries when harm occurs due to users or third parties, and the burden of disproving fault lies with the intermediary. Second, despite the presumption of fault, the role of users or third parties is not ignored; if the intermediary adheres to applicable regulations and proves no negligence or misconduct, they are exempt from liability (Abhari & Miri, 2011).

In cyberspace, which is largely under the control of the state, the government has a dominant role. If state liability in cyberspace is made contingent on proving fault, ordinary injured citizens will face considerable challenges in establishing fault on the part of the government. This could severely restrict the possibility of holding the state civilly liable—an outcome that is neither fair nor just. In contrast, Islamic jurisprudence and legal doctrines emphasize that where a loss can be causally attributed to an agent, compensation is mandatory, regardless of whether fault is established (Mohammadi Nia & Karamati Moaz, 2024).

In cyberspace, protecting users' privacy is a fundamental duty of individuals and institutions operating in this realm. Fault in cyberspace may occur in various forms, directly or indirectly resulting in privacy violations. Some examples of fault in this context include:

- a. **Negligence in data protection:** If a company or individual fails to take adequate measures to protect users' personal data, leading to unauthorized access or disclosure, this is considered fault and gives rise to civil liability.
- b. **Improper use of data:** Organizations that use personal data without the consent of users and violate their privacy are acting in accordance with the elements of fault-based liability, as their actions result in harm to the user.
- c. **Failure to comply with data protection laws:** Many countries have clear regulations for protecting privacy and personal data in cyberspace. If an entity violates these laws and causes harm, it bears the responsibility for compensation.

Accordingly, the fault-based liability theory plays a decisive role in establishing civil liability for privacy violations in cyberspace. This theory ensures that individuals and organizations that fail in their duty of care toward user privacy are held accountable and obligated to provide compensation. In addition to protecting user rights, this approach serves as a deterrent against irresponsible behavior in the digital environment.

### 3.2. *Risk-Based Liability Theory*

Transformations in anthropological foundations on the one hand, and advances in industry and technology along with the emergence of economic enterprises on the other, have created new relationships in the world, such that the fault-based theory—despite its historical depth and dominance—could no longer adequately address new issues in civil liability. This led some scholars to strongly criticize it. According to these critics, the mental element of fault cannot provide a practical solution for people, particularly the vulnerable, in today's complex context. Proving fault, especially in cases where harm is caused by machinery, often appeared difficult or even impossible. Therefore, to facilitate the establishment of liability and the compensation of damages, attempts were made to remove the element of fault from civil liability, establishing instead that “as soon as a person causes harm, they must compensate for it, whether the act that caused the damage was right or wrong” (Katouzyan, 2016). In other words, proponents of the risk theory believe that liability arises from a person's activity, not from their fault.

One of the most important advantages cited for the risk theory is that by removing fault as a condition for civil liability, damage claims become easier to pursue, and the injured party is relieved from the burden of proving fault. In contrast, proponents of the fault theory argue that removing the element of fault does not simplify liability claims but rather complicates them. In any incident, multiple causes may contribute, and the judge may struggle to resolve the matter. This has led to the emergence of various theories about multiple causation. While the fault theory identifies the cause linked with the wrongful act, the risk theory broadens the scope. Several other advantages have also been suggested for the risk theory, each of which has received reasoned responses from supporters of the fault theory. Consequently, some advocates of the risk theory have



modified their views to include a type of fault, while others have reformulated the pure risk theory into a new concept of inherent risk.

The risk-based liability theory is one of the legal foundations of civil liability and is also applicable to privacy violations in cyberspace. In this theory, unlike fault-based liability, proving fault or negligence is not required for establishing liability. Instead, merely creating a risk or engaging in an inherently hazardous activity is sufficient to impose responsibility for compensating the resulting damages.

One of the key legal foundations that can be observed under civil liability in cyberspace—particularly in the European Union and notably in the legal system of the United Kingdom—is the risk theory (Mohammadi Kordkhili, 2022). In cyberspace, risk-based liability can be applied in circumstances where the nature of an activity inherently poses threats to individuals' privacy.

Some examples of privacy violations in cyberspace that can be examined under this theory include:

a. **Online platforms and social networks:** Platforms that share users' private information are inherently at risk of violating user privacy due to the nature of their operations. Even in the absence of carelessness or specific fault in publishing or storing data, liability for compensation may arise due to the inherently risky nature of their activities.

b. **Big data collection and processing:** Companies that collect and process large volumes of user data without clear consent or with vague permissions bear responsibility for any misuse or privacy violations stemming from their handling of sensitive data—even in the absence of any demonstrable fault.

c. **Use of emerging technologies such as artificial intelligence:** AI tools and surveillance technologies are considered inherently high-risk due to their extensive access and potential intrusions into user privacy. Even without fault, users of these technologies may be held civilly liable for potential privacy violations.

The risk-based liability theory can offer several advantages in terms of enhancing privacy protection in cyberspace, including:

a. **Increased obligations for companies and online platforms:** By imposing liability without requiring proof of fault, companies and platforms are compelled to implement stronger measures to safeguard privacy.

b. **Protection of users and victims of privacy violations:** Since users may face challenges in proving the fault of the violator, the risk theory makes it easier for them to receive compensation.

c. **Deterrence from privacy breaches:** This theory encourages risk reduction and the implementation of robust safeguards because actors in cyberspace know they will be liable for damages if privacy is violated.

Therefore, the risk-based liability theory, as a legal foundation for civil liability in the context of privacy violations in cyberspace, can serve as an effective tool for protecting users from risks inherently associated with online activities. By applying this theory, companies and technology providers are required to adopt more stringent measures to protect users' data, while users gain greater immunity against potential privacy breaches. This theory contributes not only to the preservation of individual privacy but also to the creation of a safer and more responsible environment for the use of modern technologies in cyberspace.

### 3.3. *The Right-Guarantee Theory*

This theory proposes that civil liability and compensation for harm should be approached from a different perspective. According to this theory, neither fault, nor the injurious act, nor the creation of a hazardous environment constitutes the basis of civil liability. In other words, attention should not be focused on the injurious actor or the harmful act itself. Rather, civil liability is founded upon the guaranteed right of the injured party that has been violated. That is, human beings possess rights such as liberty, security, and health. These rights are recognized and guaranteed by the legislator. Therefore, if one person causes damage to another, they have, in effect, infringed on that individual's right to security and well-being. The legal guarantee of such rights by the legislator must be enforced through civil liability, which entails compensating the victim for the harm suffered.

The right-guarantee theory is one of the significant legal foundations in civil liability and is particularly relevant and applicable in the context of privacy violations in cyberspace. According to this theory, individuals are entitled to protection and guarantees against violations of specific rights, including the right to privacy. This approach bases civil liability not merely on

fault, but rather on the individual's inherent right to privacy. Therefore, under this theory, liability for privacy violations stems from the legal guarantee of that right and obligates the violator to compensate for damages.

The right-guarantee theory asserts that everyone has the right to live in a safe and secure society where their rights are protected. No one has the right to endanger the rights, safety, or well-being of others. As soon as a right is violated and harm occurs, it must be compensated, and this obligation to compensate is what constitutes civil liability. The principal advantage of this theory is its focus on protecting the rights of victims and ensuring legal safeguards for them (Sartipzadeh & Ghafari, 2018).

In the right-guarantee theory, it is assumed that individuals in society possess inherent, inviolable rights that must be fully protected by law and the judicial system. Among these rights is the right to privacy, which in cyberspace is especially vulnerable due to the ease of access to personal data and the frequent disclosure of private information. According to this theory, a privacy violation warrants compensation even if no fault or negligence can be proven.

In cyberspace, the application of the right-guarantee theory is essential for protecting users' privacy. With the rapid expansion of digital technologies and methods of data collection and processing, individuals' privacy is increasingly threatened and violated. Examples of privacy violations where this theory can be invoked include:

- a. **Disclosure of personal information by platforms and websites:** If a platform or website discloses private user information or transfers it to third parties, it bears the responsibility for compensating damages under the right-guarantee theory.
- b. **Monitoring and tracking online behaviors:** Many digital companies track users' online activities through various technologies and use the data for commercial purposes. Under the right-guarantee theory, such practices constitute privacy violations and require compensation.
- c. **Improper use of user data and information:** If users' personal data are used without their consent for unauthorized or contrary purposes, the violator is held civilly liable under the right-guarantee theory and must provide compensation for the resulting damages.

Thus, the right-guarantee theory, as a legal foundation for civil liability, offers an effective approach to safeguarding privacy in cyberspace. By invoking this theory, the right to privacy is recognized as an inviolable entitlement, and any infringement—regardless of fault—results in liability for compensation. This theory, with its emphasis on guaranteeing user rights, can effectively protect individuals' privacy against potential violations and contribute to a safer and more trustworthy digital environment.

#### 4. Conclusion

Privacy, as one of the most fundamental human rights, is protected under both legal and jurisprudential systems, and its violation may give rise to civil liability. An examination of the jurisprudential and legal foundations reveals that civil liability arising from privacy violations in both domains is based on principles and rules that emphasize the necessity of compensation.

In Islamic jurisprudence, principles such as the *no-harm* rule (*la darar*), the principle of respect for the believer's privacy, the principle of respect for human dignity, the principle of validity, the principle of generality of consent, and the rule of causation all clearly establish the sanctity of private space. These principles not only offer protection against unauthorized intrusion into individuals' personal domains but also require compensation for resulting damages.

On the other hand, the legal system, drawing upon the theories of fault-based liability, risk-based liability, and the right-guarantee theory, provides a rational framework for determining civil liability in cases of privacy violations. The fault-based theory requires proof of the violator's negligence or misconduct, while the risk-based theory deems the occurrence of harm sufficient. The right-guarantee theory emphasizes unconditional protection of privacy rights, irrespective of fault or risk.

Therefore, it can be concluded that, from both jurisprudential and legal perspectives, privacy violations entail civil liability. Whether grounded in jurisprudence, which considers intrusion into personal rights a religious prohibition, or in legal doctrine, which guarantees protection through compensation, such violations are unlawful and must be remedied. Consequently, to strengthen enforcement mechanisms in this area, legal and judicial systems must adopt effective measures—based on these foundations—to prevent privacy violations and ensure adequate redress for damages.

## 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

- Abhari, H., & Miri, H. (2011). A comparative study of the foundations of civil liability of internet service providers. *Comparative Legal Research*, 15(3).
- Badini, H., Khoyini, G., & Karami, H. (2020). Protection of privacy in cyberspace with emphasis on ethical and jurisprudential principles. *Ethical Research*, 10(4).
- Bahrami Ahmadi, H. (2011). *Rules of jurisprudence* (Vol. 2). Tehran: Imam Sadiq University Press.
- Barikloo, A. (2017). *Civil liability*. Tehran: Mizan Publishing.
- Foroughi, F., Borji, M. N., & Moslehi, J. (2014). Foundations of the prohibition of privacy violation in Iranian and American law. *Legal Studies Journal*, 6(3).
- Katouzian, N. (2016). *Extracontractual obligations: Civil liability* (Vol. 2). Tehran: University of Tehran Press.
- Khoyini, G. (2018). *Philosophy of law*. Tehran: Majma Scientific and Cultural Publishing.
- Kulayni, M. B. Y. (2008). *Al-Kafi*. Tehran: Dar al-Kutub al-Islamiyyah.
- Mir Dadashi, S. M. (2014). *Civil liability of public institutions in Iranian and Egyptian law*. Qom: Mofid University Press.
- Mohaghegh Damad, S. M. (2020). *Rules of jurisprudence, civil section* (Vol. 1). Tehran: Center for Islamic Science Publishing.
- Mohammadi, A. H. (2020). *Rules of jurisprudence*. Tehran: Mizan Legal Foundation.
- Mohammadi Kordkhili, H. (2022). Foundations of civil liability arising from internet communications in Iranian law and the European Union. *International Legal Research*, 15(55).
- Mohammadi Nia, O., & Karamati Moaz, H. (2024). Jurisprudential and legal foundations of civil liability of the government regarding filtering (purification) of social media networks. *Comparative Research in Jurisprudence, Law, and Politics*, 6(4).
- Mousavi Khalkhali, S. M. M. (1997). *Fiqh al-Shi'a - Book of Ijarah*. Tehran: Monir Cultural Center Publishing.
- Mowhidd, M. A. (2002). *In the air of rights and justice*. Tehran: Karnameh Publishing.
- Qanavati, J., & Javar, H. (2011). Foundations of respect in recognizing and protecting privacy in communications. *Islamic Law Journal*, 8(29).
- Qasemzadeh, S. M. (2008). *Foundations of civil liability*. Tehran: Mizan Publishing.
- Rostami, V., & Bahadori Jahromi, A. (2009). Civil liability of the government. *Islamic Legal Research Journal*, 10(29).
- Safaei, S. H., & Rahimi, H. (2017). *Civil liability (extracontractual obligations)*. Tehran: Samt Publishing.
- Sartipzadeh, R. T., & Ghafari, M. (2018). Elements and conditions of civil liability of the government for compensation. National Conference on New and Creative Ideas in Management, Accounting, Legal and Social Studies.
- Seyyed Saadati, F. (2013). Protection of privacy in cyberspace based on Islamic norms. *Cultural Strategy Quarterly*, 23.
- Tusi, M. B. H. (2008). *Al-Mabsut fi Fiqh al-Imamiyah*. Tehran: Al-Maktabah al-Murtazaviya.