

“A Study of the Fundamentals and Challenges of Criminal Liability for Publishing Criminal Content on Social Networks in Iranian Criminal Law”

Arina Abdollahi^{1,*}

1- Master of Criminal Law and Criminology, Islamic Azad University, Sanandaj Branch,
Sanandaj, Iran. arynabdahy91@gmail.com

Abstract

The rapid proliferation of social networks in Iran has fundamentally altered the landscape of public communication, providing a dynamic yet volatile environment for the dissemination of criminal content. While these platforms facilitate unprecedented connectivity, they also serve as conduits for offenses ranging from defamation and hate speech to violations of public morality. The Iranian criminal legal system, primarily rooted in traditional paradigms, faces significant structural and conceptual challenges in addressing these modern cyber-threats. This review article aims to critically analyze the conceptual foundations and enforcement challenges of criminal liability for the publication of criminal content on social networks within the Iranian legal framework. Adopting a review-oriented methodological approach, this study synthesizes academic research, legal doctrines, and policy analyses to assess how Iranian criminal law manages the attribution of liability among users, administrators, and platform operators. The findings reveal that criminal liability in cyberspace is no longer a centralized, straightforward issue but a layered, participatory phenomenon. Traditional elements of actus reus and mens rea are severely challenged by algorithmic amplification, anonymous identities, and non-verbal symbolic communication. The study identifies critical gaps in Iranian judicial practice, including the ambiguity surrounding intermediary liability for channel administrators and the persistent evidentiary limitations in cross-border digital cases. The existing legal framework often struggles to distinguish between legitimate freedom of expression and criminal dissemination, leading to inconsistencies that undermine both public security and civil rights. The conclusion emphasizes that a successful legal response requires a multi-dimensional reform strategy, moving beyond reactive, isolated prohibitions. It advocates for the establishment of specialized cyber-judicial expertise, clearer definitions for intermediary accountability, and the integration of digital literacy into national policy. Ultimately, the article argues for a harmonized approach that balances social protection with procedural fairness to create a resilient cyber-legal framework capable of addressing evolving digital realities.

Keywords: Criminal Liability, Social Networks, Iranian Criminal Law, Cybercrime, Digital Governance

1. Introduction

The rapid expansion of social networks has fundamentally transformed communication, information circulation, and public interaction, but it has also created a new environment in which criminal content can be produced, amplified, and normalized with extraordinary speed. In Iran, this development has posed serious questions for criminal law, particularly regarding the legal basis for assigning criminal liability when unlawful material is published, forwarded, reposted, commented on, or managed through digital platforms.

Unlike traditional media, social networks are decentralized, interactive, and technically layered, which makes it difficult to determine who the “publisher” of content actually is and whether liability should attach to the original uploader, the administrator of a channel or page, the platform itself, or even secondary users who contribute to dissemination. Prior research has shown that the governance structure of social networks in Iran remains a complex policy issue, especially because regulation must respond simultaneously to public order, digital security, expressive freedom, and the changing architecture of online communication (Eslami et al., 2020; Gillespie & Mohammadhosseini, 2021). At the same time, studies on the impact of social networks on cybercrime and on the spread of unethical or socially harmful content suggest that these platforms are not merely passive channels of communication but active spaces in which harmful behavior may be facilitated, encouraged, or operationalized (Mohammadi & Firouz, 2025; Zargar et al., 2020). From this perspective, the legal problem is not simply whether content is “bad” or “offensive,” but whether the publication of such content satisfies the conditions for criminal responsibility under Iranian criminal law, including *actus reus*, *mens rea*, causation, and the attribution of fault in an online environment (Asadi, 2026; Barzegar-Kahnemouyi, 2024).

The significance of this topic is heightened by the fact that criminal content on social networks does not affect only the direct participants in an online exchange; it may also harm third parties, undermine public morality, intensify hate-based hostility, expose individuals to victimization, and weaken social security. Empirical and doctrinal studies have indicated that criminal or unethical content disseminated through networks such as Instagram and Telegram can have measurable effects on social trust, social order, and behavioral patterns, especially where content is designed for wide circulation and emotional reaction (Osareh-Nejad Dezfuli et al., 2019; Danesh Nari et al., 2024). In addition, the spread of hate speech and insulting or degrading messages in cyberspace demonstrates that the harms caused by online content are not limited to direct threats or explicit offenses; they may also arise from symbolic violence, collective incitement, personality-rights violations, and repeated exposure to harmful narratives (Naderi & Khaledian, 2023; Ghavami-Pour Serashkeh & Mahmoudi, 2025). The criminal-law challenge is therefore twofold: first, to identify the content and conduct that should be considered criminal in the digital context; and second, to establish a legally sustainable framework for responsibility that can distinguish between intentional participation in illicit publication and mere presence, negligence, or technical involvement. This difficulty is particularly visible where emojis, short-form reactions, reposting features, anonymous accounts, and algorithmic amplification blur the boundary between expressive behavior and participation in offense, making interpretation and proof more complicated than in offline settings (Laki et al., 2023; Sheidaian et al., 2021). Accordingly, a review of the foundations and challenges of criminal liability in this area is not only doctrinally important but also practically necessary for courts, legislators, prosecutors, and digital regulators.

This article adopts a review-oriented approach and examines the foundations of criminal liability for publishing criminal content on social networks in Iranian criminal law, along with the principal legal and practical challenges that arise in enforcement. The analysis focuses on three interconnected dimensions. First, it considers the conceptual and normative basis of liability, including how criminal law traditionally understands publication, participation, aiding, and intent, and how these concepts must be adapted to account for platform-based communication. Second, it addresses the institutional and regulatory challenges of enforcement in cyberspace, such as proving authorship, preserving digital evidence, defining the responsibility of administrators and intermediaries, and managing the tension between state regulation and platform self-governance (Gillespie & Mohammadhosseini, 2021; Asadi, 2026). Third, it examines the broader criminological and policy implications of online criminal content, including its association with recidivism, high-risk behaviors, victimization, and the commercialization of harmful digital practices (Adibi Rekavandi, 2024; Zarei & Nikkhah, 2024). By synthesizing the available literature, this article seeks to clarify how Iranian criminal law can respond more coherently to the realities of social-network communication without collapsing into over-criminalization or leaving harmful conduct without adequate legal accountability. In this sense, the discussion is not limited to technical liability rules; it also raises deeper

questions about proportionality, digital governance, public ethics, and the proper balance between freedom of expression and the protection of social order in online spaces.

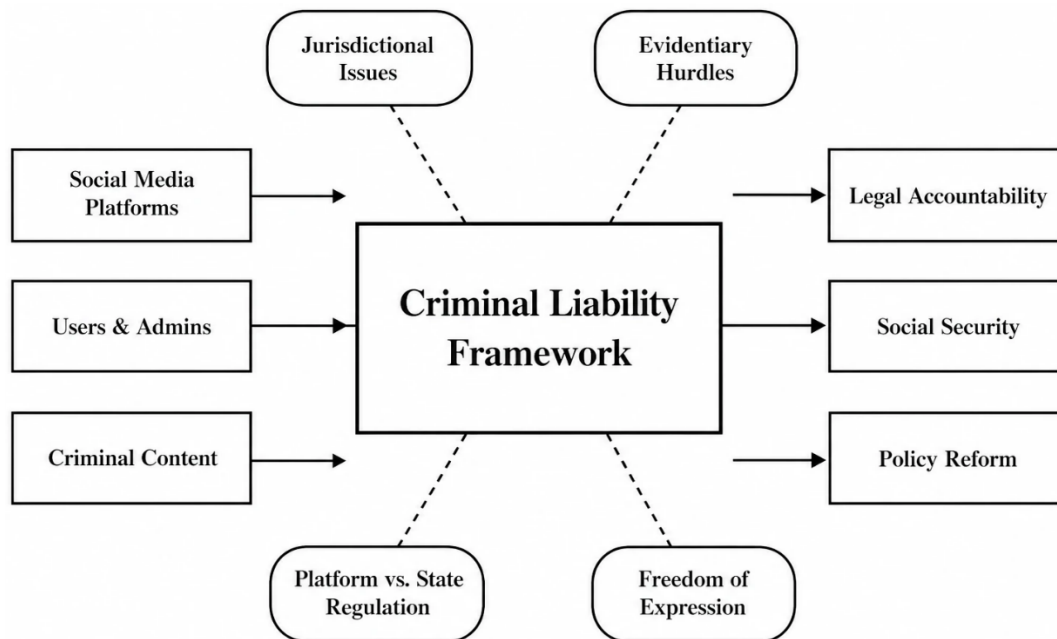


Figure 1. Conceptual Framework of Criminal Liability for Online Content in the Iranian Legal System.

The conceptual model depicted in Figure 1 illustrates the multifaceted ecosystem of criminal liability within the context of Iranian social networks. At the core of the model is the Criminal Liability Framework, which serves as the primary legal mechanism for processing digital offenses. The model is structured into three main dimensions:

1. **Inputs (Drivers of Liability):** On the left, the model identifies the primary sources of legal engagement: the Social Media Platforms themselves (as the technical infrastructure), the Users & Administrators (as the active human agents), and the Criminal Content (the material basis of the offense). These elements interact to trigger the legal process.
2. **Influencing Challenges (Contextual Variables):** Surrounding the central framework are the four critical challenges identified in this study. Jurisdictional Issues and Evidentiary Hurdles represent technical and legal obstacles to enforcement, while the tension between Platform vs. State Regulation and the protection of Freedom of Expression represent the normative and policy conflicts that lawmakers must balance.
3. **Outputs (Regulatory Goals):** On the right, the model shows the intended outcomes of a functional liability framework. These include achieving Legal Accountability for offenders, ensuring Social Security for the public, and providing a basis for continuous Policy Reform to adapt to the evolving digital landscape.

In summary, this model demonstrates that criminal liability for online content is not a simple linear process but a complex interaction between technical actors, legal obstacles, and social objectives.

2. Conceptual and Legal Foundations of Criminal Liability for Online Content

The conceptual framework for defining “criminal content” within the architecture of Iranian social networks requires a nuanced understanding of how digital information traverses public, semi-public, and private virtual spaces. In the traditional Iranian legal paradigm, criminal content is largely categorized based on its potential to infringe upon public morality, national security, or the dignity of individuals. However, the transition to social media necessitates a broader interpretation of these definitions because the digital environment is characterized by persistent visibility, algorithmic amplification, and the active engagement of users. Research suggests that content, which might be ignored in a transient, offline conversation, becomes “criminal” in an online context precisely because of its capacity for rapid dissemination and its impact on social security (Zargar et al., 2020). The definition of criminal content, therefore, cannot be static; it must encompass the functional reality of how content is perceived by the public, manipulated by the network, and utilized to incite behavior. As studies on public ethics have demonstrated, components such as user-generated commentary, visual symbolism, and the overall narrative framing of a post determine whether content is classified as socially harmful or inherently criminal, often requiring authorities to look beyond the literal meaning of text and evaluate the intent behind the circulation of the data (Osareh-Nejad Dezfouli et al., 2019). Consequently, the legal foundation for liability must be built upon an appreciation of the unique social dynamics of digital networks, where the boundary between personal expression and the commission of a crime is frequently blurred by the platform's own design features.

The elements of criminal liability—specifically the *actus reus* (guilty act) and *mens rea* (guilty mind)—undergo significant transformation when transposed from the physical world to the digital realm, creating distinct challenges for attributing responsibility. In the context of Iranian criminal law, the act of “publishing” is no longer limited to the initial creator of a post; it extends to those who facilitate the content’s availability, such as channel administrators, group moderators, and even algorithmic systems that promote specific trends. The liability of channel administrators, in particular, is a critical area of study, as they are often positioned as the gatekeepers of their respective digital environments. Research indicates that administrators in domestic messaging networks bear a specific, heightened duty of care regarding the dissemination of content contrary to public decency, and their failure to prevent or remove such content can constitute a distinct form of criminal negligence or even complicity (Barzegar-Kahnemouyi, 2024). Furthermore, the *actus reus* itself is becoming increasingly complex due to the use of non-textual communicative tools. The interpretative challenges posed by emojis, stickers, and reaction functions in social networks have complicated the judicial process, as these symbols can fundamentally alter the meaning of a text, transforming seemingly benign statements into criminal threats or insults, thereby necessitating a more sophisticated approach to interpreting digital evidence (Laki et al., 2023). Without a clear consensus on how these communicative acts translate into legal elements, courts often struggle to maintain consistency in their rulings, leading to unpredictable outcomes in cyber-criminal trials.

Furthermore, the theoretical underpinnings of this liability must reconcile the dichotomy between state-imposed regulation and the governance models utilized by digital platforms. The emergence of “platform governance” suggests that modern digital spaces are not merely neutral hosts but are active regulators that shape user behavior, often prioritizing engagement over legal compliance or public safety (Gillespie & Mohammadhosseini, 2021). This creates a theoretical conflict in criminal law: if the platform’s own architecture facilitates or encourages the dissemination of harmful content, the legal burden of responsibility cannot solely rest on individual users or local administrators. Instead, the theoretical foundation of criminal liability must evolve to address the systemic nature of digital networks, acknowledging that regulation by the platform often competes with, and sometimes undermines, regulation by the state (Gillespie & Mohammadhosseini, 2021). This necessitates a regulatory framework that holds platforms accountable for their design choices, which may indirectly incentivize the publication of criminal content. Recent policy studies in Iran emphasize that the current governance structure is insufficient if it treats platforms as passive conduits rather than active participants in the digital ecosystem (Eslami et al., 2020). Therefore, establishing



a solid theoretical basis for liability requires shifting toward an approach that integrates standard criminal-law principles with a modern understanding of cyber-sociology, ensuring that liability attaches in a proportional manner to all actors who exert influence over the flow of criminal content within the network (Asadi, 2026).

3. Criminal Liability for Publishing Criminal Content in Iranian Criminal Law

3.1. Relevant Legal Provisions in Iran

Iranian criminal law addresses the publication of criminal content through a combination of the Islamic Penal Code, the Cybercrimes Law of 2009, and various regulations on media and online platforms, yet the integration of these instruments in the digital context remains incomplete and frequently contested. The Cybercrimes Law specifically criminalizes acts such as insult, defamation, publication of obscene content, and dissemination of material contrary to public morality and decency, but its provisions were drafted before social networks acquired the algorithmic, interactive, and horizontally expanded structure they possess today. This temporal mismatch means that courts are often forced to interpret older provisions through analogy and purposive reasoning rather than through clear legislative guidance, which generates inconsistency and unpredictability in judgments (Mohammadi & Firouz, 2025). Moreover, the legal framework does not systematically distinguish among the different roles that actors play in the dissemination process, treating posting, sharing, commenting, and managing a page as a single undifferentiated category of "publication." Consequently, the identification of the relevant legal provision depends heavily on the subjective characterization of each digital act, which creates vulnerability to arbitrariness and makes the enforcement of criminal norms in cyberspace particularly contentious. At the same time, the constitutional recognition of freedom of expression imposes an implicit limitation on the criminalization of online content, requiring prosecutors and courts to demonstrate that the harm caused by a specific publication outweighs the expressive interest at stake (Naderi & Khaledian, 2023). The legal provisions, therefore, exist within a fragile balance, where the letter of the law must be reconciled with the realities of digital communication and the competing values of social protection and individual liberty.

3.2. Role of Intent, Knowledge, and Participation

The attribution of criminal liability for online content depends critically upon establishing the mental state of each participant, and this requirement is substantially complicated by the collaborative and rapid nature of social-network interactions. In the physical world, intent is usually inferred from the direct, observable relationship between the actor and the harmful consequence, but in cyberspace, the chain of causation is fragmented across multiple users, devices, and platforms, making it difficult to determine whether a person genuinely intended to commit an offense or merely engaged in casual digital behavior that had unintended legal consequences. The concept of knowledge is equally problematic, because social-network interfaces may conceal the criminal nature of content from ordinary users, particularly where emojis, sarcasm, visual memes, or indirect allusions are used to express a message that is not immediately apparent on its face (Laki et al., 2023). Iranian courts have struggled with this ambiguity, as they must decide whether a defendant who simply shared or reacted to content possessed sufficient awareness of its criminal character to justify punishment, and this determination often relies on circumstantial and contextual evidence that is inherently uncertain. Furthermore, the doctrine of participation is rarely adapted to the specific dynamics of digital networks, where an individual may contribute to the commission of an offense without ever directly communicating with any other participant, simply by amplifying content, disabling moderation features, or refusing to remove harmful material after being notified (Barzegar-Kahnemouyi, 2024). The question of whether passive presence or silent endorsement constitutes criminal complicity remains unresolved in both doctrine and judicial practice, leaving a significant gap between the traditional requirements of the criminal

law and the operational realities of online behavior (Ghavami-Pour Serashkeh & Mahmoudi, 2025). Addressing this challenge requires a reconceptualization of intent and participation that acknowledges the distinct ways in which agency is exercised in digital environments without abandoning the fundamental principle that punishment presupposes a blameworthy state of mind.

3.3. Liability of Users, Administrators, and Platform Managers

The question of who bears criminal responsibility in the dissemination of unlawful content has become one of the most controversial issues in Iranian cyberspace jurisprudence, because the actors involved possess fundamentally different levels of control, awareness, and technical capacity. Ordinary users may publish or repost criminal content without understanding its legal implications, and their liability is often contested on the grounds that they were merely exercising freedom of expression or acting out of ignorance of the content's criminal character. In contrast, channel and page administrators occupy a position of enhanced responsibility, because they are presumed to have the authority to moderate, filter, or remove content; their failure to exercise this authority over material contrary to public decency can be characterized as negligence or, in more serious cases, as tacit approval of the offense (Barzegar-Kahnemouyi, 2024). The degree to which administrators are held liable therefore depends significantly on factors such as the size of their audience, the persistence of the harmful content, and whether they had received specific notice of the violation, but these factors are not uniformly recognized across judicial decisions. Platform managers and technology companies present an even higher order of complexity, because they operate across jurisdictions and control the very infrastructure through which content circulates, yet they are frequently shielded from local criminal liability by their remote location and by the technical architecture of their services. The prevailing approach in Iranian law has been to treat platforms primarily as intermediaries whose responsibility derives from their failure to cooperate with judicial authorities or to implement reasonable takedown mechanisms, rather than as active agents of the offense (Gillespie & Mohammadhosseini, 2021). This perspective, however, is increasingly criticized for failing to acknowledge the extent to which platform algorithms, recommendation systems, and engagement-driven design actively shape which criminal content reaches the public (Asadi, 2026; Mohammadi & Firouz, 2025). A coherent framework for criminal liability must therefore distinguish carefully among these categories of actors, assigning responsibility in proportion to actual control and awareness, while ensuring that the practical enforcement of the law is not defeated by the dispersion of authority across the digital ecosystem (Eslami et al., 2020; Adibi Rekavandi, 2024).

4. Major Challenges in Proving and Enforcing Liability

4.1. Jurisdictional Problems in Social Media Cases

One of the most persistent obstacles to the enforcement of criminal liability in the digital era is the mismatch between the territorial nature of Iranian criminal law and the global, borderless architecture of social networks. When criminal content is published on platforms like Instagram or Telegram, the physical location of the server, the uploader, and the platform's headquarters are often in different countries, each governed by conflicting legal standards regarding speech and privacy. Iranian judicial authorities frequently face "jurisdictional vacuums" where they possess the legal authority to prosecute a resident user but lack the technical or diplomatic means to compel foreign platforms to provide the metadata or user logs necessary for a conviction (Gillespie & Mohammadhosseini, 2021). Furthermore, the debate over "regulation on the platform versus regulation by the platform" highlights a fundamental sovereignty challenge; global platforms often prioritize their own community standards over local Iranian laws, leading to a situation where content deemed criminal under Iranian law remains accessible due to the platform's refusal to cooperate with local warrants (Asadi, 2026). This creates a fragmented legal landscape where the state's ability to protect social security and public order is severely hampered by the technical and geopolitical realities of the internet.

4.2. Identification of Offenders and Digital Evidence

The technical difficulty of identifying the true author of criminal content constitutes a major hurdle in the Iranian judicial process, as offenders frequently utilize anonymizing tools, fake profiles, and Virtual Private Networks (VPNs) to obscure their digital footprint. Unlike traditional crimes where physical evidence is tangible, digital evidence is ephemeral, easily manipulated, and requires specialized forensic expertise to be admissible in court. Studies on criminal identification on platforms such as Instagram show that even when a profile is linked to a crime, proving that a specific individual was the one behind the screen at the exact moment of publication remains a significant hurdle (Danesh Nari et al., 2024). This problem is exacerbated by the use of non-verbal communication, such as emojis and stickers, which can carry criminal intent but are difficult to interpret with the degree of certainty required by criminal law (Laki et al., 2023). Without a robust mechanism for digital attribution, many cases fail at the evidentiary stage, leading to a sense of impunity among cyber-offenders and a corresponding increase in recidivism and high-risk behaviors within these digital spaces (Adibi Rekavandi, 2024).

4.3. Freedom of Expression vs. Criminal Restriction

The tension between the constitutional protection of freedom of expression and the need to restrict criminal content represents a core normative challenge for the Iranian legal system. Defining the exact point at which a critical opinion or a social commentary transforms into a "hate crime" or an "offense against public decency" is a subjective and often politicized process. Research into hate crimes in cyberspace indicates that without clear, objective criteria for what constitutes harmful speech, there is a risk of over-criminalization, which can stifle legitimate public discourse and civic engagement (Naderi & Khaledian, 2023). On the other hand, the unrestricted spread of unethical or inflammatory content can lead to female victimization, the objectification of individuals, and a general erosion of social security (Sheidaian et al., 2021; Zargar et al., 2020). Iranian lawmakers are thus faced with the difficult task of crafting laws that are specific enough to target actual criminal behavior without being so broad that they infringe upon the fundamental rights of users to participate in the digital public square (Eslami et al., 2020).

4.4. Technical and Procedural Obstacles

Finally, the procedural framework for handling cyber-crimes in Iran often lags behind the rapid technological evolution of social networks. The legal system struggles to keep pace with new business models and "anti-marketing" strategies that facilitate criminal behavior under the guise of digital entrepreneurship (Zarei & Nikkhah, 2024). Additionally, the lack of standardized executive guarantees for compliance with national standards means that even when a crime is identified, the process of removing the content or holding the administrator accountable is slow and inefficient (Asadi, 2026). The role of channel administrators remains a particularly gray area; while they are often held liable for the content within their groups, the lack of clear procedural guidelines on how they should moderate content in real-time creates a "liability trap" that discourages responsible platform management (Barzegar-Kahnemouyi, 2024). These technical and procedural barriers collectively undermine the effectiveness of the Iranian criminal justice system in responding to the unique challenges of the digital age, necessitating a comprehensive reform of both substantive law and judicial procedure (Mohammadi & Firouz, 2025; Osareh-Nejad Dezfuli et al., 2019).

5. Findings and Discussion

The review of Iranian criminal law concerning the dissemination of criminal content on social networks demonstrates that the legal system is currently positioned between two competing realities: on the one hand, the necessity of protecting social order, public morality, and individual rights in cyberspace; and on the other

hand, the practical and conceptual limitations of applying traditional criminal-law doctrines to highly dynamic digital environments. The findings of the reviewed literature indicate that social networks have transformed the structure of criminal participation by decentralizing the process of publication and allowing multiple actors to contribute simultaneously to the production, amplification, and normalization of unlawful content. Unlike conventional criminal acts where the offender is usually identifiable and physically connected to the prohibited behavior, cyberspace disperses agency across users, administrators, advertisers, recommendation algorithms, and platform infrastructures, thereby complicating the legal process of attributing criminal responsibility (Gillespie & Mohammadhosseini, 2021; Mohammadi & Firouz, 2025). The reviewed studies consistently reveal that Iranian criminal law has not yet fully adapted its substantive and procedural mechanisms to these transformations, resulting in interpretive inconsistencies, evidentiary difficulties, and gaps in enforcement (Asadi, 2026; Eslami et al., 2020).

Table 1. Major Foundations of Criminal Liability in Social Networks under Iranian Criminal Law

Legal Foundation	Description	Main Challenge	Supporting Source
Publication of unlawful content	Dissemination of illegal text, image, or video	Ambiguous definition of publication	Mohammadi & Firouz (2025)
Criminal intent	Awareness and intention to spread harmful content	Difficulty proving digital intent	Laki et al. (2023)
Participation and complicity	Shared responsibility among multiple users	Unclear limits of participation	Barzegar-Kahnemouyi (2024)
Protection of public morality	Prevention of immoral or indecent content	Broad interpretation by courts	Zargar et al. (2020)
Protection of personality rights	Safeguarding dignity and privacy	Conflict with free expression	Ghavami-Pour Serashkeh & Mahmoudi (2025)
Cybersecurity and public order	Preventing online threats and instability	Cross-border enforcement issues	Asadi (2026)
Platform governance	Regulation through digital platforms	Weak accountability mechanisms	Gillespie & Mohammadhosseini (2021)

The findings summarized above indicate that Iranian criminal law relies heavily upon classical concepts such as intent, participation, and publication, yet these principles become unstable when applied to decentralized online environments. The ambiguity surrounding digital publication particularly weakens legal certainty because reposting, reacting, or indirectly amplifying content may produce harmful consequences without fitting neatly into traditional criminal categories (Laki et al., 2023). As a result, courts often adopt broad interpretations to fill legislative gaps, increasing the risk of inconsistent rulings.

Another significant finding emerging from the reviewed literature is that the role of social-network administrators and platform managers has become central to contemporary debates on criminal liability. Earlier legal approaches focused almost exclusively on the direct offender, but the architecture of social media has redistributed power toward intermediaries who control visibility, moderation, and circulation mechanisms. Channel administrators, for instance, are increasingly perceived as quasi-regulatory actors whose failure to remove harmful material may itself constitute a form of criminal negligence or tacit approval (Barzegar-Kahnemouyi, 2024). Simultaneously, global platforms employ algorithmic systems that actively prioritize engagement, often amplifying sensational or controversial content regardless of its legality under domestic law (Gillespie & Mohammadhosseini, 2021). This evolution has fundamentally altered the concept of fault in cyberspace because harmful outcomes may emerge not from one intentional actor but from an interactive network of users and automated systems.

Table 2. Main Actors and Their Potential Criminal Liability in Social Networks

Actor	Nature of Role	Type of Possible Liability	Key Legal Problem
Ordinary user	Posting or sharing content	Direct criminal liability	Lack of legal awareness
Channel administrator	Managing and moderating content	Negligence or complicity	Undefined moderation duties
Platform manager	Providing infrastructure	Indirect or regulatory liability	Jurisdictional limitations
Content creator	Producing criminal material	Primary criminal liability	Attribution of authorship
Followers/commenters	Amplifying harmful discourse	Secondary participation	Ambiguous participation threshold
Advertisers/influencers	Promoting harmful pages	Commercial facilitation liability	Weak monitoring mechanisms
Automated algorithms	Recommending content	Structural contribution to harm	Absence of legal personhood

The table demonstrates that liability in cyberspace is no longer concentrated on a single offender. Instead, criminal conduct emerges through layered interactions among users, administrators, and digital infrastructures. This diffusion of responsibility complicates the application of traditional doctrines because the degree of actual control over harmful content varies substantially among actors. The absence of clear standards for intermediary liability therefore remains one of the most urgent deficiencies in Iranian cyber-criminal law.

The review further demonstrates that evidentiary and procedural difficulties remain among the most serious barriers to effective enforcement. Criminal prosecution in cyberspace depends heavily on digital evidence, including metadata, IP logs, screenshots, archived communications, and algorithmic traces, yet many of these forms of evidence are unstable or technically vulnerable to manipulation. Research on criminal identification in Instagram environments indicates that proving authorship frequently depends upon circumstantial evidence rather than direct forensic certainty, which weakens prosecutorial reliability and raises concerns regarding due process (Danesh Nari et al., 2024). Moreover, the prevalence of anonymous accounts and encrypted communication has intensified the challenge of linking online behavior to a legally identifiable individual. The studies also reveal that visual symbols and emojis increasingly function as communicative tools capable of conveying threats, insults, or coded criminal meanings, thereby forcing courts to interpret digital language in ways not anticipated by traditional evidentiary doctrine (Laki et al., 2023).

Table 3. Key Evidentiary Challenges in Cybercrime Prosecution

Evidentiary Issue	Description	Impact on Criminal Proceedings	Supporting Source
Anonymous accounts	Hidden identity of offenders	Difficulty identifying suspects	Danesh Nari et al. (2024)
VPN and encryption use	Concealment of digital location	Weakens jurisdictional authority	Asadi (2026)
Manipulation of evidence	Editing or deleting online data	Reduced evidentiary reliability	Mohammadi & Firouz (2025)
Emoji interpretation	Ambiguous symbolic communication	Inconsistent judicial interpretation	Laki et al. (2023)
Cross-border servers	Data stored outside Iran	Delayed judicial cooperation	Gillespie & Mohammadhosseini (2021)

Algorithmic amplification	Automated spread of content	Difficulty assigning causation	Eslami et al. (2020)
Rapid dissemination speed	Viral spread within minutes	Delayed intervention effectiveness	Osareh-Nejad Dezfuli et al. (2019)

The evidence-related challenges identified above demonstrate that criminal procedure in cyberspace requires technological adaptation alongside legal reform. Existing evidentiary frameworks were largely designed for physical crimes involving tangible proof, whereas digital environments produce fluid, mutable, and often transnational evidence. Without investment in digital forensic expertise and clearer procedural standards, the gap between cybercriminal behavior and judicial capability is likely to widen further.

An additional finding concerns the broader criminological and social consequences of criminal content dissemination. The literature strongly suggests that exposure to violent, unethical, hateful, or degrading online material can contribute to normalization processes that increase aggression, recidivism, and high-risk behavior patterns among users (Adibi Rekavandi, 2024). Female victimization, cyber-harassment, and personality-rights violations appear particularly significant in Iranian social networks, where visual objectification and coordinated harassment campaigns may inflict psychological and reputational harm extending far beyond the virtual environment (Sheidaian et al., 2021; Ghavami-Pour Serashkeh & Mahmoudi, 2025). At the same time, policymakers face the challenge of balancing these harms against the constitutional and ethical importance of preserving freedom of expression and public participation in digital discourse. Excessive criminalization risks suppressing legitimate criticism and social debate, while insufficient regulation may encourage the spread of harmful narratives and criminal subcultures (Naderi & Khaledian, 2023).

Table 4. Proposed Legal and Policy Reforms for Iranian Cyber Criminal Law

Proposed Reform	Objective	Expected Benefit	Related Source
Clearer definition of criminal content	Reduce interpretive ambiguity	Greater judicial consistency	Mohammadi & Firouz (2025)
Specialized cybercrime courts	Improve technical expertise	Faster and more accurate rulings	Asadi (2026)
Stronger platform cooperation rules	Enhance evidence access	Better enforcement capacity	Gillespie & Mohammadhosseini (2021)
Digital literacy programs	Raise public legal awareness	Prevention of accidental offenses	Eslami et al. (2020)
Advanced forensic infrastructure	Improve evidence authentication	Increased prosecutorial reliability	Danesh Nari et al. (2024)
Protection of personality rights	Reduce online victimization	Greater user trust and safety	Ghavami-Pour Serashkeh & Mahmoudi (2025)
Balanced free-expression safeguards	Prevent over-criminalization	Preservation of civil liberties	Naderi & Khaledian (2023)

The proposed reforms illustrate that effective cyber-criminal regulation requires an integrated approach combining legal precision, technical capability, institutional reform, and educational policy. Merely expanding criminal prohibitions without addressing evidentiary weaknesses and governance deficiencies is unlikely to produce sustainable outcomes. A balanced legal framework should therefore pursue accountability while simultaneously preserving procedural fairness and legitimate digital expression. Overall, the findings indicate that Iranian criminal law is currently undergoing a transitional phase in its encounter with digital modernity. Traditional legal concepts remain relevant, but their practical

implementation has become increasingly strained under the pressures of algorithmic communication, transnational platforms, and participatory online culture. The future effectiveness of criminal liability in this area will depend largely upon the ability of lawmakers and judicial institutions to construct a coherent cyber-legal framework that is technologically informed, normatively balanced, and procedurally reliable (Asadi, 2026; Gillespie & Mohammadhosseini, 2021; Mohammadi & Firouz, 2025).

6. Conclusion

This review article has analyzed the foundations and challenges of criminal liability for the publication of criminal content on social networks within the Iranian legal system. The investigation reveals that the digital era has fundamentally disrupted the traditional paradigm of criminal law, necessitating a shift from a reactive, individual-focused approach to a proactive, systemic framework that accounts for the complexities of modern social media. The findings highlight that the act of "publishing" is no longer a discrete event attributable to a single individual, but rather a fluid process involving an interconnected network of users, page administrators, platform algorithms, and commercial entities. This diffusion of agency creates a significant "liability gap" where existing laws, designed for a pre-digital or early-digital era, struggle to adequately capture the nuances of online conduct, leading to inconsistencies in judicial interpretation and enforcement (Mohammadi & Firouz, 2025; Gillespie & Mohammadhosseini, 2021).

The core challenge for Iranian law lies in reconciling the protection of public order, morality, and social security with the preservation of freedom of expression and digital innovation. As established in the review, the absence of a clear, standardized definition of "criminal content" in the digital context—particularly when utilizing non-verbal cues such as emojis or symbolic interaction—leaves both citizens and the judiciary in a state of legal uncertainty (Laki et al., 2023). Furthermore, the reliance on traditional evidentiary methods, while effective for physical crimes, is increasingly insufficient for the ephemeral, encrypted, and cross-border nature of digital evidence. The technical hurdles, including the use of VPNs, anonymizing tools, and the jurisdictional impossibility of compelling foreign platforms to comply with local warrants, suggest that substantive legal reform must be accompanied by significant investment in digital forensic infrastructure and specialized judicial training (Asadi, 2026; Danesh Nari et al., 2024).

To address these shortcomings, it is recommended that Iranian lawmakers pursue a multi-dimensional reform strategy. First, the legislature should clarify the scope of liability for various actors within the digital ecosystem, distinguishing between primary offenders who create and initiate criminal content, and secondary actors—such as channel administrators and platform hosts—whose liability should be contingent upon their capacity to moderate and their failure to act upon notification (Barzegar-Kahnemouyi, 2024). Second, the establishment of specialized cyber-criminal courts or units, equipped with advanced digital forensic capabilities, is essential to bridge the gap between technical complexity and judicial output. Third, policy efforts should prioritize public education and digital literacy, as many instances of criminal content dissemination stem from ignorance of the law or a lack of understanding regarding the long-term impact of online behavior on social security and personal reputation (Eslami et al., 2020; Zargar et al., 2020). Finally, the regulation of social networks must be viewed as an ongoing process rather than a static legislative achievement. As technologies such as generative AI and new forms of algorithmic influence continue to evolve, the legal framework must remain agile, evidence-based, and proportional. An overly restrictive approach risks suppressing legitimate civic discourse and alienating the public, while a hands-off approach leaves vulnerable groups—particularly women and youth—exposed to victimization and objectification (Sheidaian et al., 2021; Ghavami-Pour Serashkeh & Mahmoudi, 2025). Ultimately, the goal of Iranian criminal law in this domain should be to foster a secure, ethical, and responsible digital environment that serves the interests of the public without infringing upon fundamental liberties. By harmonizing substantive legal precision with robust procedural capability, Iran can build a coherent cyber-law framework capable of addressing the challenges of the present and the uncertainties of the future.

References

- Adibi Rekavandi, R. (2024). A criminological study of the impact of social networks on recidivism patterns and high-risk behaviors. *Encyclopedia of Comparative Jurisprudence and Law*, 1-25. [In Persian]
- Asadi, S. (2026). Executive guarantees for compliance with global and national standards in virtual platforms against committing crimes and publishing criminal content. *Comparative Research in Jurisprudence, Law, and Politics*, 7(4), 1-20. [In Persian]
- Barzegar-Kahnemouyi, S. (2024). Criminal liability of channel administrators in domestic messaging networks against the dissemination of content contrary to public decency. *International and National Conference on Management, Accounting, and Law Studies*, 10(10), 2581-2609. [In Persian]
- Danesh Nari, A., Tabarsi, F. H., Hejazi, S., & Mahla, M. (2024). Criminal identification on Instagram: A case study of followers' comments on thugs' pages. *Social Welfare Quarterly*, 24(92), 237-276. [In Persian]
- Eslami, M., Jafari-Moghaddam, S., & Hojjat, H. (2020). Governance structure and policymaking of social networks in Iran. *Public Policy*, 24(6), 151-171. [In Persian]
- Ghavami-Pour Serashkeh, S., & Mahmoudi, M. (2025). Violation of the personality rights of third parties in social networks. *Public Law Scale (Mizan-e-Hoghugh-e-Ame)*, 1(2). [In Persian]
- Gillespie, T., & Mohammadhosseini, M. (2021). From regulation on the platform to regulation by the platform (The challenge of legislation in cyberspace; Who is responsible for publishing inappropriate content?). *Society, Culture, and Media*, 39(10), 245-260. [In Persian]
- Laki, A., Saberi, M., & Moradi, M. (2023). The role of emojis in committing crimes and interpretative challenges. *Legal Research*, 22(54), 313-344. [In Persian]
- Mohammadi, F., & Firouz, A. (2025). Investigating the impact of social networks on the increase of cybercrimes and its legal challenges. *Legal Discourse*, 13(26), 5-33. [In Persian]
- Naderi, N., & Khaledian, K. (2023). Investigating hate crimes in cyberspace. *Legal Studies*, 69(8), 71-94. [In Persian]
- Osareh-Nejad Dezfali, S., Firouzian, E., & Ghane, A. (2019). Extraction and prioritization of components effective in reducing the dissemination of criminal content regarding public ethics in Telegram. [Conference Paper/Technical Report]. [In Persian]
- Sheidaian, M., Dehghani, R., Mir-Khalili, S. M., & Darabi, S. (2021). Criminological explanation of female victimization in social networks; With emphasis on objectification theory. *Modares Criminal Law and Criminology*, 1(2), 67-95. [In Persian]
- Zarei, A., & Nikkhah, H. (2024). Providing an anti-marketing model to prevent criminal behaviors in the online and digital business environment. *Business Management*, 16(2), 349-387. [In Persian]
- Zargar, A., Abdolrahmani, R., Sahari, S., & Omid, O. (2020). Investigating the impact of unethical content of virtual social networks on social security (Case study: Instagram network). *Scientific Quarterly of Social Security Studies*, 11(63), 73-96. [In Persian]