Feasibility of the Government's Civil Liability for Business Closures Caused by Filtering

1. Samsam Kazemi: Department of Private Law, Yas.C., Islamic Azad University, Yasuj, Iran
2. Ali Pourjaveheri *: Department of Law, Yas.C., Islamic Azad University, Yasuj, Iran

*Correspondence: 2298889279@iau.ir

Abstract

This article examines the major challenges governments face in relation to internet filtering, with a particular focus on the Iranian context. Internet filtering has become a key instrument of state control in the digital era, justified by authorities on grounds of national security, cultural preservation, and public order. However, the consequences of such measures extend far beyond their stated objectives, affecting multiple dimensions of governance and society. The study highlights the legal and constitutional conflicts generated by filtering, particularly the tension between state authority and citizens' rights to freedom of expression and access to information. It identifies ambiguities in the law regarding liability and the absence of clear compensation mechanisms for businesses harmed by disruptions. Economically, filtering disrupts e-commerce, undermines innovation, deters investment, and worsens unemployment challenges, especially among youth dependent on digital platforms for livelihood opportunities. Socially, it fuels public dissatisfaction, normalizes circumvention practices, and disrupts education and communication, eroding trust in government institutions. Administratively, filtering policies expose fragmentation among state agencies, overlapping jurisdictions, and the inefficiency of blunt regulatory instruments in comparison to more proportionate models elsewhere. On the international stage, filtering attracts criticism from human rights organizations, creates conflicts with international legal commitments, and damages national reputations in global digital networks. Comparative evidence from China, Turkey, and the European Union reveals alternative approaches and underscores the global complexity of filtering as a governance tool. Overall, the study concludes that filtering policies, while intended to safeguard state interests, generate extensive legal, economic, social, and diplomatic costs that challenge the very legitimacy and effectiveness of government regulation in the digital age.

Keywords: Internet filtering; government challenges; civil liability; digital rights; Iran; e-commerce disruption; constitutional conflicts; state regulation; human rights; international law

Received: 27 April 2025
Revised: 25 July 2025
Accepted: 04 August 2025
Published: 01 September 2025

Citation: Kazemi, S., & Pourjaveheri, A. (2025). Feasibility of the Government's Civil Liability for Business Closures Caused by Filtering. *Legal Studies in Digital Age,* 4(3), 1-13.

1. Introduction

The rise of the internet as a global communication infrastructure has transformed political, social, and economic systems across the world. Internet governance, broadly defined as the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the internet, has become a central concern for governments, corporations, and civil society alike (Kurbalija, 2016). Central to debates about governance is the issue of filtering, censorship, and control over online content. While governments often justify filtering as a means of protecting national security, morality, or social order, such interventions raise profound legal, economic, and human rights questions (Akdeniz, 2010).

Globally, states adopt different models of filtering. Some countries, like China, employ comprehensive systems of control, such as the Great Firewall, that block a wide range of political and social content (Goldsmith & Wu, 2006). Others adopt targeted approaches, limiting access to specific websites or platforms deemed harmful, such as terrorist propaganda or child exploitation material (Douwe, 2019). In democratic societies, filtering tends to be subject to judicial oversight and must conform to proportionality and necessity tests to avoid unjustified restrictions on freedom of expression (Belli & Zingales, 2017). Nonetheless, even in these contexts, governments grapple with the tension between maintaining open digital environments and responding to security or public order concerns. The European Court of Human Rights, for instance, has repeatedly emphasized that access to the internet is integral to the enjoyment of freedom of expression under Article 10 of the European Convention on Human Rights (Council of, 2014).

The economic significance of internet access cannot be overstated. Digital connectivity underpins the modern economy, enabling e-commerce, digital finance, online education, and the platform economy. Manuel Castells argues that the network society, in which economic and social activity is organized around digital communication networks, constitutes the defining characteristic of globalization (Castells, 2010). Disruption of access through widespread filtering or shutdowns has direct consequences for employment, trade, and innovation. Recent studies show that internet shutdowns cost economies billions of dollars annually, with small and medium-sized enterprises suffering the most due to their dependence on social media platforms for marketing and customer engagement (Tiewul, 2021). In contexts where youth unemployment is high, such as in many Middle Eastern countries, filtering and restrictions directly undermine efforts to foster innovation-driven entrepreneurship and reduce economic vulnerabilities (Abedin, 2022).

The human rights dimension of filtering adds another layer of complexity. The United Nations Human Rights Council has repeatedly recognized that the same rights people have offline must also be protected online, including the right to freedom of expression and access to information (United Nations Human Rights Council, 2016). Reports by the UN Special Rapporteur on Freedom of Expression have highlighted how internet shutdowns and broad censorship measures not only stifle political dissent but also impair access to essential services such as health, education, and emergency communication (United Nations Special Rapporteur on Freedom of Expression, 2017). Civil society organizations such as the Electronic Frontier Foundation have similarly underscored the liability of governments for adopting sweeping censorship regimes that harm citizens' rights and livelihoods (Electronic Frontier, 2020).

Iran presents a particularly significant case in global discussions of internet filtering. The Iranian government maintains a monopoly over internet infrastructure and has consistently implemented filtering policies targeting both foreign and domestic online platforms. Scholars note that filtering in Iran is justified by officials primarily on cultural and moral grounds, as well as concerns over national security (Rahmani & Javan Arasteh, 2015). Yet, the practical consequences of these policies have been severe. Businesses that rely on social media for sales, customer communication, and advertising face recurring disruptions that undermine their stability and growth (Hosseini, 2015). For example, the blocking of widely used platforms forces users and entrepreneurs to depend on virtual private networks (VPNs), which are costly, unreliable, and legally ambiguous. This not only erodes trust in the regulatory system but also pushes digital entrepreneurship into informal or semi-legal domains (Abbasi & Hosseini, 2021).

The Iranian context also demonstrates the wider economic and social challenges of filtering. With internet penetration expanding across the population, particularly among the younger demographic, restrictions affect not only businesses but also education, social interaction, and access to global knowledge networks (OpenNet, 2013). Filtering has led to widespread dissatisfaction among citizens and has become a source of social and political tension. International watchdogs such as Freedom House consistently rank Iran among the least free in terms of internet access, citing extensive blocking of political, social, and economic platforms (Freedom House, 2023). The reliance on blunt tools of filtering, rather than more sophisticated or proportionate methods, reflects broader governance challenges in balancing state authority with citizens' rights (Banisar, 2021).

Despite the significance of the issue, there is a noticeable gap in research that comprehensively analyzes the challenges faced by governments in implementing filtering policies. Much of the existing literature focuses on the legal implications of civil liability (Zargoush, 2012), the human rights consequences of internet shutdowns (Kaye, 2019), or the economic impacts of censorship (Abedin, 2022). However, less attention has been devoted to understanding the systemic and institutional challenges governments themselves encounter when attempting to regulate the internet through filtering. These challenges include legal ambiguities, institutional overlaps, technological inefficiencies, and international pressures. A deeper investigation of these difficulties is essential for evaluating not only the legitimacy of filtering policies but also their sustainability in the long term.

The present study seeks to address this gap by examining the major challenges that governments, particularly in the Iranian context, face in relation to internet filtering. The objective is not merely to critique the policies from a human rights or economic perspective, but to identify and analyze the structural, legal, administrative, and diplomatic challenges that arise from filtering practices. This approach allows for a more nuanced understanding of the complexities governments must navigate, while also highlighting the implications for citizens and businesses.

Accordingly, the research asks several guiding questions. What are the primary legal and constitutional constraints that complicate governmental attempts to justify filtering? How does filtering impact the economic landscape, especially for internet-based businesses and entrepreneurs? In what ways does filtering produce social and cultural challenges that may undermine state legitimacy? How do overlapping administrative authorities and institutional inefficiencies hinder the effective implementation of smart filtering policies? Finally, how do international human rights obligations and global diplomatic pressures shape the strategies governments adopt in this domain?

By pursuing these questions, the study aims to provide a comprehensive account of the governmental challenges of filtering. This will not only contribute to the scholarly literature on internet governance but also offer insights for policymakers who must reconcile the often-conflicting demands of security, morality, economic growth, and human rights in the digital age.

2. Theoretical Framework

Civil liability as a legal concept has long been central to the relationship between the state and its citizens. In administrative law, civil liability is understood as the obligation of the state to provide compensation when its actions, whether lawful or unlawful, cause harm to individuals. This principle rests on the recognition that the state, despite being the supreme authority within its jurisdiction, is not above accountability and must answer for the damages inflicted upon its citizens when exercising its powers (Harlow, 1988). Unlike private law disputes where liability is often based on contractual obligations, civil liability of the state emerges primarily in public law contexts where the government's exercise of authority impacts private interests. The underlying rationale is that the monopoly of power held by the state requires a system of checks that protect individuals from potential misuse of that power.

A crucial component in the doctrine of state liability is the distinction between governmental acts, also referred to as sovereign acts, and administrative or commercial acts. Governmental acts are those that fall squarely within the realm of sovereignty, such as maintaining public order, regulating national security, or enforcing judicial decisions. In most legal systems, states are granted immunity for damages resulting from these acts, under the argument that the general interest of the community outweighs the private interests of individuals (Zargoush, 2012). Administrative or commercial acts, on the other hand, involve state activities that resemble those of private actors, such as running public enterprises, providing internet

services, or engaging in commercial transactions. In these cases, the state is often held liable on the same terms as private entities, since it is not acting in its unique sovereign capacity but as a participant in the broader market (Abbasi & Hosseini, 2021).

The practical significance of this distinction becomes clear when applied to internet governance and filtering. If filtering is considered a governmental act aimed at safeguarding national security or protecting cultural values, then the state often asserts immunity against claims for damages. Conversely, if filtering disrupts the commercial services provided by the state, such as internet provision through state-controlled telecommunications, then the government may bear civil liability as a service provider (Rahmani & Javan Arasteh, 2015). The difficulty lies in the fact that filtering policies usually involve a mixture of both sovereign and administrative dimensions, creating ambiguity in determining whether liability should be imposed.

The theories of liability provide different approaches to resolving this ambiguity. Fault-based liability, the most traditional doctrine, requires proof that the state acted negligently, unlawfully, or in violation of established duties. In the digital sphere, this could mean showing that the government failed to implement filtering in a proportionate or technically competent manner, thereby causing unnecessary disruption to lawful business activities (Laidlaw, 2015). Strict liability, by contrast, imposes responsibility on the state regardless of fault. Under this theory, the mere fact that harm occurred due to state action suffices to trigger compensation. This approach is particularly relevant in contexts where states exercise monopolistic control over critical infrastructure such as internet access, leaving citizens with no alternative providers (Weber, 2010). The risk theory further extends this notion by suggesting that because the state engages in inherently risky activities—such as controlling information flows—it should internalize the risks of harm and compensate those adversely affected, even if no negligence is proven (Abedin, 2022).

In the context of digital rights, these theories must be understood alongside constitutional and human rights guarantees. The right to freedom of expression, which includes the right to seek, receive, and impart information, is explicitly protected in numerous international instruments. The UN Human Rights Council emphasized in its landmark 2016 resolution that the same rights people have offline must be protected online, underscoring the state's obligation not to restrict internet access arbitrarily (United Nations Human Rights Council, 2016). Reports by the UN Special Rapporteur on Freedom of Expression further reinforce this by stating that internet shutdowns and blanket filtering measures are rarely justifiable under international law, as they disproportionately affect both political participation and access to essential services (United Nations Special Rapporteur on Freedom of Expression, 2017).

Comparative constitutional perspectives further illuminate how digital rights intersect with state liability. In the United States, the First Amendment guarantees freedom of speech and has been interpreted to provide strong protections against government censorship. Although the U.S. does not impose direct civil liability on the state for internet restrictions, courts have consistently struck down attempts at overbroad filtering on constitutional grounds, reinforcing the principle that the burden of justification rests heavily on the government (Goldsmith & Wu, 2006). In Europe, the European Court of Human Rights has recognized access to the internet as integral to the exercise of Article 10 rights, thereby obligating governments to ensure restrictions are necessary, proportionate, and prescribed by law (Council of, 2014). By contrast, in China, the state embraces a model of comprehensive control over digital spaces, justified by national security and social stability concerns, and does not recognize civil liability for filtering measures. Instead, liability often falls upon private platforms for failing to comply with state censorship mandates (Banisar, 2021).

The Iranian system reveals a hybrid model where the government simultaneously acts as the primary provider of internet services and the regulator imposing restrictions. In such a context, applying the distinction between governmental and administrative acts becomes complex. On the one hand, the state argues that filtering is a sovereign function justified by national security. On the other hand, as the monopoly provider of internet services, the government's actions resemble those of a commercial actor whose failure to provide stable and unrestricted access causes economic losses (Hosseini, 2015). This dual role creates a tension that demands theoretical clarity and underscores the relevance of strict and risk-based liability frameworks.

The broader theories of internet governance also inform the analysis. Scholars argue that governance of the internet cannot be understood merely through domestic legal frameworks but must be situated within global political and economic structures

(Mueller, 2010). The rise of transnational digital platforms challenges state sovereignty, while at the same time creating pressures for governments to assert control through measures such as filtering. Castells' theory of the network society highlights how information flows transcend borders, meaning that national filtering policies often have global repercussions, such as discouraging foreign investment or isolating domestic users from international markets (Castells, 2010). From this perspective, state liability is not merely a domestic issue but part of broader debates about global justice and digital inclusion.

The economic logic behind liability theories gains additional relevance in the digital economy. Abedin's comparative analysis of censorship emphasizes that the harm caused by filtering extends beyond immediate business losses to include long-term impacts on innovation ecosystems, as entrepreneurs are discouraged from investing in uncertain regulatory environments (Abedin, 2022). Similarly, Belli and Zingales highlight how platforms serve as critical infrastructures of communication and commerce, making their disruption a matter of public interest and not merely private inconvenience (Belli & Zingales, 2017). The consequence is that when governments impose filtering, they interfere with core economic functions of society, thereby increasing the urgency of holding them accountable under civil liability doctrines.

At the same time, states often invoke competing justifications that complicate the liability analysis. Kaye observes that governments frame filtering as a tool to protect citizens from harmful content such as disinformation, hate speech, or extremism, but in practice these measures frequently overreach and suppress legitimate expression (Kaye, 2019). The Electronic Frontier Foundation further argues that liability rules must consider not only the direct economic harms but also the chilling effect on free expression when citizens fear punishment for circumventing restrictions (Electronic Frontier, 2020). Such concerns emphasize the importance of interpreting state responsibility through the lens of human rights law as well as administrative law.

The comparative perspective also reveals differences in institutional accountability mechanisms. In liberal democracies, judicial review acts as a safeguard by ensuring that filtering policies conform to constitutional standards. In contrast, authoritarian systems rely on executive decrees, leaving little room for judicial or legislative oversight (Banisar, 2021). This divergence underscores why liability theories must adapt to institutional contexts. In settings where courts are independent, fault-based liability may suffice because citizens can seek remedies. In settings where courts are not impartial, strict or risk-based liability frameworks may be more appropriate to conceptualize the state's obligations in principle, even if they are not enforceable in practice.

From a doctrinal standpoint, Weber argues that internet governance poses unique regulatory challenges because the global nature of digital communication clashes with territorially bounded legal systems (Weber, 2010). Filtering policies are national in scope, but their effects are transnational, creating conflicts of law and undermining the coherence of liability regimes. OpenNet's case study of Iran further demonstrates that extensive filtering not only disrupts domestic markets but also complicates international cooperation, as businesses and NGOs perceive the environment as unpredictable and hostile (OpenNet, 2013). These comparative insights illustrate why understanding state liability in the context of filtering requires both a domestic and international lens.

Taken together, the theoretical framework illustrates that civil liability and state responsibility in the context of filtering must be analyzed through multiple layers: the doctrinal distinction between sovereign and administrative acts, the competing theories of liability, the principles of digital and constitutional rights, and the comparative experiences of different legal systems. While no single theory provides a definitive answer, each highlights a dimension of the problem. Fault-based liability stresses accountability for negligence, strict liability emphasizes compensation regardless of fault, and risk theory insists on internalizing the inherent dangers of state control over critical infrastructures. Digital rights frameworks remind us that beyond economic losses, filtering affects the very fabric of democratic participation and personal autonomy. Comparative perspectives reveal that approaches differ widely, but the common challenge is reconciling the legitimate aims of governments with the rights and expectations of citizens in the digital era.

This framework sets the stage for analyzing the specific challenges governments encounter in implementing filtering policies. By grounding the discussion in established theories of liability and human rights, while also recognizing the unique features of internet governance, it becomes possible to better evaluate the legitimacy, feasibility, and consequences of filtering practices in both national and international contexts.

3. Government's Role in Internet Filtering

Governments have long occupied a central role in shaping the architecture and regulation of the internet, often justified by their monopoly over infrastructure and regulatory authority. In many jurisdictions, particularly in states with centralized governance models, the government controls the provision of internet services through state-owned or heavily regulated telecommunications providers. This monopoly allows governments to act not only as regulators but also as service providers, placing them in a dual role where the boundaries between public authority and commercial activity become blurred. In contexts such as Iran, the government maintains strict control over bandwidth distribution, international gateways, and licensing of internet service providers, ensuring that all points of access are subject to state oversight (OpenNet, 2013). Such control allows authorities to implement filtering policies directly at the infrastructural level, without reliance on private actors, thereby consolidating the state's power over digital communication and limiting avenues for contestation by citizens or businesses.

The legal framework that supports internet filtering in Iran further entrenches governmental authority. Several laws, charters, and regulations provide the state with broad discretion to determine what content is permissible online. While the Iranian Constitution recognizes certain freedoms, including freedom of expression, it also allows for limitations when deemed necessary for public order and morality, creating a constitutional basis for filtering. Complementary legislation, including rules issued by the Supreme Council of Cyberspace and the Computer Crimes Law, grants state agencies explicit powers to block access to websites and digital platforms deemed harmful or contrary to cultural, political, or religious values (Rahmani & Javan Arasteh, 2015). The Citizen's Rights Charter similarly acknowledges access to information but leaves room for broad limitations, allowing authorities to justify filtering under the guise of protecting public interests (Abbasi & Hosseini, 2021). The presence of overlapping regulatory bodies, including the judiciary, the Ministry of Information and Communications Technology, and security organizations, demonstrates the fragmented yet pervasive legal structure through which filtering is institutionalized.

The motivations behind filtering policies are varied, reflecting a mix of security, political, and cultural concerns. From a security perspective, governments argue that filtering is necessary to combat terrorism, organized crime, and cyber threats. This justification has become more pronounced in the digital age, where extremist groups and hostile foreign actors use online platforms for recruitment, propaganda, and coordination (Banisar, 2021). In the Iranian context, authorities frequently highlight the risks of external influence and information warfare, claiming that unrestricted access to global platforms could facilitate destabilization. Politically, filtering serves as a tool for controlling dissent and managing narratives. Social media platforms have played crucial roles in mobilizing protest movements, and restricting access to these tools allows governments to limit the speed and scale of collective action (Freedom House, 2023). Culturally, filtering is framed as a means of preserving moral values and protecting citizens from content considered offensive or contrary to societal norms. This includes blocking sites related to pornography, gambling, and politically sensitive issues, which the state portrays as threats to the moral fabric of society (Hosseini, 2015).

Yet, these motivations must be understood within the broader tension between state sovereignty and individual rights. Governments frequently invoke morality and cultural protection to justify measures that also serve political ends. For instance, the state may claim to protect families and children from harmful online material while simultaneously blocking independent news sites and opposition platforms (Kaye, 2019). The challenge lies in distinguishing between legitimate regulatory objectives and overreach that undermines freedom of expression. International human rights law stresses that restrictions on internet access must meet the criteria of legality, necessity, and proportionality (United Nations Human Rights Council, 2016). However, in practice, broad discretionary powers granted by national legal frameworks often make it difficult for citizens to challenge filtering decisions or seek remedies for the harms caused (Laidlaw, 2015).

The government monopoly over internet regulation in Iran creates unique difficulties in balancing public order, morality, and freedom of access. As the sole provider of key infrastructure, the government has a responsibility similar to that of a utility provider, ensuring reliable access to essential services. When restrictions disrupt economic activities, particularly for online businesses and entrepreneurs, the state's dual role as both regulator and service provider places it in a position of potential liability (Abedin, 2022). Theories of risk-based liability argue that where citizens have no choice but to rely on state-controlled

internet services, the state should bear responsibility for the economic and social harms caused by disruptions (Weber, 2010). However, in Iran, legal and institutional frameworks often shield the state from accountability, creating a gap between responsibility in principle and remedies in practice.

At the same time, filtering policies raise significant governance challenges. The reliance on blunt instruments of restriction, such as nationwide blocking of platforms, demonstrates technological inefficiencies compared to more targeted or "smart" filtering models used elsewhere. In Europe, for example, governments have attempted to adopt proportionate filtering measures subject to judicial oversight, ensuring that restrictions address specific harms without unduly infringing on broader freedoms (Council of, 2014). By contrast, Iran's approach often involves blanket bans that affect millions of users, including those engaging in lawful and socially beneficial activities. This lack of precision not only generates economic costs but also undermines public trust in governance, as citizens perceive restrictions as arbitrary or politically motivated (Electronic Frontier, 2020).

Another layer of complexity arises from international pressures and reputational costs. Global watchdogs and advocacy organizations consistently criticize Iran's filtering policies as violations of digital rights, which affects the country's international standing and deters foreign investment (OpenNet, 2013). At a time when digital connectivity is central to global trade and diplomacy, persistent filtering policies risk isolating the country from international markets and knowledge networks. This dynamic reflects what Mueller describes as the broader conflict between state sovereignty and global information flows, where national restrictions clash with the inherently transnational nature of the internet (Mueller, 2010). The result is not only domestic discontent but also diplomatic friction, as international bodies push for adherence to global standards of digital rights (Belli & Zingales, 2017).

Cultural motivations behind filtering, though often justified in terms of protecting moral values, also reflect the government's effort to assert authority in a rapidly changing social landscape. The internet facilitates exposure to diverse cultures, ideas, and lifestyles, challenging traditional structures of authority. Governments seeking to maintain social cohesion therefore frame filtering as a necessary defensive measure. Castells emphasizes that the network society reshapes cultural and political identities, meaning that controlling information flows is also a way of managing these transformations (Castells, 2010). However, such control risks backfiring, as citizens increasingly rely on circumvention tools to access blocked content, creating a digital arms race between censors and users. This reliance on VPNs and proxies erodes the effectiveness of filtering, demonstrates public resistance, and highlights the limitations of top-down control in a networked society (Douwe, 2019).

The balancing act between public order, morality, and freedom of access thus emerges as the central dilemma for governments engaged in filtering. While states assert their authority to protect national interests, they simultaneously face the challenge of ensuring that such measures do not disproportionately harm citizens' rights or the digital economy. International legal principles demand proportionality, but national frameworks often privilege state discretion over individual protections. The Iranian experience exemplifies this tension, where broad filtering serves immediate political and cultural objectives but generates long-term economic, social, and diplomatic costs. Governments must therefore navigate these competing imperatives, recognizing that legitimacy in the digital age depends not only on maintaining order but also on respecting the rights and expectations of digitally connected citizens.

4. Identifying the Major Challenges of Government in Relation to Filtering

The implementation of internet filtering by governments is not a straightforward exercise of regulatory authority. It is instead fraught with complex challenges that span legal, economic, cultural, administrative, and international domains. In the Iranian case, these challenges are magnified by the government's monopolistic control over infrastructure, the blurred line between sovereign and commercial acts, and the growing reliance of citizens and businesses on digital platforms. The following sections outline the most critical obstacles that governments face in their approach to filtering, highlighting how these difficulties affect not only citizens but also the legitimacy and effectiveness of the state itself.

4.1. Legal and Constitutional Challenges

The first challenge arises from the fundamental conflict between filtering measures and constitutional rights. Constitutions in most modern states, including Iran, recognize certain freedoms, such as freedom of expression and the right to access information, even if they are subject to limitations. Filtering, especially when applied broadly and indiscriminately, directly undermines these rights by restricting citizens' ability to receive and disseminate information through digital platforms. The United Nations Human Rights Council has underscored that the same rights people have offline must also be protected online, making the curtailment of internet access without clear necessity and proportionality a violation of international human rights law (United Nations Human Rights Council, 2016). In practice, however, governments invoke public order and morality to justify restrictions, a justification that often lacks transparency and creates legal uncertainty (Laidlaw, 2015).

Ambiguities in domestic law compound this problem. In Iran, the Constitution and subsequent cybercrime legislation allow for restrictions in cases deemed necessary for national security, cultural protection, or religious values. Yet, the exact scope of what qualifies as harmful or unlawful content remains vague. This vagueness grants broad discretion to state authorities and undermines the principle of legal certainty. Citizens and businesses cannot reliably predict which platforms or services may be subject to filtering, leaving them in a perpetual state of uncertainty (Abbasi & Hosseini, 2021). Scholars have pointed out that such ambiguity opens the door to selective or politically motivated enforcement, allowing governments to target opposition voices under the guise of protecting national interests (Kaye, 2019).

Another legal difficulty lies in the lack of explicit mechanisms for compensation when filtering causes damages. Businesses that depend on digital platforms for commerce and communication suffer significant losses during disruptions, but national legal frameworks rarely provide remedies. Zargoush has argued that state liability in cases of unexpected or emergency measures should be grounded in clear legal frameworks that ensure citizens can seek compensation (Zargoush, 2012). However, in practice, Iranian law lacks a systematic approach to redress. Theories of fault-based or strict liability remain largely academic, with no effective enforcement in court (Weber, 2010). The result is a widening gap between the state's accountability in principle and its immunity in practice, undermining public confidence in the rule of law.

4.2. Economic and Commercial Challenges

The economic consequences of filtering present another major challenge for governments. In economies increasingly dependent on digital platforms, filtering disrupts e-commerce, digital finance, and start-up ecosystems. Abedin's comparative analysis shows that internet shutdowns and filtering policies directly undermine innovation and productivity by creating uncertainty in market environments (Abedin, 2022). Start-ups in particular are disproportionately affected, since they often rely on affordable digital tools such as social media and cloud platforms for marketing, customer relations, and service delivery. In Iran, many entrepreneurs have turned to platforms like Instagram and WhatsApp for commerce, and their sudden blocking leaves businesses without cost-effective alternatives (Hosseini, 2015).

The broader negative effect on employment and innovation cannot be ignored. Filtering stifles opportunities for young people who might otherwise enter digital professions, forcing them to seek work in traditional sectors with limited prospects. Castells' theory of the network society emphasizes how economic growth in the twenty-first century is linked to digital networks, meaning that restrictions on access exclude societies from the main drivers of development (Castells, 2010). In Iran, where youth unemployment is already high, filtering exacerbates structural challenges in the labor market by curtailing access to global gig platforms, remote work opportunities, and online education that could empower younger generations.

Foreign investment is also deterred by unstable internet policies. Multinational companies prioritize regulatory stability and reliable infrastructure when considering investment opportunities. Filtering policies that are unpredictable or sweeping send a clear signal of regulatory risk, discouraging foreign firms from entering the market. Freedom House reports that countries with severe internet restrictions are frequently excluded from global digital value chains, as investors fear both reputational and operational risks (Freedom House, 2023). In Iran, the combination of sanctions and filtering amplifies the perception of instability, further isolating the country from global economic networks.

4.3. Social and Cultural Challenges

Filtering also generates social and cultural tensions that complicate governance. Public dissatisfaction is one of the most immediate outcomes, as citizens experience restricted access to platforms that facilitate communication, education, and entertainment. The erosion of trust in government is particularly acute when citizens perceive filtering as politically motivated rather than genuinely protective. Kaye highlights how governments often present filtering as a measure against harmful content, but in practice it suppresses legitimate speech and creates widespread cynicism about state intentions (Kaye, 2019).

One consequence of public dissatisfaction is the widespread proliferation of VPNs and other circumvention tools. In Iran, VPN usage has become not only a technical workaround but a cultural norm, especially among younger generations (Douwe, 2019). This reliance undermines the effectiveness of filtering policies and creates a cat-and-mouse dynamic between regulators and citizens. It also fosters a culture of everyday illegality, where citizens are routinely forced to break the law simply to access information or conduct business. Such conditions erode respect for the legal system and deepen the legitimacy crisis facing the state.

The impact on education, communication, and social participation further illustrates the cultural costs of filtering. With the increasing integration of digital platforms into education, students and teachers face barriers to accessing resources, participating in online learning communities, and engaging with international scholarship (Banisar, 2021). Communication within families and social groups is also disrupted when popular platforms are blocked, pushing people to adopt less secure alternatives. Social participation in civic life, including political engagement and grassroots organization, is curtailed by the unavailability of tools that allow citizens to coordinate and exchange ideas (Electronic Frontier, 2020). The cumulative effect of these disruptions is the alienation of citizens from both the state and the global community.

4.4. Administrative and Governance Challenges

The implementation of filtering policies exposes deep administrative and governance problems. A significant challenge is the lack of coordination among state agencies. In Iran, multiple entities—including the judiciary, the Ministry of Information and Communications Technology, and security organizations—possess overlapping authority over filtering. This institutional fragmentation results in inconsistent enforcement and confusion about which agency is accountable for specific restrictions (Rahmani & Javan Arasteh, 2015). In some cases, one agency may block a platform while another resists, creating contradictory signals for both citizens and businesses.

Overlapping authorities exacerbate inefficiencies and lead to politicization of regulatory decisions. Abbasi points out that the absence of clear delineation of responsibilities allows agencies to pursue their own agendas under the umbrella of state authority (Abbasi & Hosseini, 2021). Such conditions not only generate uncertainty but also weaken the rule of law by creating opaque and unreviewable processes. Without a transparent chain of responsibility, it becomes nearly impossible for citizens to contest filtering decisions or demand accountability.

A further governance challenge is the inefficiency in applying smart filtering policies. In contrast to targeted, content-specific blocking mechanisms employed in parts of Europe and North America, Iran often relies on sweeping measures that block entire platforms regardless of whether harmful content is present (Council of, 2014). This blunt approach reflects technological limitations and a lack of investment in more sophisticated filtering tools. The inefficiency of these methods results in collateral damage, as businesses, educators, and ordinary citizens lose access to beneficial content alongside the restricted material. The failure to develop proportionate mechanisms highlights a broader issue of governance capacity in adapting to the complexities of the digital era (Weber, 2010).

4.5. International and Diplomatic Challenges

Finally, filtering policies generate significant international and diplomatic challenges. Governments that impose broad restrictions face criticism from human rights organizations and international watchdogs, which consistently rank such countries among the least free in terms of internet access. Reports by Freedom House highlight how internet restrictions correlate with lower scores in political rights and civil liberties, framing filtering as a tool of authoritarian control (Freedom House, 2023).

International NGOs, such as the Electronic Frontier Foundation, argue that such policies violate obligations under treaties like the International Covenant on Civil and Political Rights, which protect the rights to freedom of expression and access to information (Electronic Frontier, 2020).

Conflicts with commitments under international law further complicate state strategies. The UN Special Rapporteur on Freedom of Expression has criticized internet shutdowns and filtering as disproportionate measures rarely justified under international human rights standards (United Nations Special Rapporteur on Freedom of Expression, 2017). For Iran, which has ratified several human rights treaties, the persistence of broad filtering creates tension between its international commitments and domestic practices. This tension not only exposes the country to international censure but also weakens its position in diplomatic negotiations where human rights performance is scrutinized (Belli & Zingales, 2017).

Damage to digital reputation constitutes another challenge. In an era where digital connectivity is integral to global commerce and diplomacy, countries that persist in broad filtering risk isolation. OpenNet has documented how Iran's extensive filtering regime has deterred international collaboration in research, education, and commerce, further marginalizing the country within the global digital economy (OpenNet, 2013). Mueller similarly emphasizes that filtering represents a clash between the territorial logic of states and the transnational logic of digital networks, a clash that can undermine states' ability to participate effectively in global governance (Mueller, 2010). This reputational damage is not easily repaired, as foreign governments and companies often view filtering regimes as evidence of instability and risk.

The challenges facing governments in relation to filtering thus extend far beyond the technical act of blocking content. They encompass constitutional conflicts, legal ambiguities, economic disruptions, cultural alienation, administrative inefficiencies, and international isolation. Together, these challenges reveal the inherent difficulty of sustaining broad filtering policies in the digital era, where connectivity is a cornerstone of economic growth, human rights, and international cooperation. For Iran, these difficulties highlight the need for a critical reassessment of its approach, balancing legitimate security and cultural concerns with the imperatives of rights protection, economic development, and global integration.

5. Case Studies and Evidence

The study of government challenges in relation to internet filtering becomes clearer when it is grounded in specific case studies that illustrate both the consequences of such measures and the varied approaches adopted across jurisdictions. By examining major filtering events in Iran and beyond, as well as legal disputes that have emerged in their wake, it is possible to trace how filtering policies affect businesses, individuals, and governments themselves. Comparative examples from China, Turkey, and the European Union further highlight the diversity of legal and political frameworks governing filtering, revealing the global complexity of balancing state authority with digital freedoms.

In Iran, several high-profile filtering events underscore the heavy costs of state-imposed restrictions. During periods of political unrest, such as widespread protests, authorities have often responded with sweeping shutdowns or the blocking of popular social media platforms. Freedom House notes that Iran consistently ranks among the least free environments for internet users due to recurrent restrictions targeting platforms like Facebook, Twitter, and more recently, Instagram and WhatsApp, both of which are integral to commerce and communication for millions of citizens (Freedom House, 2023). The sudden blocking of Instagram in 2022, for instance, left thousands of small businesses without a marketplace, disrupting livelihoods in sectors ranging from fashion to food services. Abedin has emphasized that filtering does not simply halt communication but dismantles the ecosystem of trust and continuity that digital businesses rely on (Abedin, 2022). These disruptions show that while the government views filtering as a necessary security measure, the social and economic consequences are profound and long-lasting.

Legal disputes and complaints filed by businesses in Iran further reveal the tensions filtering creates within the national legal framework. Although Iranian courts have historically been reluctant to hold the state liable for damages arising from sovereign acts, cases have been brought by entrepreneurs arguing that filtering constitutes an administrative failure rather than a sovereign decision. Rahmani has argued that liability should extend to situations where filtering disrupts commercial activity because the state acts both as regulator and as the monopoly provider of internet services (Rahmani & Javan Arasteh, 2015). Despite this reasoning, effective compensation mechanisms remain absent, leaving businesses without recourse. Abbasi similarly notes that

ambiguities in Iranian law allow state authorities to evade responsibility, forcing businesses to absorb the losses caused by unpredictable restrictions (Abbasi & Hosseini, 2021). The absence of judicial enforcement in these disputes illustrates the structural weakness of domestic law in protecting businesses against state overreach.

The Iranian experience is not unique, as similar conflicts have occurred elsewhere. In Turkey, for example, filtering has often been used to restrict access to platforms like Twitter and YouTube during politically sensitive moments. Douwe describes how the Turkish Constitutional Court eventually intervened, ruling that the blanket blocking of Twitter violated constitutional rights to freedom of expression (Douwe, 2019). This case illustrates how judicial review can act as a corrective mechanism against excessive filtering, ensuring that measures meet tests of proportionality and legality. Unlike Iran, where judicial oversight is limited, the Turkish case demonstrates the potential for courts to restore balance between state authority and individual rights, though challenges remain due to recurring government attempts to impose new restrictions.

China provides perhaps the most prominent case study with its "Great Firewall," an extensive system of internet filtering and surveillance designed to control both domestic information flows and cross-border communications. Goldsmith and Wu argue that China's model shows the possibility of a highly controlled digital environment that nonetheless supports economic growth, albeit under tightly managed conditions (Goldsmith & Wu, 2006). The Chinese approach integrates filtering into the very architecture of internet access, combining state mandates with corporate compliance to ensure comprehensive control (Akdeniz, 2010). While this model has allowed the Chinese government to maintain stability and promote domestic alternatives such as WeChat and Weibo, it has also attracted widespread criticism for its violations of freedom of expression and international human rights norms (Banisar, 2021). The contrast with Iran is instructive: whereas China has developed domestic platforms that serve as substitutes for blocked international services, Iran lacks equivalent homegrown alternatives, leaving businesses without viable replacements when restrictions occur.

The European Union provides a different perspective, emphasizing proportionality and human rights in the regulation of filtering. The European Court of Human Rights has held that while governments may impose restrictions on internet access in pursuit of legitimate aims such as national security, those restrictions must be necessary, proportionate, and prescribed by law (Council of, 2014). In practice, this has meant that blanket bans on platforms are rarely permissible. Laidlaw underscores that European law frames digital platforms as essential infrastructures for exercising freedom of expression, requiring states to justify restrictions through transparent and accountable processes (Laidlaw, 2015). The proportionality test applied in the EU illustrates a model where the rights of individuals remain at the center of filtering debates, providing a legal standard against which state actions are judged.

Comparing these case studies reveals striking differences in outcomes for both governments and citizens. In Iran, filtering leads to widespread use of circumvention tools, creating a culture of digital illegality and undermining respect for the legal system (Douwe, 2019). In Turkey, court rulings offer a partial safeguard but have not prevented recurrent clashes between government and civil society over access to platforms. In China, filtering is embedded within a broader strategy of digital sovereignty, ensuring the development of parallel domestic ecosystems but at the cost of individual freedoms (Castells, 2010). In the European Union, filtering is tightly constrained by judicial oversight, reflecting a commitment to balancing state authority with fundamental rights (United Nations Special Rapporteur on Freedom of Expression, 2017).

These case studies also provide evidence of the reputational costs governments incur when they pursue aggressive filtering strategies. International organizations such as Freedom House consistently rank countries like Iran and China at the bottom of their internet freedom indexes, highlighting how restrictive policies affect global perceptions (Freedom House, 2023). The Electronic Frontier Foundation argues that these reputational harms are not merely symbolic but carry economic consequences, as foreign investors interpret filtering as a signal of instability and legal risk (Electronic Frontier, 2020). OpenNet's research on Iran similarly documents how filtering isolates the country from international collaboration in research and commerce, exacerbating the very vulnerabilities that governments claim to be addressing (OpenNet, 2013).

In each of these cases, filtering demonstrates a recurring pattern: governments attempt to assert control over digital spaces, but the consequences often extend beyond their intended targets, producing economic, social, and diplomatic costs. The Iranian experience reveals how fragile economies and limited legal protections exacerbate these challenges, while the Chinese model shows how states can sustain filtering by simultaneously cultivating domestic alternatives. Turkey's experience illustrates the

role of constitutional courts in mediating between government power and individual rights, and the European Union demonstrates how robust human rights frameworks constrain state authority.

Taken together, these examples confirm that filtering is not merely a technical or administrative measure but a deeply political act with wide-ranging implications. Governments that pursue filtering must navigate not only domestic pressures but also international norms and economic realities. The evidence from Iran and comparative cases underscores the central theme of this study: that the challenges of filtering are multifaceted and often create consequences that governments themselves struggle to manage, whether in the form of legal disputes, economic losses, or reputational damage on the global stage.

6. Conclusion

The exploration of government challenges in relation to internet filtering demonstrates that such measures are far more complex than simple exercises of regulatory authority. Filtering is not only a technical mechanism of controlling online spaces but also a deeply political act that reverberates across legal, economic, cultural, administrative, and diplomatic domains. Governments that employ filtering often justify it on the grounds of national security, cultural protection, or public morality, but the consequences extend well beyond those stated objectives, shaping the very relationship between the state, its citizens, and the global community.

One of the central findings is that filtering exposes profound contradictions within governance structures. On the one hand, states claim sovereign authority to regulate digital spaces, while on the other, they assume responsibilities similar to commercial actors when providing internet services. This dual role complicates questions of accountability and liability, leaving citizens and businesses in a state of uncertainty. Legal ambiguities, weak enforcement mechanisms, and the absence of compensation frameworks further undermine public trust in the rule of law.

Economically, filtering disrupts the foundations of digital commerce, erodes the prospects of start-ups, and discourages foreign investment. It limits opportunities for innovation and employment, particularly for younger generations who rely on digital platforms to engage with the global economy. Socially, filtering alienates citizens from the state, encourages widespread circumvention, and undermines respect for legal norms. It affects education, communication, and civic engagement, weakening the social fabric that governments claim to protect.

From an administrative perspective, filtering policies reveal inefficiencies, overlapping authorities, and inconsistent enforcement, highlighting structural governance challenges. Governments often resort to blunt, disproportionate measures rather than investing in targeted or transparent solutions, thereby exacerbating public dissatisfaction and reducing the legitimacy of regulatory institutions. At the international level, filtering damages a country's digital reputation, isolates it from global cooperation, and exposes it to criticism for failing to uphold fundamental rights.

Altogether, the evidence suggests that filtering generates consequences that governments themselves struggle to control. While intended to preserve order, morality, or sovereignty, these measures often produce long-term costs that outweigh their short-term benefits. Sustainable governance in the digital era requires moving beyond the blunt instrument of filtering toward approaches that balance legitimate state concerns with the imperatives of economic development, social participation, and human rights. Only by rethinking strategies of digital regulation can governments hope to manage the complexities of the networked world in ways that enhance legitimacy, foster innovation, and strengthen trust between the state and its citizens.

Ethical Considerations

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

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

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

References

Abbasi, K., & Hosseini, M. (2021). Civil liability of the state in cyberspace restrictions. *Iranian Journal of Law and Technology*, *13*(2), 45-70.
Abedin, B. (2022). Internet censorship and state liability: Comparative perspectives. *Journal of Cyber Policy*, *7*(3), 301-319.
Akdeniz, Y. (2010). *Internet content regulation: Law and freedom of expression*. Routledge.
Banisar, D. (2021). *Global trends in internet censorship and access to information*.
Belli, L., & Zingales, N. (2017). Platform regulations and digital rights. *Internet Policy Review*, *6*(2), 1-20.
Castells, M. (2010). *The rise of the network society*. Wiley-Blackwell.
Council of, E. (2014). *Guide to human rights for Internet users*. Council of Europe Publishing.
Douwe, K. (2019). The legal framework of internet shutdowns. *Human Rights Law Review*, *19*(2), 345-372.
Electronic Frontier, F. (2020). *Censorship and liability: Government responsibilities in digital spaces*.
Freedom House. (2023). *Freedom on the Net: The Global Drive to Control Big Tech*.
Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford University Press.
Harlow, C. (1988). *Administrative liability and the state*. Oxford: Clarendon Press.
Hosseini, S. J. (2015). Civil liability in social networks. Proceedings of National Conference on Law and Technology, Shiraz, Iran.
Kaye, D. (2019). *Speech police: The global struggle to govern the Internet*. Columbia Global Reports.
Kurbalija, J. (2016). *An introduction to Internet governance*. DiploFoundation.
Laidlaw, E. (2015). *Regulating speech in cyberspace: Gatekeepers, human rights and corporate responsibility*. Cambridge University Press.
Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. MIT Press.
OpenNet, I. (2013). *Internet filtering in Iran: A country study*.
Rahmani, S., & Javan Arasteh, H. (2015). Fiqh–legal analysis of state liability in filtering damages. *Journal of Islamic Law Studies*, *6*(12), 45-68.
Tiewul, B. (2021). The legality of internet shutdowns under international law. *International Journal of Human Rights*, *25*(4), 579-598.
United Nations Human Rights Council. (2016). *Resolution on the promotion, protection and enjoyment of human rights on the Internet, A/HRC/32/L.20*.
United Nations Special Rapporteur on Freedom of Expression. (2017). *Report on internet shutdowns and restrictions*.
Weber, R. H. (2010). *Shaping Internet governance: Regulatory challenges*. Springer.
Zargoush, M. (2012). Theoretical foundations of state liability in unexpected events. *Journal of Public Law and Human Rights*, *2*(8), 33-59.