



Behnam Khatami
Managing Partner

+98 21 2240 0434
behnam.khatami@namiassociates.com



Mansour Vesali
Senior Associate

+98 21 2240 0434
mansour.vesali@namiassociates.com



Navid Ghodsi
Associate

+98 21 2240 0434
navid.ghodsi@namiassociates.com

Iranian Users and Foreign Digital Platforms Implications, Legal Exposure and Regulatory Compliance Strategies

Background

Over the past decade, Iran has emerged as a significant user market for global digital platforms, notwithstanding filtering policies and intermittent access restrictions. Iranian users remain highly active across a wide range of online services, including social media, messaging applications, streaming services, online gaming platforms and digital health-related services. This sustained demand has incentivised many foreign platforms to make their platforms compatible with Iranian community standards and norms, and more importantly, to make their content comply with Iranian laws and regulations.

This engagement typically occurs through cross-border service delivery models. Platforms are hosted outside Iran, operated by foreign legal entities, and distributed through global app stores or web-based access, while key operational elements such as user onboarding, content delivery, moderation, and monetisation are performed digitally.

Economic sanctions have been part of the dynamics of online platforms presence in Iran's market over the past years. Sanctions have particularly played a decisive role in shaping this digital-only engagement. Financial and trade restrictions imposed mainly by the U.S. have effectively compelled foreign platforms to place their headquarters, infrastructure, contractual arrangements, payment processing, and compliance functions outside Iran, while simultaneously discouraging or prohibiting local incorporation, branches, and representation offices. Although sanctions explain the absence of local entities, they do not negate the fact that services are actively rendered into Iran through technical channels. Accordingly, the enforcement measures aimed at preventing Iranian users' access to unauthorised content yet remains applicable.

A common misconception among foreign platform operators is that incorporation or headquarters outside Iran automatically shield them from Iranian law and enforcement. In

practice, however, Iranian regulatory bodies may not base their jurisdiction over foreign platforms solely on the platform's foreign corporate seat or nationality. Instead, they may focus on factual criteria such as targeting of Iranian users and dissemination of content accessible in Iran. Where such elements exist, foreign platforms may be treated as subject to Iranian imperative rules, particularly in areas involving public order, morality, religion, or national security.

Regulatory practice in Iran demonstrates that enforcement against online platforms has been taken seriously. While authorities have acted aggressively in case of domestic platforms' expansive responsibility over user-generated content (**UGC**), they have also deployed a combination of legal and technical measures against foreign platforms hosting non-compliant UGC, including content takedown orders, platform or application blocking, exerting pressure on intermediaries, and in certain exceptional cases, criminal proceedings against managing directors¹.

Against this backdrop, the purpose of this article is to move beyond abstract discussions of jurisdiction and focus on regulatory compliance as a risk-mitigation strategy. It explains why foreign platforms serving Iranian users may become subject to Iranian regulatory requirements and sets out recommendations for platform governance to align with those requirements. This article's focus is exclusively on platforms regulatory compliance considerations in relation to public law and does not address violations of private rights, including intellectual property and data protection claims, nor tax, customs, or other fiscal consequences arising from platform operations.

General Content Restrictions in Practice

Content restriction laws in Iran are grounded in a combination of general laws and specific sectoral regulations. The general legal basis for determining restricted online content categories is rooted in Islamic Penal Code 1996 (*Ta'zirat* section) and Computer Crimes Law 2009, which generally prohibits content that is against public order and morality. More specific types of content are prohibited by laws such as Press Law 1986, Child Protection Law 2020, as well as executive regulations such as the Regulation on Activities of Iranian Internet Websites 2006 and the Regulation Governing Computer Information Networks 2001 (**Information Networks Regulation**).

As the identification and classification of prohibited content under these numerous laws can be complicated and based on subjective interpretation, the Committee for the Determination of Instances of Criminal Content (**Committee**), which operates under the supervision of Attorney General's Office, classifies and makes a list of instances of unlawful content.² These classifications operate as normative guidance for enforcement authorities. This list may be updated from time to time and upon the meetings of the Committee.

¹ For example, the summons issued in 2014 by the Shiraz Prosecution Office against Mark Zuckerberg, in his capacity as the founder of Facebook (now, Meta), while simultaneously initiating proceedings in relation to WhatsApp and Instagram too.

² Article 22 of the Computer Crimes Law 2009.

To this date, the principal categories relevant to online platforms include the following categories:

- (i) *content against public morality and decency*: including sexually explicit or obscene material;
- (ii) *content against religion and sacred values*: including insults or showing disrespect toward Islamic principles, religious beliefs, sacred figures, or religious rituals;
- (iii) *content against public order and national security*: including promotion in favor of groups opposed to the Government, or content that unlawfully affects elections, referenda, or formal civic processes;
- (iv) *content defaming public authorities*: including insults to the authority or legitimacy of state institutions or officials;
- (v) *content promoting or facilitating criminal conduct*: including promotion of violence, drugs, and fraud;
- (vi) *content against health, safety, and public welfare*: including misinformation about medicine with material risk implications;
- (vii) *content related to commercial and economic offences*: including promotion of smuggling, illicit trade, or prohibited commercial activities;
- (viii) *content against children and minors*: including material affecting children's physical, mental, or moral development; and
- (ix) *content related to Gambling and betting*: including promotion or providing services for gambling, betting, or gambling-like mechanisms.
- (x) *content related to Israel*: including any endorsement or support of Israel, or provision of any services to Israelian platforms.

In addition to these statutory prohibitions, Iranian law also provides a special authority for Supreme Council of Cyberspace (**SCC**) to issue orders in relation to the activities in cyberspace. The SCC which has been established pursuant to the order of the Supreme Leader of Iran, holds a supra-legal status whose decisions, according to the established practice, have the force of law.³ Therefore, a platform may be blocked upon the order or resolution of SCC, even if the content in it is not listed in the abovementioned categories.

Platform's Responsibility

³ Supreme Leader's Order on Establishment of Supreme Council of Cyberspace 2012

Foreign platforms that host UGC which is accessible to Iranian users will be subject to a legal environment where there is no explicit allocation of responsibilities over such content and its terms and conditions. Instead, responsibility is inferred from a combination of regulations and resolutions, which together establish a user-centric allocation of liability, coupled with mandatory cooperation duties for platforms.

The clearest articulation of this approach appears in the SCC's Resolution on Policies and Measures for the Organisation and Regulation of Social Messaging Platforms 2017 (**SCC Resolution**). Article 10 of the SCC Resolution provides that responsibility for users' actions on social networks rests with the users themselves, while obliging service providers to cooperate with competent authorities in accordance with applicable laws. This provision is also reflected in the Judiciary's Regulation on the Legal Protection of the Activities of Domestic Social Messaging Platforms 2018 (**Judiciary Regulation**), which adopts the same conceptual distinction between user responsibility and platform cooperation.

A similar inference can be drawn from the Information Networks Regulation. Article 5.3.1 of the Information Networks Regulation states that "Internet service providers (**ISPs**) and users are responsible for the content they make available on the network", which implies that where content is generated by users, responsibility rests with the user rather than the hosting platform. Article 5.3.2 reinforces this approach by placing responsibility for compliance with intellectual property laws on the provider of the information, a logic that has may be extended by analogy to other categories of unlawful content.

These provisions generally imply that responsibility for unlawful UGC does not automatically transfer to the platform or service provider merely by virtue of hosting the content. However, if UGC is considered unlawful according to the abovementioned list, the Committee may order filtering or blocking of the platform, or, where hosting infrastructure is located in Iran, direct the hosting service provider to remove the content.

Such perspective is also largely supported by judicial precedent. In a recent case involving an online classified-ads platform (similar to eBay), the Supreme Court overturned the conviction of the platform's CEO for unlawful user-posted content, holding that responsibility rested with the users and expressly relying on the SCC Resolution and the Judiciary Regulation. The Court further clarified that this principle is not limited to messaging services and applies broadly to platform-based online services. In another case concerning a video-sharing platform, the Supreme Court similarly acquitted the CEO, reasoning that where a platform merely hosts content uploaded by users subject to platform rules and applicable law, liability remains with the user, and the platform is only responsible where it delays or fails to comply with lawful instructions issued by the competent committee. In both cases, timely removal of the content played a decisive role in the outcome.

Enforcement

Once content is classified as falling within a prohibited category, platforms are expected in practice to prevent its availability to users in Iran through removal, restriction, or technical

blocking, regardless of whether the content is generated by users or by the platform itself. While this expectation is not grounded in statutory obligation on platforms, it reflects the regulatory objective of preventing access to unlawful content within Iranian territory. Where a platform fails to take corrective action, authorities typically intervene by imposing access restrictions at the network level, including blocking Iranian IP addresses from reaching the platform through ISPs. This form of ISP-level blocking which applies without even a prior notice is the principal enforcement measure applied in cases of non-compliant content and carries significant commercial consequences for foreign platforms by effectively excluding them from the Iranian user market.

In cases where the platform's hosting infrastructure or service provider is located in Iran, the competent committee or court may instead issue a direct takedown order to the hosting service provider requiring removal of the unlawful content.

While the platform operator or its representatives are not, in principle, criminally liable for the mere existence of unlawful UGC, non-compliance with official removal or blocking orders carries independent legal consequences. In particular, failure to comply with a lawful order issued by the SCC, the Committee, courts, or the cyber police to remove unlawful content constitutes a criminal offence under the Computer Crimes Law 2009, exposing the platform operator to criminal liability for disobedience, rather than for the underlying content itself.

Regarding the effect of reactive moderation by platform, Iranian laws and regulations currently do not provide a formal legal framework for platforms to request reconsideration after content removal. In other words, there is no legally established right for a platform to seek reassessment of its website by the Committee following removal of prohibited content. In practice, however, an unofficial procedure exists whereby a platform can submit a written request to the Deputy for Cyberspace of the Attorney General's Office, confirming that the prohibited content has been removed and requesting unblocking.

Recommendations for Risk Mitigation

For platforms serving Iranian users, the decisive factor in reducing regulatory exposure is not only formal jurisdictional basis, but the ability to demonstrate good faith and operational compliance. In practice, Iranian authorities assess whether a platform has taken reasonable and timely steps to prevent access to unlawful content and to cooperate with competent bodies.

A critical first step is the refinement and localisation of platform legal materials. Generic global terms are rarely sufficient. Platforms should adopt terms and conditions and community rules that encompass Iranian mandatory content categories, supported by a tailored content moderation policy. Making such legal material available in Persian will also help indicate the good faith.

Platforms should also designate a clear regulatory contact point. Embedding cooperation clauses within legal documents and maintaining a defined mechanism for receiving and

executing legal requests from Iranian authorities, even in the absence of a physical presence in Iran is of high importance to mitigate the risk of platform shutdown.

More importantly, regulatory compliance should be treated as an ongoing process rather than a one-off exercise. As the content restriction regulation in Iran is subject to timely updates, periodic audits of moderation practices, legal documentation, and continuous monitoring of regulatory and judicial developments are essential to maintaining alignment with evolving expectations.

Given the aggressive nature of Iranian content restrictions law, early legal structuring, regulatory compliance check, and localisation play a significant role in minimising enforcement risk. Platforms that proactively adapt their regulatory governance and documentation to Iranian requirements are best positioned to preserve market access while maintaining regulatory resilience.

* * *

Disclaimer: The content of this article is provided for informational purposes only and does not constitute legal advice. While every effort has been made to ensure the accuracy and relevance of the information presented, Nami Associates Law Firm accepts no liability for any errors, omissions, or reliance on the content herein. Readers are strongly advised to seek professional legal consultation tailored to their specific circumstances before making any decisions or taking any action based on the information provided in this article. The content should not be interpreted as creating a lawyer-client relationship or as a substitute for personalised legal advice.

Nami Associates is a leading full-service law firm licensed by Iran's Central Bar Association and based in Tehran.⁴ With decades of collective experience, the firm is widely recognised for its exceptional expertise in advising on complex and high-value legal matters in the Iranian market. Nami Associates provides comprehensive legal services across a broad spectrum of practice areas, including corporate and M&A, projects and finance, intellectual property, regulatory compliance, and dispute resolution.

For further information about our practice and experience, please feel free to reach out to us.

Nami Associates Law Firm

37 Asef (Ejazi) Street, Unit 4 South
Zafaraniyeh, Tehran 1988893433, Iran

+98 21 2240 0434 +98 21 2241 8899

info@namiassociates.com

www.namiassociates.com

⁴ Central Bar Association license number 26300099, registration number 53221 and national identification number 14010847783.