The Scope of Governmental Monitoring and Regulation of Cyberspace in Relation to Individual Privacy (Based on Imami Jurisprudence)

■ Mehdi Dargahi[1]
■ Hassan Rezai[2]

Abstract

The government's actions in monitoring and regulating content in cyberspace are deemed necessary for various reasons, including the maintenance of a stable system, the preservation of the supremacy and authority of the state, and the promotion of religious values. On the contrary, general religious principles emphasize the prohibition of spying, highlighting the importance of respecting individuals' privacy. It is evident that the act of monitoring and regulating cyberspace can potentially infringe upon this privacy, particularly in terms of information and communication privacy. Given that the extent of governmental intervention in monitoring and regulating cyberspace, as well as the prohibition of infringing upon individuals' communication and informational privacy, is not clearly defined in Imami jurisprudence, the question of how much intervention is permissible raises a significant problem. It is essential to delve further into this issue to arrive at an appropriate and satisfactory resolution. The preservation of the Islamic system, the maintenance of the supremacy and authority of the Islamic state, and the establishment of religion are among the reasons that justify the exercise of authority in monitoring and regulating cyberspace, even if it infringes upon privacy. However, a careful analysis of the evidence suggests the hypothesis that these governance practices

1. Faculty member, Al-Mustafa International University. Email: aghigh_573@yahoo.com
2. Faculty member, Al-Mustafa International University. Email: tafvin@miu.ac.ir

The Scope of Governmental Monitoring and Regulation of Cyberspace in Relation to Individual Privacy

■ Mehdi Dargahi and Hassan Rezai

should be conducted based on scientific principles while observing the limits of necessity. It is crucial to ensure that such measures are implemented without disclosing individuals' hidden secrets within this realm. This article aims to explore the limitations and deficiencies in the evidence relating to monitoring and regulating cyberspace while safeguarding individuals' information privacy. It seeks to elucidate the jurisprudential factors contributing to privacy violations. To achieve this objective, the methodology employed involves collecting library data and analyzing jurisprudential propositions. The outcome of this analysis is the examination and clarification of the extent to which governmental intervention in monitoring and regulating cyberspace is permissible in relation to individuals' privacy.

Keywords: Exercise of authority, monitoring and regulating cyberspace, privacy, Imami jurisprudence.

1. Introduction

The advancement of technology has profoundly impacted human life, particularly in the realm of social interaction. This transformation has been facilitated by the establishment of interconnected computer networks on digital platforms. These platforms have catalyzed high-speed communication, leading to transformative changes. For instance, they allow easy and unrestricted access to any data and messages, irrespective of geographical boundaries. This has ushered in an era of trans-spatial and timeless communication, thus revolutionizing how we connect and interact globally. The virtual space has brought about substantial progress across various domains such as the economy, culture, politics, law, and more. Furthermore, the rapid advancement of cyberization has fueled significant developments, albeit with new challenges emerging in the field of jurisprudence. While jurisprudence aims to govern all aspects of human life, its ability to effectively address the demands and navigate the dynamics of cyberspace in diverse spheres remains unproven.

It is important to acknowledge that jurisprudential rulings on cyberspace are not separate from the physical realm; rather, it is an integral part of it. Many legal rulings in cyberspace align with those in the physical world, even when the actors involved are real individuals. However, due to the unique nature of cyberspace, specific regulations are required, and it is imperative for jurisprudence to actively engage in this domain. One notable concern revolves around the government's authority in monitoring and regulation of cyberspace, particularly in relation to individuals' privacy rights. This issue is closely monitored and scrutinized by advocates of human rights and civil liberties at the community level, who approach it with utmost sensitivity. Undoubtedly, the anonymity of user identities within this digital realm, along with the capacity to conceal one's identity, has resulted in its macro-management extending beyond national borders. While cyberspace has led to significant communication possibilities, it has also presented governments with a range of social, cultural, economic, political, and security challenges both domestically and internationally. Consequently, governments engage in the monitoring and regulation of cyberspace within their territories, even though they do not publicly acknowledge it.

While they claim to safeguard individual freedoms, particularly in terms of privacy, they often implement monitoring and restrictive measures when national security concerns arise. However, it is important to note that privacy remains an unfulfilled demand and desire of the people.

Due to the historical exclusion of Shiites from attaining a political system and establishing a government based on pure Islam, and the emergence of new governance challenges in the realm of cyberspace, the jurisprudential issues concerning government, particularly in governing cyberspace, have received less attention from Shiite jurists. However, it is worth noting that the scholarly foundations and basic principles pertaining to these issues can be found within jurisprudential texts and sources.

Given the significance of protecting individuals' privacy within cyberspace, along with the general prohibition of spying and the need for monitoring and regulating, it becomes essential to establish a framework for exercising authority over cyberspace while upholding individual privacy. This framework should align with the principles of Imami jurisprudence, which emphasize the necessity of preserving the system, establishing religion, and safeguarding the supremacy and sovereignty of the Islamic state. This approach aims to prevent any unwarranted leniency or extremism when attributing the perspective of jurisprudence to potential violations of individuals' privacy. By elucidating the extent of sovereignty within this context, it is crucial to strike a balance that avoids excessive intrusion or negligence in practice, even though occasional instances of excess or deficiency may occur to a certain degree.

The research begins by outlining the fundamental concepts involved and then proceeds to elaborate on the necessity of monitoring and regulating cyberspace. This is accomplished by presenting three reasons that demonstrate the importance of such measures in the context of cyberspace. Subsequently, the conflict between the imperative to preserve privacy and the process of monitoring and regulating cyberspace is explored, followed by a jurisprudential analysis that offers two approaches to reconciling these concerns. Lastly, the research addresses the jurisprudential factors involved in privacy violations within the context of monitoring and regulating cyberspace.

2. Explanation of Basic Concepts

Providing an explanation of the fundamental concepts in the research serves not only to enhance the purposefulness of the dialectic but also to facilitate the reader's understanding of the author's perspective regarding the interpretation of the terminology used in the study. This clarification is crucial in order to mitigate any potential misunderstandings that may arise during the course of the research.

2.1. Exercise of Authority

The term "exercising authority" refers to the actions carried out by those in positions of superior command power or acts of will that surpass the will of others (Ghazi 2004, 180). This encompasses the governmental actions undertaken with universal power and as expressions of that power (Jafari Langroodi 2017, 471). If a jurist assumes leadership in a government and oversees the administration of society during the period of the Major Occultation of the final Shiite Imam, with the aim of discovering Islamic rulings and establishing a government based on pure Islamic teachings, as well as the theory of absolute or unconstrained authority or guardianship of the jurist, they would possess the powers and authority akin to an Infallible Imam in matters pertaining to social affairs and the welfare of the Islamic society (Imam Khomeini 1421 AH, 1:637; Sabzawārī 1413 AH, 1:261; Momen 1425 AH, 1:414; Ḥāʾirī 1424 AH, 23). The term "exercise of authority" refers to the actions of guardianship carried out by the jurist in the management of the Islamic society. These responsibilities may be delegated to certain governing bodies, enabling them to act independently and directly in some or all stages of implementation.

2.2. Regulation of Cyberspace

Although significant attention has been given to "cyberspace" in cultural matters and the realm of communication, we continue to encounter diverse interpretations when attempting to describe it. Through an extensive examination of existing definitions and an analysis of its elements, some authors have made notable efforts to provide a comprehensive understanding. Consequently, we can define cyberspace as a virtual and intangible domain,

serving as an environment for social interaction that emerges through a network of interconnected computers on a digital platform (Esmaeeli and Nasrollahi 2016, 60).

Furthermore, as indicated by other authors, the scope of cyberspace encompasses a wide range of data and communications, including information transmitted through websites, blogs, chat rooms, forums, social networks, dating platforms, electronic mail, mobile phones, SMS, Bluetooth, and similar mediums (Tabatabaee and Layali 2018, 87).

The regulation of cyberspace should not be solely understood as a means of deprivation, obstruction, limitation, or negation, as defined by the competent authorities in the field, aimed at purposefully and systematically impeding the flow of information (Ismaeeli and Nasrollahi 2016, 57). It is important to acknowledge the positive aspect of regulation as well. In other words, regulating cyberspace does not merely entail restricting and preventing access, such as through filtering. In many instances, it may involve the creation of a new domain independent of the international scope, as well as the inclusion of educational, promotional, and preaching content. Therefore, in the context of this research, the concept of regulating cyberspace also encompasses such positive elements.

2.3. Monitoring Cyberspace

The monitoring of cyberspace involves gathering information about deficiencies and strategizing to enhance productivity in implementing the government's small-scale and large-scale plans across social, cultural, economic, and political domains, as well as ensuring the resilience of society within this realm, including both hardware and software aspects. The primary objective is to secure and safeguard cyberspace while identifying any social irregularities within it. Thus, in this research, monitoring is recognized as an initial stage in regulating cyberspace, encompassing both negative and positive aspects.

It is important to highlight that the ultimate objective of monitoring and regulation, as described above, is the pursuit of personal and social excellence for individuals within society. According to the Islamic worldview, this pursuit aligns with the enlightenment of the human soul through divine guidance and the

progression towards a fulfilling life. Moreover, by embracing religious principles and implementing Islamic values in both personal and social matters, it becomes feasible to attain this ultimate goal in the physical realm as well as in the cyberspace platform of society.

3. The Necessity of Monitoring and Regulating Cyberspace

Given that the regulation of cyberspace encompasses both its positive and negative aspects, it is essential to support the analysis of monitoring and regulating it with evidence that is not limited to any particular claim. In order to illustrate the necessity of monitoring and regulating the cyberspace in a comprehensive manner, the following three reasons shall be presented, shedding light on both its positive and negative dimensions.

3.1. Maintaining System Integrity

In the realm of political jurisprudence, the term "system" encompasses various aspects, including the administration of people's lives and well-being, the foundation of an Islamic country (referred to as the Islamic system), the current political regime, as well as the political, economic, cultural, and social micro-systems. Additionally, it encompasses the overall system of the nation and the principles of Islam (see Malek Afzali, et al. 2012, 129-33). The necessity and obligation to protect and preserve the Islamic system are determined based on its alignment with the collective welfare of society.

According to common sense, it is deemed essential to prioritize the public interests of society (see Montazeri 1409 AH, 4:298). Rational judgments are considered obligatory under the principle of mutual entailment between Sharia and reason (which states that whatever reason dictates, God's law also dictates). Consequently, the necessity of preserving the Islamic system is rooted in safeguarding the general social interests, just as its disruption would entail neglecting those very interests. Therefore, the preservation of the Islamic system is independent of factors such as objection, harm, coercion, and necessity. Based on the aforementioned rationale, members of society hold an obligation to preserve the Islamic system, irrespective of whether its preservation may involve challenges to public interests,

difficulties, objections, coercion, and similar circumstances (see Alidoost 2009, 127).

The preservation of the Islamic system is closely linked to safeguarding the overall societal well-being. In the context of the Islamic worldview, the concept of exigency refers to benefits that encompass spiritual goodness, both in the individual and societal sense, with a primary focus on attaining eternal happiness and true perfection in the afterlife (Dargahi 2020, 110). It becomes evident that securing the spiritual and material well-being of society can only be achieved by adhering to divine commands. The government's claim to prioritize the interests of society can only be substantiated by nurturing the genuine perfection of individuals, which can be accomplished through the practice of the teachings of pure Islam. Furthermore, within our sacred religion, there are explicit references to the duty of preserving the Islamic system. According to reports from the Infallibles (cf. Montazeri 1409 AH, 300-6), one of the fundamental divine responsibilities bestowed upon duty bearers, especially the Islamic ruler, is to protect the core principles of Islam or the Islamic system (see Imam Khomeini 1999, 11:494 and 15:329).

In the present day, the preservation of the Islamic system is intricately tied to the preservation of the Islamic government, which was established with the aim of implementing the principles of Islam in accordance with the teachings of pure Islam (see Imam Khomeini 1415 AH, 2:665). Furthermore, ensuring the protection of the Islamic system, in line with reason and conscience, necessitates the monitoring and regulation of cyberspace, including both its negative and positive dimensions. In fact, prioritizing the monitoring of information within the virtual realm, both domestically and internationally, takes precedence over monitoring activities in the physical realm. This approach recognizes the vital role that cyberspace plays in safeguarding the integrity of the Islamic system. In essence, akin to the Islamic system in the physical world, the monitoring of government officials and agents by the Islamic system is imperative to curbing abuses of power, ensuring the protection of public freedoms, rights, and, ultimately, serving the overall public interest. This discreet monitoring serves as a mechanism to hold accountable those entrusted with positions of authority and to maintain a system that upholds the principles of justice and transparency.

The objective is to monitor the continued qualifications of government officials, as well as to continuously track the anti-Islamic and military activities carried out by foreign governments, nations, hypocrites, and their associated underground groups. This comprehensive monitoring approach aims to identify and counteract the schemes and conspiracies orchestrated by the adversaries of the Islamic system, thereby equipping it with the necessary means to thwart their efforts. Moreover, by acquiring information about the conditions of the general public and social trends, the government becomes aware of issues, needs, legal gaps, and administrative shortcomings. It then endeavors to address these concerns and improve the overall well-being of society. Similarly, in the realm of cyberspace, a parallel approach should be adopted. By monitoring the digital landscape, the government can gain insights into emerging challenges, societal demands, and regulatory gaps, allowing for proactive measures to address them effectively. Considering that cyberspace provides a cost-effective, rapid, and unconventional means to undermine the Islamic system, it has become a crucial area of focus. The anonymity and ability to conceal one's identity within this realm have facilitated its external manipulation, extending beyond the physical boundaries of the Islamic system.

Furthermore, apart from the ongoing monitoring and regulation, it is essential to enable the Islamic system to take appropriate actions and reactions against cyber-attacks. These attacks aim to destroy and compromise computer infrastructure, disrupt data by denying or altering access, manipulate personal and financial information of individuals, and spread false information. Such cyber-attacks are conducted with the intention of tarnishing the reputation of individuals, undermining the economy, security, politics, and even the reputation of the country and its government.

The response to religious, sectarian, moral, cultural, and social attacks should be conducted with heightened sensitivity. Neglecting preventive measures, procrastinating and failing to plan for the creation of authentic Islamic content for teaching, preaching, and promotion within this realm can have detrimental consequences. Such negligence can disrupt the economic, cultural, political, and social systems within Islam, ultimately

posing a threat to the Islamic system and the Islamic state over time. It is crucial not to underestimate the impact of the virtual space and assume it is disconnected from reality, as technological advancements have enabled cyberspace to permeate various domains such as politics, law, culture, economy, and security. Additionally, the cyber environment has facilitated transnational activism without direct human intervention. It is important to recognize that the realm of culture and ideas is not confined to a virtual space; rather, it holds tangible significance in both real and virtual domains.

Any entity that directly influences the thoughts of thinkers, imparts messages to the mind, or instills attributes in the soul is undeniably real and not merely virtual. Thought exists everywhere, and the transmission of knowledge and ideas is a tangible reality (Javadi Amoli 2013). The intermingling of virtual and physical spaces in the present era highlights the interconnectedness between preserving the Islamic system in the physical realm and preserving it in the realm of cyberspace.

In light of the practical examples set by the infallibles, particularly the Prophet Muhammad (s) and Imam Ali (a), in their administration and governance, their emphasis on reminding their appointed governors is evident through numerous reports found in hadith sources (Muntazeri 1409 AH, 4:309-379). Recognizing that the physical realm lacks distinctive characteristics in this context, it follows *a fortiori* that information surveillance and regulation in the virtual space are important. This approach is adopted to protect the Islamic system, leveraging the necessity and requirement of monitoring and controlling the digital realm.

3.2. Establishment of Religion

Based on both speculative and textual evidence, and in accordance with the theory supported by certain Imami jurists, the responsibility of establishing an Islamic government during the occultation of Imam al-Mahdi (may Allah hasten his reappearance) falls upon a just and qualified jurist (see Andalibi and Dargahi 2015, 33-49). Quranic verses (Quran 42:13; 22:41) outline the duties of prophets and Islamic leaders, which we have reason to believe are not exclusive to them and encompass the jurist guardians who are entrusted with political and

administrative affairs. These verses emphasize the critical obligation of establishing the religion and creating the necessary conditions for the implementation of divine decrees, as well as preventing their abandonment. Based on the principles of ontology and anthropology, establishing the religion or implementing Islamic teachings within society, both in the physical and cyberspace realms, provides the means for individuals to attain personal and social perfection, ultimately leading to a virtuous and fulfilling life—an Islamic life, to be precise (see Momen 1425 AH, 1:329).

When the conditions for implementing Islamic rulings in both the physical and virtual realms are met, and the implementation of one does not contradict the implementation of the other, the complete implementation of Islamic rulings can be achieved. However, if certain conditions necessary for implementing specific Islamic rulings in either the real or cyberspace are not present, or if the implementation of certain rulings hinders the implementation of others, the responsibility of the ruler and, consequently, the government becomes twofold.

First and foremost, a practical approach is employed to distinguish between rulings of varying importance, allowing for the establishment of necessary conditions to implement the more important rulings within society. This prioritization aims to create an environment that removes obstacles hindering the simultaneous implementation of both more and less important rulings. By adopting practical solutions, the Islamic government endeavors to enable the implementation of both categories of rulings concurrently. Consequently, the responsibility of the ruler and subordinates of the Islamic government, in both the physical and virtual domains, can be summarized as follows: The implementation of Islamic rulings should consider the relative importance of each ruling, taking into account the specific requirements of time and place. In this comprehensive framework, the ruler and subordinates are tasked with ensuring that both more and less important rulings are implemented in society. This approach involves assessing the qualitative and quantitative significance of each ruling within the context of their coexistence. In certain cases, this responsibility can be delegated to specific governing bodies within the Islamic

government, empowering them to independently and directly address this matter.

If we consider the duty of the ruler and, by extension, the Islamic government to enforce rulings as the major premise of our reasoning, and view each imagined ruling in the cyberspace as its minor premise—a ruling that has been deduced, explained, and presented by scholars in the field of jurisprudence—we can conclude that the implementation of each of these rulings is indeed among the responsibilities of the ruler and the Islamic government.

It may be argued that the ruler and the government are only accountable for implementing social orders and do not have the responsibility or authority to govern individual matters concerning members of society, especially in the cyberspace. However, this perspective stems from a limitation placed on the powers and responsibilities of the ruler solely in social affairs, and a division between individual and social rulings. Yet, it is important to note that this division and the criterion used to define it, which aims to explain the powers of the ruler and the government in exercising authority, is not accurate. This is because such a division does not exist within religious sources, which primarily involve the concepts of "God's right" and "people's right." It is clear that this division is not the determining factor for defining the powers of the ruler and the government.

To provide further clarity, it is essential to outline the premises. Based on the explicit or implicit contents of certain Quranic verses (Quran 3:104, 110, 114; 4:63, 79; 7:157; 9:71, 112) and the authentic hadiths transmitted from the infallible Imams (a), one of the obligatory rulings is the duty to enjoin what is good and forbid what is evil. The interpretations found in some hadiths regarding this duty, such as referring to it as "the highest and most honorable duties" and "the foundation of obligations" (Kulaynī 1407 AH, 5:55), signify its status as a significant divine obligation and a guarantee for the implementation of religious commands.

Regarding the duty of enjoining what is good and forbidding what is evil, hadiths (Ḥurr a-ʿĀmilī 1409 AH, 16: 133-35) and the statements of jurists (e.g., Najafī 1404 AH, 21: 383; Montazeri 1409a AH, 2: 215) suggest that one of its stages necessitates physical intervention in the affairs of others. However, in order to prevent chaos, such intervention becomes obligatory (Muḥaqqiq

al-Ḥillī 1412 AH, 2: 15). Nevertheless, the legitimacy of this order is contingent upon the permission of the Islamic ruler, or *Walī al-amr* (Muḥaqqiq al-Ḥillī 1415 AH, 1: 259; Najafī, 1404 AH, 21: 383-96). Originally, it is considered one of the powers and duties of the ruler to act directly, or grant permission or delegate others to act on their behalf (Ṭūsī 1996, 150; Imam Khomeini, n.d., 1: 482; Montazeri 1409b AH, 2: 218).

Neglecting this duty by the ruler or their authorized representatives and delegates can lead to the normalization of forbidden acts and the neglect of obligations, blurring the distinction between good and evil in the eyes of the people (see Kulaynī 1407 AH, 5: 59). Such abandonment not only undermines the principles of Islam but also creates a contradiction between claims and actions, fostering pessimism among the people towards the ruler and the Islamic government. Consequently, it is the responsibility of the ruler and their appointed officials within the Islamic government to implement and establish the necessary conditions for the realization of divine decrees in both the physical and virtual realms. There is no realm of decrees beyond this realm of responsibility. However, it is important to note that the significance of each ruling and the consideration of public interests may vary. Therefore, in the implementation of guardianship and governance, priority is given to rulings that have social impact, consequences, and outcomes. This approach aims to create an Islamic living environment for the members of society.

Hence, it is incumbent upon the ruler or the governing bodies acting on their behalf to utilize the comprehensive and applicable principles of enjoining good and forbidding evil. Through careful groundwork and strategic planning, both in terms of infrastructure and policies, they should establish the justifications for implementing Islamic rulings in both physical and virtual spaces. This entails the essential task of monitoring and regulating the cyberspace, addressing its negative aspects while also fostering its positive elements. It is important to note that regulation may be necessary in certain domains, encompassing both negative and, in some cases, positive aspects.

3.3. The Supremacy and Authority of the Islamic Government

Acknowledging the comprehensive, all-encompassing nature of

Islam, supported by philosophical arguments in both classical and contemporary theology, entails the recognition of its teachings as superior to the rulings derived from prior religions, laws, and human-made legislations. This understanding, rooted in reason necessitates the authority of a government that upholds Islamic values and teachings. It becomes evident that honor and excellence are achieved through the implementation of Islamic ideology and principles in the governance and exercise of authority (Dargahi 2020, 104).

According to the interpretations of certain scholars, Quranic teachings, and the prophetic tradition (Montazeri Moghaddam 2011, 49; Katānī, n.d., 1: 205), it becomes imperative for individuals within the Islamic society, particularly the rulers and officials, to regulate and govern their actions in all domains in alignment with the progress of the Islamic state. The cyberspace is among these domains, as contemporary human life has expanded extensively within the realm of technology. This expansion has significantly impacted cultural, economic, social, political, and military systems, leading to the emergence of virtual reality as an influential element alongside the external and physical reality we experience.

Given the influence of non-Muslim entities over the content and structure of the virtual space, it becomes even more crucial to safeguard the dignity and prestige of the Islamic government in this realm. In particular, the emergence of cyberspace, currently under the direct influence of the United States (Bell 2010, 169), including the configuration of popular social networks such as Twitter, Facebook, and Google+, underscores this point. Consequently, it is essential to monitor and regulate the cyberspace, considering both its negative and positive aspects, with the aim of preserving the honor and dignity of the Islamic government and averting any potential harm, particularly cyber-attacks, as outlined in the preceding explanations.

It is important to note that based on the aforementioned three pieces of evidence, the need for monitoring and regulating cyberspace is evident. Such operations and activities should be carried out through an organized approach or mechanism, much like the establishment of an institution or a regulatory body. Furthermore, it is crucial to

develop a well-defined and comprehensive legal framework encompassing all aspects of cyberspace. This framework should be formulated through consensus and consultation with experts in the field. By doing so, it can serve as a standard for distinguishing between extreme and moderate practices within the context of monitoring and regulation.

4. Privacy Considerations in the Surveillance and Regulation of Cyberspace

Preserving individuals' privacy is a crucial aspect when it comes to the surveillance and regulation of cyberspace. In the subsequent discussion, we will briefly address the prohibition of privacy violations and its boundaries. We will then delve into the inherent conflict between the imperative to protect privacy and the necessity to monitor and regulate the virtual realm. This will be followed by a jurisprudential analysis of the relative prioritization of these two concerns, considering two different approaches. Finally, we will explore the jurisprudential criteria and factors that contribute to understanding this delicate balance.

4.1. Respect for Privacy and Its Scope

The authority to enter, gather information, and monitor individuals' privacy, as perceived by those who believe they are exempt from prosecution and legal consequences in this domain (see Eskandari 2010, 157), has led some authors to address specific examples of privacy in a dedicated, codified, and independent manner. Numerous articles emphasize the prohibition of privacy violations, drawing support from certain Quranic verses and hadiths. However, it is important to note that some of these propositions have limitations in their scope, lacking the necessary inclusiveness and generality to establish the prohibition of violating certain categories of privacy, such as information privacy and communication privacy. Their focus lies primarily on the prohibition of physical privacy violations, encompassing aspects related to physical space and sexuality.

For instance, verses that emphasize seeking permission before entering someone's house (Quran 24: 27-28) or family members seeking permission to enter their parents' room at specific times (Quran 24: 59; Kulaynī 1407 AH, 3: 67; Ṣadūq 1403 AH, 163)

primarily underline the importance of preserving individuals' spatial and sexual privacy (see Ṭabarsī 1994 and Makārim 1995, under those holy verses). On the other hand, certain hadiths that mention the legitimacy of self-defense in the face of violations of territorial integrity and the permissibility of using force, including shedding the aggressor's blood if necessary (Kulaynī 1407 AH, 7:290, 291), pertain to privacy violations within the context of spatial privacy (see Imam Khomeini 1403 AH, 1: 487; Sabzawārī 1413 AH, 28: 156).

Similarly, there are arguments concerning hadiths that highlight the obligation to keep one's secrets from others (Ṣadūq 1413 AH, 1:482) or the prohibition of revealing the secrets of others (Kulaynī 1407 AH, 2:359). While these hadiths underscore the significance of maintaining confidentiality, it is important to note that the obligation to keep secrets or the prohibition of revealing them is not directly linked to the prohibition of privacy violation. Thus, the arguments put forth by certain authors, relying solely on these narrations, may warrant scrutiny and further examination.

Certainly, Quranic verses (Quran 49: 12) and hadiths (Kulaynī 1407 AH, 2: 354, 355, and Majlisī 1403 AH, 71:7, 72: 252) explicitly state "do not spy," indicating that all forms of spying, regardless of the motive, are prohibited. The general nature of this prohibition extends to all categories of privacy, including information privacy and communication privacy. In essence, spying entails investigating and obtaining concealed information about matters that individuals consider private and personal (Ardabīlī, n.d., 417 and Ṭabāṭabāʾī 1417 AH, 18: 323).

Spying can be categorized into different types based on the underlying motives and intentions. It can be conducted with corrupt motives, aiming to harm a believer. Alternatively, it can be carried out without harmful intentions, driven by a mere curiosity to uncover hidden aspects of others' lives (which can be considered as intrusion). Furthermore, spying can also occur with good intentions. In such cases, it may serve a necessary purpose, such as uncovering instances of bribery, embezzlement, enemy forces, and similar matters. Additionally, there are instances where spying may be motivated by good intentions but is unnecessary, such as identifying qualified individuals for government positions and similar purposes (see Kharrazi 2001, 57).

All the aforementioned scenarios fall under the category of "spying," and based on the evidence provided by the term itself, the ruling of prohibition applies regardless of motives and motivations. It may be argued that the verse "do not spy" in the twelfth verse of Surah al-Hujurat, within its contextual framework, only prohibits spying with corrupt intentions in the affairs of believers, thereby excluding spying with good intentions and spying into the matters of hypocrites and disbelievers. However, it is evident that the nature of the matter does not prevent the application of the prohibition ruling in all cases since they all constitute instances of "spying" in general, regardless of the people involved or the specific circumstances. Even allowing open inspection, under the pretext of immorality, raises concerns (Imam Khomeini 1415 AH, 1: 278).

Furthermore, the application of the prohibition ruling on spying is not limited to the Quranic verse alone. A reliable hadith from Imam al-Ṣādiq (Kulaynī 1407 AH, 2:354) establishes the unequivocal prohibition of spying without any constraints or conditions.

Based on the perspective outlined earlier, which draws upon the evidence and the breadth of its implications, it can be concluded that spying on privacy, particularly in the realm of information and communications within both physical and virtual spaces, which individuals generally prefer to keep hidden from others, is considered haram (forbidden). This prohibition applies to all individuals and entities, including the government and governing bodies.

2.4 A Jurisprudential Analysis of Privacy Considerations being outweighed by Considerations of Cyberspace Monitoring and Regulation

Cyberspace possesses the unique characteristic of enabling users to conceal their identities, facilitating bold acts of theft, data denial, data manipulation, and an overall increase in cyber-attacks. Unlike the tangible world, the government's ability to swiftly respond to such deviations and their perpetrators is severely limited. Exploiting this aspect, adversaries target the Islamic system, tarnishing its reputation and sowing doubt among society members regarding Islamic beliefs, teachings, and

principles. This medium serves as a cost-effective tool for distorting the honor of the Islamic state and disseminating false news and misinformation, while also promoting social and Islamic abnormalities.

Given the possibility of anonymity in cyberspace, there arises the necessity to regulate and monitor its negative and positive aspects. This serves the purpose of identifying disruptive elements that may undermine micro or macro systems or pose significant threats to social interests. However, it is important to acknowledge that such regulation and monitoring can potentially encroach upon individuals' privacy within the cyberspace.

In further explanation, people's actions can be categorized into three states: purely personal with no social aspect, or having social effects that individuals attempt to contain, or possessing a social and general aspect inherent to the nature, essence, consequences, and outcomes of the action.

Monitoring and filtering of cyberspace, particularly in cases with a public aspect like the second and third cases, may inadvertently encroach upon personal privacy. These encroachments could be inevitable as a means to accomplish such measures. Consequently, it becomes essential to conduct a jurisprudential analysis of privacy violations resulting from the monitoring and regulation of cyberspace by governing bodies.

4.2.1. A Preliminary Hypothesis: Applying the Principle of "Priority of the More Important over the Less Important"

In the context of monitoring and regulating cyberspace, when assessing the trade-off between the advantages and disadvantages of privacy violation, the rule of "prioritizing the more important over the less important" comes into play. According to this rule, if the benefit derived from privacy violation outweighs its drawbacks, priority is given to the party with the more compelling justification (Meshkini, n.d., 87; Khoei 1420 AH, 4: 278). Additionally, it is worth noting that some scholars also reference this rule in relation to the principle that "the end (goal) does not justify the means" (Alidoost 2009, 453).

Given the displeasure of the religious legislator towards neglecting or abandoning the maintenance of the system and disregarding public interests, as well as violating the authority and dignity of the Islamic system, it can be inferred that the prohibition of spying and privacy infringement is a "potential" rather than

actualized ruling. As previously stated, the duty of the ruler within an Islamic government is to prioritize divine decrees within the societal context, even if certain decrees hinder the implementation of others. This underscores the importance of preserving the system and upholding the glory of the Islamic system.

Furthermore, it is crucial to establish the conditions for enforcing decrees by devising practical solutions during the implementation phase, particularly when conflicts arise. Resolving such conflicts becomes paramount in order to ensure the implementation of important matters or, in the event of violation or closure, to confine the impact to a minimum. Hence, within the context of monitoring and regulating cyberspace, which encompasses information gathering, uncovering hidden truths, and addressing anomalies and cyber-attacks, as previously elucidated, intruding upon individuals' privacy is not only permissible but also necessary and obligatory in cases of significant importance (refer to Kharazi 2001).

In addition to addressing the issue of conflicts when complying with jurisprudential rulings and the necessity of prioritizing the more important over the less important, another hypothesis is put forward to account for the jurisprudential aspect of privacy violations in the monitoring and regulation of cyberspace. This hypothesis is not without plausibility as some scholars of the principles of jurisprudence believe in the problem of "gradation" (*tarattub*) that the more and the less important rulings are simultaneously actualized (Sadr 1418 AH, 1:v340-39), in addition to the application of protecting the system and arguments in its favor in light of preserving public interests according to the earlier hypothesis.

4.2.2. The Second Hypothesis: Use of Secondary Titles and the Introduction of Secondary Rulings

As previously mentioned, the Islamic system was established with the purpose of upholding Islamic principles and implementing them according to pure Islamic teachings. The adherence to these teachings by individuals within society stands as a prominent factor in safeguarding the Islamic system and government. To illustrate this point, it is imperative for everyone, including both natural and legal entities, to refrain from infringing upon the privacy of individuals, where this obligation stems from the prohibition of prying into and spying on the confidential matters of others. Failure

to fulfill this obligation by members of society can significantly undermine the integrity of the Islamic system.

As pointed out earlier, the preservation of the Islamic system is intricately linked to the collective welfare of society. It is the responsibility of the society to safeguard the system and prevent any harm, disruption, hardship, emergency, or other factors that may jeopardize its stability. Now, let us consider a scenario where maintaining the system conflicts with certain fundamental principles or implementing those principles leads to the disruption of the system in specific circumstances. In such cases, as the circumstances or titles change, the corresponding Islamic rulings must also adapt accordingly. When primary titles shift, the applicable ruling must adjust, and when secondary titles emerge, corresponding secondary rulings come into play.

In other words, adhering to the principle of not violating individuals' privacy and upholding the primary ruling of the prohibition of spying can, in certain cases, lead to the disruption of the Islamic system. In these situations, the public interest of society becomes compromised due to the violation of the primary ruling. Consequently, this shift in circumstances necessitates a transformation of the ruling from the primary ruling to the secondary ruling of legitimacy, where the violation of privacy becomes both permissible and obligatory in order to protect the overall integrity of the system.

Therefore, if government agencies were to cease entering people's privacy during the process of monitoring and regulating cyberspace, specifically in the context of uncovering and tracking hackers and perpetrators of cyber-attacks, under the pretext of preserving the system and safeguarding the public interests of society, a secondary ruling permits such actions. In fact, based on the importance of certain examples, it may be deemed necessary to violate privacy. This is what Imam Khomeini meant when he said, "[spying] is obligatory for the preservation of Islam and the preservation of the lives of Muslims" (Imam Khomeini, 15: 116).

4.3. Jurisprudential Elements of Privacy Violation in the Process of Monitoring and Regulating Cyberspace

The process of prioritizing the more important over the less important or determining the secondary ruling relies on recognizing the significance or relevance of the secondary title. Consequently, the primary criterion used to assess the legitimacy of government institutions

encroaching upon people's privacy, particularly in cyberspace monitoring and regulation, is knowledge rather than mere assumptions or speculative reasoning. In other words, there must be specific knowledge, or at the very least general knowledge, that it is impossible to protect the system or establish religion or the Islamic government without infringing the privacy of certain individuals during the monitoring and regulation of cyberspace.

In essence, when discussing the importance of preserving the public interest or the honor of the Islamic government as the primary consideration in the first hypothesis, or the secondary title of preserving the system in the second hypothesis, it becomes necessary to clearly define the scope of individuals who need to be subject to control and surveillance by governing bodies in the process of monitoring and regulating cyberspace. For example, in order to track and identify perpetrators of cyber-attacks on the country's fuel distribution system, it may be imperative to monitor the activities of specific individuals in cyberspace and intrude upon their privacy within this realm. Thus, engaging in discussions about prioritizing the more important or proposing a secondary ruling is not permissible when it comes to other individuals, and violating their privacy based on mere assumptions and speculations would lack jurisprudential legitimacy.

The second aspect regarding the legitimacy of violating people's privacy through monitoring and regulating cyberspace is that it should be limited to the extent of necessity. The application of secondary titles, such as maintaining the system, protecting public interests, or upholding the honor of the Islamic state, becomes doubtful beyond this particular extent. By default, the principle should not apply in those situations.

In the scenario mentioned above, it is possible to determine the relevant dimensions of governing bodies by examining a specific set of data within the realm of general knowledge, without the need to violate other data, location privacy, or the privacy of individuals and their dependents. In such cases, the principles of prioritizing the more important or secondary titles do not apply, and therefore further unwarranted investigations are not considered legitimate. However, it should be noted that if competent authorities recognize the necessity of such actions in specific instances, it becomes legitimate and even obligatory based on the significance of the matter. This may be the only

viable approach to safeguard the honor of the Islamic government, protect the Islamic system, or establish religious principles.

One aspect of monitoring and regulating cyberspace, in order to safeguard the Islamic system and establish religious principles, is to prevent the dissemination of indecency within society and take action against those who promote it on the internet. However, when assuming the legitimacy (both permissible and obligatory) of violating individuals' privacy, it is crucial that such encroachments, carried out by governing bodies within the limits of general knowledge and necessity as previously explained, do not contribute to the spread of indecency or expose the faults and hidden secrets of individuals.

This aspect is based on evidence for the prohibition of spreading indecency. It is supported by the holy verse, "Indeed those who want indecency to spread among the faithful—there is a painful punishment for them in the world and the Hereafter, and Allah knows and you do not know" (Quran 24:1 9), as well as similar themes found in hadith sources (e.g., Ṭūsī 1414 AH, 357). The spreading of indecency is considered one of the actions for which severe punishments, both in this world and the Hereafter, are promised.

The afterlife punishment mentioned in the verse indicates the prohibition of this act from a jurisprudential standpoint. Furthermore, the verse's reference to a worldly punishment for spreading indecency could encompass both Sharia punishments and the individual and social consequences that arise from such actions. Quranic exegetes have interpreted the meaning of "spreading indecency" to encompass a broad range of acts involving the dissemination of indecent content under any circumstances. Therefore, it is incorrect to restrict its meaning solely to lies and baseless accusations and their dissemination (see Ṭabāṭabāʾī 1417 AH; Makarim 1995).

During the monitoring and regulation of cyberspace, government agencies may come across mistakes and wrongdoings unrelated to the specific issue being investigated while encroaching upon people's privacy. Such cases are prevalent in societies where faith is weak. However, it is important to prevent the spread of these cases. By doing so, not only can we uphold the sanctity and honor of individuals, but we can also avoid the desecration that would occur through the dissemination of these flaws and wrongdoings, which would be considered as spreading indecency.

These issues are addressed in the fifty-third letter of Nahj al-Balaghah by

Imam ʿAlī (a). It highlights that in intelligence activities aimed at gathering information about the integrity of government officials, there may be instances where the ruler becomes aware of certain matters that should remain hidden. In such cases, it is necessary to refrain from revealing the hidden faults and avoid defaming individuals in all information-related practices, including the exercise of authority during the monitoring and regulation of cyberspace.

Conclusion

In light of the evidence pointing to the importance of protecting the Islamic system, establishing religion, and maintaining the supremacy and authority of the Islamic state, it is crucial to analyze and apply these principles to the realm of cyberspace. In order to achieve an Islamic way of life through the negative and positive monitoring and regulation of cyberspace, governing actions must be carried out while simultaneously ensuring the privacy of individuals within society is preserved.

In situations where conflicts arise between the need to preserve privacy and the process of monitoring and regulating cyberspace, it is important to consider the principle of prioritizing what is more important over what is less important. Additionally, introducing secondary considerations can help inform the decision-making process. In this context, it can be argued that monitoring and regulating cyberspace, even if it involves violating individuals' privacy, can be deemed legitimate based on these two hypotheses. Moreover, depending on the significance of the matter at hand, it may even be considered obligatory.

The legitimacy of entering into individuals' privacy during the process of monitoring and regulating cyberspace is contingent upon certain conditions that serve as criteria for evaluating the validity of such violations. These conditions include having knowledge, even if it is general knowledge, limiting the violation to the extent of necessity, and ensuring that any hidden flaws or defects discovered by governing bodies in the process are not disclosed. These three conditions are essential for legitimizing governmental intervention into individuals' privacy during the monitoring and regulation of cyberspace.

References

The Holy Quran

Nahj al-Balaghah

1. Alidoost, Abolghasem. 2009. *Fiqh wa maṣlaḥat*. Tehran: Publications of Research Institute of Islamic Culture and Thought.

2. Andalibi, Reza, and Dargahi, Mahdi. 2015. *Ḥajj wa wilāyat faqīh*. Tehran: Mashʿar Publications.

3. Ardabīlī, Aḥmad b. Muḥammad. n.d. *Zubdat al-bayān fī aḥkām al-Qurʾān*. Tehran: Maktabat al-Jaʿfariyya li-Ihyaʾ al-Athar al-Jaʿfariyya.

4. Bell, David. 2010. *Darāmādī bar farhang cyber*. Translated by Masoud Kowsari and Hossein Ghomi. Tehran: Jame'eshenasan Publications.

5. Dargahi, Mahdi. 2020. *Mabānī-yi fiqhī-yi ʿizzat, ḥikmat, wa maṣlaḥat dar taʿāmulāt bayn al-milalī-yi dawlat Islāmī*. Ḥukūmat Islāmī 25, no. 2 (summer): 101-20.

6. Eskandari, Mostafa. 2010. *Māhiyyat wa ahammiyyat ḥarīm khuṣūṣī*. Ḥukūmat Islāmī 15, no. 4 (winter): 148-76.

7. Esmaeeli, Mohsen, and Mohammad Sadegh Nasrollahi. 2016. *Pālāyish faḍāyi majāzī: ḥukm wa masāʾil ān az dīdgāh fiqh*. Dīn wa Irtibāṭāt 23, no. 1 (spring and summer): 53-80.

8. Ghazi (Shariat Panahi), Abolfazl. 2004. *Ḥuqūq asāsī wa nahād-hāyi siyāsī*. Tehran: Mizan Publications.

9. Ḥāʾirī al-Yazdī, Shaykh ʿAbd al-Karīm. 1418 AH. *Durar al-fawāʾid*. Qom: Islamic Publishing Institute.

10. Ḥāʾrī, Sayyid Kāẓim al-Ḥusaynī. 1424 AH. *Wilāyat al-Amr fī ʿaṣr al-ghayba*. Qom: Majmaʿ Andisheh Islami.

11. Ḥillī, Jaʿfar b. al-Ḥasan. 1412 AH. *Al-Nihāya wa-Nukatihā*. Qom: Islami Publications.

12. Ḥillī, Jaʿfar b. al-Ḥasan. 1415 AH. *Sharāʾiʿ al-Islām*. Qom: al-Maʿarif al-Islamiyya.

13. Ḥur al-ʿĀmilī, Muḥammad b. al-Ḥasan. 1409 AH. *Wasāʾil al-Shīaʿa*. Qom: Al al-Bayt Institute.

14. Imam Khomeini, Seyyed Ruhollah Musavi. 1415 AH. *Al-Makāsib al-Muḥarrama*. Qom: Institute for Compilation and Publication of the Works of Imam Khomeini.

15. Imam Khomeini, Seyyed Ruhollah Musavi. 1421 AH. *Kitāb al-bayʿ*. Qom: Institute for Compilation and Publication of the Works of Imam Khomeini.

16. Imam Khomeini, Seyyed Ruhollah Musavi. 1999. *Ṣaḥīfi-yi Imām*. Qom: Institute for Compilation and Publication of the Works of Imam Khomeini.

17. Imam Khomeini, Seyyed Ruhollah Musavi. n.d. *Taḥrīr al-wasīla*. Qom: Dar al-ʿIlm Press Institute.

18. Jafari Langroodi, Mohammad Jafar. 2017. *Tirmīnulujī-yī ḥuqūq*. Tehran: Nashr Ganj.

19. Javadi Amoli, Abdollah. 2013. *Payām hamāyish ʿilmī-yi faḍā-yi majāzī*. Esra International Foundation for Revelatory Sciences, Office of Archives, Documents, and Sources, Vahid Taip, 21/1/2015.

20. Katānī, Muḥammad ʿAbd al-Ḥayy. n.d. *Niẓām al-ḥukūmat al-nabawiyyat al-musammā al-tarātīb al-idāriyya*. Beirut: Shirka Dar al-Arqam ibn Abi l-Arkam.

21. Kharrazi, Seyyed Mohsen. 2001. *Kāwishī dar ḥukm fiqhī-yi Tajassus. Fiqh Ahl Bayt*, no. 26 (summer): 54-142.

22. Khoei, Sayyid Abu al-Qasim al-Musawi, al-. 1420 AH. *Ajwad al-Taqrīrāt*. Lectures of al-Muḥaqqiq al-Nāʾīnī. Qom: Mostafavi Publications.

23. Kulaynī, Muḥammad b. Yaʿqūb. 1407 AH. *Al-Kāfī*. Qom: Dar al-Kutub al-Islāmiyya.

24. Majlisī, Muḥammad Bāqir. 1403 AH. *Biḥār al-Anwār*. Beirut: al-Wafa Institute.

25. Makarim Shirazi, Nasser. 1995. *Tafsīr Nemūneh*. Tehran: Dar al-Kutub al-Islamiyya.

26. Malek Afzali, Mohsen, Mohammad Hassan Haeri, Mohammad Taghi Fakhlaee, Mohammad Javad Arasta. 2012. *Mafhūm niẓām wa kārburd ān dar fiqh wa uṣūl*. Fiqh wa Uṣūl, no. 88 (spring): 129-33.

27. Meshkini, Ali. 1413 AH. *Iṣṭilāḥāt al-uṣūl*. Qom: Islamic Publishing Office.

28. Momen Ghomi, Mohammad. 1425 AH. *Al-Wilayat al-ilāhiyyat al-Islāmiyya*. Qom: Islamic Publishing Office.

29. Montazeri Moghaddam, Hamid. 2011. *Barrasī-yi Tārīkh ṣulḥ-hāyi Payāmbar (s)*. Qom: Imam

Khomeini Education and Research Institute.

30. Montazeri Najafabadi, Hossein-Ali. 1409a AH. *Dirāsāt fī wilāyat al-faqīh*. Qom: Tafakkor Publications.

31. Montazeri Najafabadi, Hossein-Ali. 1409b AH. *Mabānī-yi Ḥukūmat Islāmī*. Translated by Mahmoud Salavati and Abolfazl Shakouri. Qom: Keyhan Institute.

32. Najafī, Muḥammad Ḥasan. 1404 AH. Jawāhir al-kalām. Beirut: Dar al-Turath al-ʿArabi.

33. Sabzwārī, Sayyid ʿAbd al-Aʿlā. 1413 AH. *Muhadhdhab al-aḥkām*. Qom: al-Manar Institute.

34. Ṣadūq, Muḥammad b. ʿAlī b. Bābawayh. 1403 AH. *Maʿānī al-Akhbār*. Qom: Islamic Publishing Office.

35. Ṣadūq, Muḥammad b. ʿAlī b. Bābawayh. 1413 AH. *Man lā yaḥḍuruh al-Faqīh*. Qom: Islamic Publishing Office.

36. Tabatabaee, Seyyed Alireza, and Mohammad Al Layali. 2018. *Qawāʿid fiqhī-yi pālāyish faḍāyi Majāzī*. Ḥukūmat Islāmī 23, no. 1 (spring): 85-116.

37. Tabatabaee, Seyyed Mohammad Hossein. 1417 AH. *Al-Mīzān fī Tafsīr al-Qurʾān*. Qom: Islamic Publishing Office.

38. Ṭabrasī, Faḍl b. al-Ḥasan. 1994. *Majmaʿ al-Bayān fī Tafsīr al-Qurʾān*. Tehran: Naser Khosrow Publications.

39. Ṭūsī, Muḥammad b. al-Ḥasan. 1414 AH. *Al-Amālī*. Qom: Dar al-Thiqafah.

40. Ṭūsī, Muḥammad b. al-Ḥasan. 1997. *Al-Iqtiṣād al-hādī ilā Ṭarīq al-Rashād*. Tehran: Chehel Sotun Publications.