Negative Interventions and Filtering Measures in the Exercise of Sovereignty over Cyberspace within the Framework of Iranian Law

1. Navid Fathollahi: PhD Student, Department of Public Law, Science and Research Branch, Islamic Azad University, Qeshm, Iran
2. Ali Rostamifar*: Assistant Professor, Department of Law, Science and Research Branch, Islamic Azad University, Qeshm, Iran
3. Thirdname Lastname: Assistant Professor, Department of Law, Science and Research Branch, Islamic Azad University, Qeshm, Iran

*Correspondence: arq119@yahoo.com

Abstract

Across the globe, discourse surrounding the internet consistently centers around a fundamental tension between two competing principles: the right to freedom of expression and free networking on the one hand, and the sovereign right of states to control public order and safeguard national interests on the other. This study, conducted using a descriptive-analytical method and library-based sources, investigates state-imposed restrictive interventions, with a particular focus on the current challenges facing the Islamic Republic of Iran. It was observed that the central issue in Iran's cyberspace—mirroring that of many other countries—is the conflict between internet sovereignty and network power (in a general sense) versus national sovereignty and authority. The findings of the study indicate that the state's negative intervention through filtering tools has proven ineffective. Therefore, there is a critical need to redesign the relationship between the state's sovereignty and citizens' rights to access cyberspace. Redefining this relationship entails a dual approach encompassing both "governance with cyberspace" and "governance over cyberspace," wherein a proper balance must be established between national sovereignty and internet sovereignty (arising from networked power). Accordingly, the redefinition of these relations should, in terms of purpose, aim to guarantee national independence and preserve the country's sovereign integrity, and, structurally and operationally, be realized through the development and expansion of the National Information Network (NIN). The principal component in formulating a desirable policy framework for cyberspace governance in the Islamic Republic lies in preserving sovereignty through a redesigned relationship between the state and cyberspace, while simultaneously protecting the internet rights of citizens. This redesign, which serves as the cornerstone of the Islamic Republic's cyberspace policy theory, must also be supported by additional elements, including appropriate tools and governance processes.

Keywords: Internet, Sovereignty, Cyberspace, Internet Governance, State Secrets, Internet Challenges.

Received: 10 March 2024
Revised: 14 April 2024
Accepted: 2 May 2024
Published: 21 May 2024

Citation: Fathollahi, N., Rostamifar, A., & Seraji, M. (2024). Negative Interventions and Filtering Measures in the Exercise of Sovereignty over Cyberspace within the Framework of Iranian Law. *Legal Studies in Digital Age,* 3(2), 345-354.

1. Introduction

The existence and diversity of structures within a political system signify the expansion of individuals' spheres of power and a corresponding limitation of the state's control—one such domain being the internet. Nearly all scholars in the field of political development consider structural diversity as an indicator of development, typically present in systems where governance is not exercised through centralized means. Diversity arises when a system becomes more complex. Huntington notes that if a society evolves from simplicity to complexity, it is on a path toward development, and naturally, the more communication structures there are, the greater the volume of interactions. However, this is contingent on whether these structures and substructures of communication are autonomous. If these structures lack independence and act as state mouthpieces, the volume of transmitted information may be high, but its diversity is not.

From the discussion on the functions of political systems in relation to communication tools, we conclude that political systems operate in three areas—political socialization, political recruitment, and political communication—in order to maintain control within their sovereign territory. In these activities, the political system attempts to dominate its subjects through the regulation of political socialization agents, especially communication media, the control of content in communicative exchanges, and targeted political recruitment (Ayazi & Pakzad, 2021). It appears that modern communication tools enhance the regulatory, symbolic, and distributive capacities of political systems. In other words, political systems with strong presence in the aforementioned areas leverage these tools to reinforce centralized governance. Therefore, this study investigates the restrictions imposed by the state in cyberspace and the related challenges in Iran.

This research employs a descriptive-analytical methodology. Through description and visualization, the researcher interprets and evaluates the data. Naturally, anyone engaging in a research project must initially possess both interest in and partial familiarity with the subject before conducting the study. I selected this topic for several reasons, and given its relevance to current internet and cyberspace conditions in Iran, I have drawn upon the views of esteemed scholars, synthesized them in this study, contributed my own insights, and offered recommendations.

2. Internet Governance Models

The policies governing cyberspace in any society reflect, on one level, that society's value orientations and epistemic frameworks, and on another, its infrastructural, institutional, and executive capacities. In other words, the mechanisms and processes that societies prioritize in their approach to internet governance reveal differing levels of capability and executive authority (Ameli & Hassani, 2018).

Five governance models for the internet have been identified:

1. **Self-Organizing Cyberspace Model**: Based on the idea that the internet is a domain of self-governed individual freedoms and that state control cannot—and should not—intervene in it (Cory, 2017).
2. **International Organizations and Institutions Model**: Based on the notion that internet governance inherently transcends national boundaries and that the most appropriate governing bodies are semi-private international cooperatives or treaty-based international organizations formed by national governments (Faris & Villeneuve, 2008).
3. **Code and Internet Architecture Model**: Based on the idea that many regulatory decisions should be embedded in communication protocols and other software that shape the internet's functional architecture.
4. **National Governments and Law Model**: Based on the view that as the internet becomes a foundational infrastructure within countries, regulatory decisions must be made by national governments through legal and statutory mechanisms (Bygrave & Bing, 2009).
5. **Economic and Market Regulation Model**: Based on the assumption that market forces will guide fundamental decisions about the nature and structure of the internet (Paige Toohey, 2013).

3. Negative Interventions through Filtering Tools in Iran

This section begins by examining the methods of filtering in Iran to clarify the mechanisms of implementation. It then discusses the perspective of state authorities toward filtering and the justificatory rationales as understood at the decision-making levels in the country.

3.1. Methods of Filtering in Iran

Identifying prohibited web pages and filtering them is carried out through several methods. The most common approaches employed in Iran are as follows:

1. **IP Address-Based Filtering**: This method was used in the early years of filtering in Iran. Due to its high error rate and widespread criticism by experts and users, it was eventually abandoned. In this method, the four-part IP address of the server hosting the prohibited site would be blocked. The major flaw in this approach is that most websites use shared hosting services. Thus, if a single restricted website is hosted on a server shared by a thousand other websites, blocking the IP address would make all those websites inaccessible. This form of filtering led to the temporary blocking of several official and government websites a few years ago, prompting filtering authorities to realize the need for a more refined method (Nasrollahi, 2019).
2. **Domain Name and URL-Based Filtering**: This is the primary method of filtering globally. In this method, a database is maintained containing a list of prohibited URLs. The filtering software compares any requested URL against this database and filters it if a match is found. The downside for filtering authorities is that thousands of new websites emerge daily, many of which may need to be blacklisted. However, users often have access to these sites for a period before the blacklist is updated. Therefore, regular updates to the database are necessary (Castells, 2022).
3. **Keyword-Based Filtering**: This method involves compiling a list of banned keywords. Filtering software scans requested URLs or search engine entries for these keywords. If found, access is denied with an error message. This method is highly error-prone and has been the source of most complaints regarding filtering in Iran (Nasrollahi, 2019). For example, words like “woman,” “girl,” and “love” are banned keywords in Iran, likely because such words may appear in URLs of pages with immoral content. However, filtering authorities, especially in earlier years, did not consider that not all pages containing these keywords were inappropriate. As a result, users were denied access to thousands of harmless or even beneficial pages. For instance, even some sections of the websites of religious authorities that addressed women's issues were inaccessible because the term “woman” was entirely filtered out (Mehdi-Pour, 2020).
4. **Content-Based Filtering**: Known globally as content filtering, this method is less commonly used in Iran. The software evaluates the page content after receiving a user’s request, and filters the page if it contains prohibited terms. This method is not suitable for large-scale national filtering and is primarily used on a limited scale (Motamed-Nejad & Motamed-Nejad, 2019).
5. **Integrated Filtering Based on New National Filtering Framework**: Since the winter of 2009, a new national filtering strategy has been implemented, combining both URL and keyword-based filtering methods simultaneously (Shirzad, 2020).

3.2. Authorities’ Perspective on Filtering and Its Legal Framework in Iran

When Iran’s digital communication infrastructure first emerged, few anticipated that the highest state official would one day need to issue a formal written order for monitoring and supervising cyberspace. However, with the Supreme Leader’s decree establishing the *Supreme Council of Cyberspace*, the importance of monitoring online content became increasingly apparent. In 2002, filtering became a serious matter of state concern (Zarei, 2006). A three-member committee was formed, including representatives from the Ministry of Intelligence, the Ministry of Culture and Islamic Guidance, and the Islamic Republic of Iran Broadcasting (IRIB) (Nasrollahi, 2015). Later, representatives from the Secretariat of the Islamic Council and the Islamic Propagation Organization were added. The committee initially distributed a list of 111,000 banned websites to internet service providers (Ameli & Hassani, 2018).

3.3. Public Order and Authority in the Realm of Filtering

France is considered the origin of the legal concept of *public order*, which has gradually entered the legal frameworks of other countries. In English legal contexts, it is often referred to as "public policy" or "public order" (Rahaei, 2019, p. 132). Notably, all related concepts—including national security, privacy, and public order—used by state institutions in Iran to justify internet filtering are inherently ambiguous and offer broad interpretative flexibility. These concepts function as essential components in a puzzle that was once perceived as disjointed but is now revealing its internal coherence. The institutional authority of the state, in its display of control, relies heavily on this ambiguity (Vincent, 2017).

Content filtering or blocking through blacklists is used in many countries. In some states, compiling these blacklists is the responsibility of government agencies and officials. In more liberal states, this function is fulfilled through user complaints and self-regulation mechanisms. Consequently, self-regulation is generally regarded as more favorable in terms of protecting freedom of expression and access to information because these fundamental rights are not compromised by government entities (Shahbazi-Nia et al., 2013). However, this does not imply that the positive rights resulting from self-regulation are inherently protected by those mechanisms. Therefore, it is necessary to establish formal mechanisms within the governance structure to resolve disputes in this domain. Accordingly, the judiciary emerges as the competent institution responsible for its fundamental mission—resolving disputes between governmental entities and the public, and safeguarding citizens' fundamental rights in the face of state power. The objective here is to empower individuals who, through a bottom-up approach, exert pressure on the state to adopt human rights-based protective policies for the internet and cyberspace (Seljuqi, 2010).

4. Key Challenges to Iranian Sovereignty in Relation to the Internet

Before outlining the Islamic Republic of Iran's policy theory toward cyberspace, it is essential to briefly explain the current state of cyberspace in Iran. At the beginning of this section, the primary issue concerning cyberspace in Iran is introduced, followed by an explanation of other existing challenges, all of which relate to the central issue.

4.1. Concern Over the Erosion of Sovereignty

The fundamental issue the Islamic Republic faces in relation to cyberspace can be framed as a tension between national sovereignty and networked sovereignty (Madnian et al., 2011). More precisely, the underlying concern that explains many other challenges in Iran's cyberspace is the potential erosion of national sovereignty due to the rising power of cyberspace and networked structures (Nasrollahi, 2015).

Before detailing this overarching issue, the researcher deems it necessary to clarify the relationship between governance and cyberspace. Governance can be divided based on the tools it uses—1) traditional, and 2) via cyberspace—and based on its domain—1) governance over the physical world, and 2) governance over cyberspace. These can be summarized as "governance over cyberspace" and "governance through cyberspace." Accordingly, four configurations are logically conceivable: 1) traditional governance over the physical world, 2) traditional governance over cyberspace, 3) governance through cyberspace over the physical world, and 4) governance through cyberspace over cyberspace (Rahmati & Shahriari, 2017).

While traditional governance over the physical world is the conventional exercise of state authority and not directly relevant to this study, most current Iranian policy discussions focus on traditional governance over cyberspace. This includes strategies aimed at controlling and directing cyberspace. Although this model covers an essential part of cyberspace governance, the other two configurations—governance through cyberspace over the physical world and over cyberspace itself—are of greater significance. The relative neglect of these latter forms of governance by Iranian policymakers and strategic documents is a central issue and defining feature of the current policy landscape (Sadeghi, 2005).

In continuing the explanation of Iran's core issue with cyberspace, it is worth emphasizing that the increasing intelligence and networked nature of power creates conflict between traditional sovereign authority and the emergent power of cyberspace actors. This challenge affects both governance *over* cyberspace and physical space, as well as governance *through* cyberspace. In Iran, these tensions manifest in line with the four types of power in a networked society as identified by Castells (Castells, 2023).

Regarding network-making power—that is, the power of actors and organizations operating within networks—examples include conflicts involving influential media actors empowered by the network, such as prominent Telegram channels, Twitter accounts, and Instagram pages that shape the public sphere. Concerning networked ownership power, which refers to control and access to information flows, notable examples include the dominance of global tech corporations like Google and Facebook over segments of the global and Iranian information exchange via services such as Gmail, YouTube, WhatsApp, and Instagram (Castells, 2023).

In terms of network standard power, which pertains to how platform standards constrain users, instances include the restrictions imposed by platforms like Instagram and Telegram on Iranian users and the Iranian government—for example, their refusal to comply with Iranian regulatory frameworks. Finally, the power to program and reprogram networks is evident in the political influence exerted by social media platforms like Facebook and Telegram in recent years, which have significantly shaped political communications and mobilization in Iran (Mehdi-Pour, 2020).

Given that the Islamic Republic's primary cyberspace-related concern is to prevent the erosion of national sovereignty and to establish a favorable balance in its favor, two major barriers obstruct this objective:

1. Reductionist policymaking approaches dominate decision-making and implementation processes. Reducing cyberspace to merely its technical dimensions leads to both developmental and restrictive policies being implemented in a narrow, infrastructure-focused way, excluding the human, social, and societal impacts of cyberspace technologies.
2. A lack of consistent regulatory enforcement in the exercise of cyberspace governance in Iran results in fragmented authority and inconsistent application of control measures (Post, 2016).

4.2. Independence of Cyberspace

Cyberspace independence, as a pillar of national sovereignty in Iran, faces two major challenges: 1) extensive dependency on the global internet network, and 2) weaknesses in corporate power and dominance. The first challenge stems from a lack of managed dependency on the global network and is exacerbated by the deep reliance of individual and institutional users across infrastructure, service, and content layers on international platforms. The second challenge involves a form of dependency arising from corporate dominance, particularly the influence of foreign-origin companies operating in Iran's digital economy. Despite their relevance, such concerns have often been overlooked in national-level cyberspace strategies. Entities like Sarava and the Iran Internet Group, as major investment consortiums with extensive portfolios in Iran's digital market, exemplify the issue of externally rooted corporate dominance (Jalili, 2021).

4.3. Security and Political Concerns

Security and politics are inseparable dimensions of cyberspace and are universally recognized as vital issues. However, in Iran, these concerns carry even greater significance, as a substantial portion of the Islamic Republic's policy theory on cyberspace revolves around a securitized perspective. Understanding the interplay between security, politics, and cyberspace in Iran requires acknowledging three critical issues.

The first issue is the prioritization of a security-oriented perspective in technology policymaking—particularly regarding cyberspace (Nasrollahi, 2019). A securitized lens results in policies that aim to restrict or delay access, which, in turn, hampers timely and intelligent digital development. The second issue is policy volatility, driven by fluctuations in Iran's political climate. These oscillations turn the expansion of cyberspace into a political bargaining chip among various factions, undermining consistent policymaking across different administrations and contributing to gaps in strategic planning and execution (Jalili, 2021).

The third issue is the instrumentalization of cyberspace as an alternative political media platform. Because the Islamic Republic of Iran Broadcasting (IRIB) holds a constitutional monopoly over audiovisual broadcasting and is institutionally independent from the executive and legislative branches, successive governments have increasingly viewed cyberspace—and especially social media—as powerful, alternative channels for political communication and public engagement (Rahmati & Shahriari, 2017).

4.4. Audience Engagement

The core issue in the domain of audience engagement within cyberspace relates to two key problems. First is the lack of an economic model for developing digital content and services. Due to the absence of a coherent and clearly defined commercial framework, many cyberspace policies in Iran that aim to support domestic platforms and services often default to rudimentary and ineffective strategies, such as the allocation of direct subsidies and preferential treatment for domestic platforms through the blocking of foreign counterparts. For instance, despite the seemingly favorable conditions created by restricting access to international platforms, domestic services like Aparat, Rubika, Bale, Esam, and Eitaa have failed or achieved only minimal success when compared to globally renowned video-on-demand platforms such as Netflix and YouTube. The second issue, which stems partly from the first, is the underdevelopment of Iran's cyberspace market, especially the absence of significant investment and the inability to cultivate tech companies at the scale of unicorns and decacorns (Mir-Mohammadi, 2012).

4.5. Regulations and Legislation

Laws and regulations are a foundational pillar of global internet governance. The principal issue in Iran is the absence of specialized legislation regarding cyberspace and the lag in legal development. Much of the existing policy documents and regulatory frameworks are generalized and non-specialized, merely outlining broad principles without addressing the nuanced realities of cyberspace. This legislative delay has left Iran with outdated laws, contributing to inefficiencies and legal gaps that hinder technological governance (Ansari, 2018a, 2018b). Key domains such as the digital economy, user privacy (for both individuals and institutions), the scope of online media and social networks (domestic and international), and deficiencies in laws like the Electronic Commerce Act and the Computer Crimes Law, along with vague documents like the Internet of Things Strategy issued by the Supreme Council of Cyberspace, exemplify this problem (Nasrollahi, 2015).

4.6. Passive Digital Diplomacy

In the broader environmental and geopolitical context of cyberspace policymaking, the nature of the Islamic Republic of Iran's interactions with global governments, institutions, and forums is a major issue. Two core problems characterize this domain. First, is the monopolistic and unilateral dominance of the United States in global internet governance, to which Iran has responded with a static and passive stance toward international digital norms, policies, and standards. Second, is Iran's absence or ineffective, symbolic, and unprofessional participation in international decision-making bodies and cyberspace forums. These two challenges have significantly hindered Iran's digital diplomacy, rendering it reactive and ineffective (Jalali Farahani, 2017).

4.7. Anxiety and Conflict from Participation in the Global Internet

The theoretical debate surrounding whether to maintain, modify, or sever Iran's participation in the global internet constitutes a critical and defining issue. This debate contributes to the pendulum swings seen in cyberspace policymaking and extends into every layer and domain of digital governance. In practice, this duality manifests either through contradictory policies such as expanding internet bandwidth while increasing censorship or through Iran's deep technological dependency across all layers of cyberspace on powerful foreign states and companies. Such dependencies have severely curtailed the sovereign capacity of the Islamic Republic in cyberspace governance and threaten national sovereignty and independence (Vakili, 2014).

4.8. Misconceptions About Cyberspace

One major cause of flawed governance perceptions arises from a failure to grasp cyberspace as a paradigm-shifting phenomenon that transforms various dimensions of Iran's social life. The first issue here is the belief among policymakers that it is possible to offer a fully sanitized version of the internet to users. However, considering the inherently mass-based, user-

driven nature of cyberspace, such a vision is practically unfeasible and leads to excessive public expenditure and ineffective policy outcomes (Ma'refat, 2014).

The second issue is the lack of an ecosystemic and holistic understanding of cyberspace. Many Iranian policymakers and mid-level managers approach cyberspace through a fragmented, one-dimensional lens and fail to see it as an extension of real societal life. Conceptual distortions further reinforce the belief that cyberspace is a non-essential or luxury domain within the country's bureaucratic and administrative structures (Ma'refat, 2014).

The third and perhaps most critical cognitive issue complicating the resolution of digital governance challenges in Iran is the presence of radical philosophical perspectives on technology. These views stem from a dualistic understanding of the relationship between culture and technology and manifest in two problematic orientations. One is essentialist and deterministic, exhibiting a technophobic disposition that aligns with neo-Luddite tendencies, leading to fear and avoidance of technology. The other is purely instrumentalist and techno-utopian, endorsing a simplistic and linear link between technological advancement and national progress. Both extremes fail to acknowledge the complex, multifaceted relationship between technology, culture, and society. As a result, current policy theory in Iran often reflects a threat-centric stance toward cyberspace, relying heavily on either direct confrontation and restriction or maximum localization strategies (Qasemi, 2019).

4.9. Lack of Long-Term Strategic Planning

Another key problem in Iran's cyberspace policy landscape is the discontinuity in long-term planning and execution. This fragmentation is observable in both policymaking and implementation. Divergences in vision among top officials and structural changes have led to frequent policy shifts, delays, and even halts in important national programs. Examples include the inconsistent development of the National Information Network and varying policies on international internet bandwidth expansion. These illustrate the structural discontinuities that characterize the current state of cyberspace governance (Qajar Qoyunlu, 2022).

4.10. Multiplicity of Policymakers and Executive Decision-Makers

The absence of a unified governance mechanism and centralized executive framework represents a fundamental structural issue. This problem has three dimensions. First, are theoretical and operational disagreements among policymakers and implementers, making unified consensus difficult. Second, are structural overlaps and jurisdictional conflicts that lead to multiple authorities attempting to regulate cyberspace. Third, is the fundamental weakness of the Supreme Council of Cyberspace, which has contributed to the first two problems. This structural weakness includes the council's lack of enforcement power to implement its policies and regulations. Consequently, the council has failed to function as the "single window" for cyberspace policymaking in the Islamic Republic, thus undermining its founding purpose (Rahai & Maleki, 2019; Rahmati & Shahriari, 2017).

The two core structural weaknesses of the Supreme Council of Cyberspace are: 1) the legal ambiguity regarding its position relative to the Iranian Parliament and the undefined boundaries in legislative authority over cyberspace, and 2) the absence of mechanisms for budget allocation, appointments and dismissals, and oversight powers necessary for the enforcement of decisions (Ansari, 2018a, 2018b)s.

5. Conclusion

In formulating a policy theory for an optimal state of cyberspace governance in the Islamic Republic of Iran, it is vital to consider the evolving nature of power and the reconfiguration of power relations within the framework of smart power, which emerges from network activity in the era of the Fourth Industrial Revolution and cyber-physical systems. Achieving a desirable cyberspace governance model requires, therefore, a redesign of the structures of sovereignty and governance—understood in their evolving relational forms—based on the decentralized intelligence that characterizes networked environments and in alignment with the four axes of power within such networks.

Given the earlier discussion on the relational models between governance and cyberspace, three principal configurations emerge for policy formulation under optimal conditions: (1) traditional governance over cyberspace, (2) networked governance over cyberspace, and (3) governance over the physical world through digital tools. While these categories are often interwoven in practice, a relative distinction among them allows for the identification and proposal of specific guiding strategies to achieve the optimal state.

a) Adoption of a Multilateral Governance Model for Cyberspace: In pursuing governance through conventional state tools over cyberspace, selecting the appropriate governance model is crucial. Given that Iran faces both technological lag in the cyberspace domain and the dominance of the United States and its multinational corporations in setting cyberspace norms, a multi-stakeholder model—often captured by the overwhelming influence of major U.S. tech firms—is currently ill-suited for Iran. Instead, a more suitable model for the Islamic Republic over the next decade is a multilateral governance approach based on a layered architecture of cyberspace, allowing for more national control while accommodating global standards.

b) Redesigning the Administrative System Based on Cyberspace: The second strategic element involves adapting Iran's administrative system to the demands of information technology and cyberspace transformation. This adaptation requires aligning the substructures of state institutions with cyberspace's technological evolution. Creating information and cyberspace departments under each agency in the form of parallel structures represents a step toward reproducing governance capabilities and reinforcing bureaucratic oversight. This transformation acts as a bridge between traditional digital governance and more advanced forms of digital-state integration.

c) Exercising Sovereign Facilitation for Cyberspace Development: The third component highlights the state's role in recognizing and leveraging new tools and dimensions of network-compliant sovereignty. In this model, the government functions as a facilitator, steering the development of cyberspace through strategic support rather than excessive direct control. This approach implies a shift from a maximalist regulatory model to one in which the government provides infrastructure, policy frameworks, and regulatory clarity, while leaving room for private sector innovation and civic participation in content and service development.

d) Using Cyberspace as a Platform for Development and Governance: Governance through cyberspace presupposes that digital infrastructure is more than a tool—it is a platform for national development. In this view, cyberspace serves as both the foundation and the driver for economic, cultural, and administrative advancement. Moreover, it becomes a platform for governance itself. Within this model, several core initiatives are prioritized: (1) establishing a systemic user identity verification mechanism, (2) implementing smart filtering of content and services based on pre-established standards, and (3) enforcing exclusive governance over national big data domains, including urban transportation, healthcare, and financial systems.

e) Evaluation of Negative State Power in Filtering Practices: As observed, the primary tool for the exercise of state negative power in cyberspace remains internet filtering, though other tools such as complete internet shutdowns or bandwidth throttling have occasionally been deployed. Nonetheless, filtering remains the most persistent mechanism. This form of authority, justified legally through state sovereignty, is operationalized via various regulatory concepts and principles. However, its efficacy is highly questionable: the widespread use of VPNs and circumvention tools among users has rendered filtering largely ineffective. Not only does this reduce the tool's impact, but it paradoxically enables users to access far more harmful content—ranging from materials on bomb-making and terrorism to child exploitation and criminal instruction—that most governments, including Iran, seek to prevent.

Consequently, the appropriate course of action should involve a reduction in the volume of filtering, particularly for functional services such as messaging platforms. Such a move could lessen users' reliance on circumvention tools. With users no longer feeling the need to bypass restrictions, the filtering of genuinely harmful content—when deemed necessary by legitimate regulatory authorities—would become more targeted, effective, and credible.

Authors' Contributions

Authors contributed equally to this article.

Declaration

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

Ethical Considerations

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

Acknowledgments

Authors thank all individuals who helped us do this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Ameli, S. R., & Hassani, H. (2018). The Dual-Spatial Nature of Cyber Harms and Disorders: Comparative Study of International Policy-Making. *Cultural Research*, *5*(17).

Ansari, B. (2018a). *Media Law*. SAMT Publications.

Ansari, B. (2018b). The Right to Access Information. In: Media Studies and Planning Office Publications.

Ayazi, R., & Pakzad, B. (2021). The Human Rights Nature of Freedom of Expression on the Internet and the Obligations of States in This Regard. *Public Law JournalIS - 20*.

Bygrave, L., & Bing, J. (2009). *Internet Governance: Infrastructure and Institutions*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199561131.001.0001

Castells, M. (2022). *The Information Age: Economy, Society, and Culture*. Tarh Noor.

Castells, M. (2023). *The Power of Communication*. Scientific and Cultural Publishing Company.

Cory, N. (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? In. Washington: Information Technology and Innovation Foundation.

Faris, R., & Villeneuve, N. (2008). Measuring Global Internet Filtering. In.

Jalali Farahani, A. (2017). Advantages and Limitations of Cyberspace in the Domains of Freedom of Expression, Freedom of Information, and Privacy. *Judiciary Legal Journal*.

Jalili, T. (2021). Internet Governance and the Necessity of Multilateral Cooperation by the Islamic Republic of IranT2 - Islamic Progress Model Conference.

Ma'refat, Z. (2014). *The Political Structure of Cyberspace in Iran* Allameh Tabataba'i University.

Madnian, G., Rahmat-Elahi, H., & Khaleghi Damghani, A. (2011). The Possibility or Impossibility of Defining Public Order in Law (A Study in the Laws of Iran, England, and France). *Comparative Legal Research*(3).

Mehdi-Pour, F. (2020). *Us and the Issues of Cyberspace*. Soroush Publications.

Mir-Mohammadi, D. (2012). *Cyberspace and Identity Transformations in Iran*. Iranian Civilization.

Motamed-Nejad, K., & Motamed-Nejad, R. (2019). *Communication Law*. Media Studies and Development Office.

Nasrollahi, M. S. (2015). *The Model of Cultural Communication Policies Governing the Regulation of Internet Filtering in the Islamic Republic of Iran* Imam Sadiq University]. Tehran.

Nasrollahi, M. S. (2019). Framing Issues of Internet Filtering in Iran: Media and Culture. *Institute for Humanities and Cultural Studies*(18).

Paige Toohey, A. (2013). *Presidential Politics: The Social Media Revolution* Claremont Colleges.

Post, D. (2016). Chaos, State, and the Internet. *Political Science Journal*(Pre-Issue 11).

Qajar Qoyunlu, S. (2022). *Introduction to the Sociology of Law and the Development of Free Flow of Information*. Mizan Publishing.

Qasemi, S. H. (2019). *The Doctrine of Second Cyber Life* Allameh Tabataba'i University.

Rahai, S., & Maleki, M. (2019). Freedom of Information and News and the Restriction of Public Morality in International Law and Islam. *Comparative Research on Islamic and Western Law*(19).

Rahmati, H. A., & Shahriari, H. (2017). Filtering and the Ethical Dilemma of Conflict. *Scientific-Research Quarterly of Ethics ResearchIS - 37*.

Sadeghi, M. (2005). The Concept and Application of Public Order in Judicial and Quasi-Judicial Authorities and Its Modern Manifestations. *Journal of Faculty of Law and Political Science, University of Tehran*, *25*(68).

Seljuqi, M. (2010). *Private International Law* (Vol. 2). Mizan Publishing.

Shahbazi-Nia, M., Isaee Tafreshi, M., & Elmi, H. (2013). The Concept of Public Order in Private International Law and Its Position in International Commercial Arbitration. *Quarterly Journal of Law, Faculty of Law and Political Science*(1).

Shirzad, O. (2020). Reflections on the Concept and Foundations of the Perfectionist State. *Scientific Quarterly of Political and International Approaches*, *11*(4).

Vakili, A. (2014). *Examining the Position, Structure, and Authority of the Supreme Council of Cyberspace in the Legal System of the Islamic Republic of Iran* Islamic Azad University, Tehran Central Branch.

Vincent, A. (2017). *Theories of the State*. Ney Publishing.

Zarei, M. H. (2006). Public Law: Functions and Challenges. *Public Law Theory*(2).