


The Impact of Social Media on Criminalization and Criminal Behaviors in the Criminal Justice Systems of Iran and Afghanistan

1. Ali Danesh Bakhteari : Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran

2. Abbas Tadayyon *: Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran

3. Mahdi Esmacili : Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran

*Correspondence: ab.tadayyon@iau.ac.ir

Abstract

Social media, as one of the most significant manifestations of communication transformation in the digital era, plays a substantial role in shaping attitudes, social interactions, and behavioral patterns of individuals. The rapid expansion of these platforms, while creating extensive opportunities for information dissemination, social participation, and crime prevention, has simultaneously provided grounds for the emergence and development of new forms of criminal behavior, thereby confronting legal systems with serious challenges in the fields of criminalization and criminal policy-making. The present study adopts a descriptive–analytical approach and relies on library-based sources to examine the role of social media in the formation and evolution of criminal behaviors and their impact on the process of criminalization in Iran and Afghanistan. The article first clarifies the concept of social media and criminalization, as well as the governing principles underlying criminalization policies. Subsequently, drawing upon criminological theories—including social learning theory, cultivation theory, labeling theory, and arousal theory—the mechanisms through which media influence criminal behaviors are analyzed. The findings indicate that social media, through facilitating observational learning, normalizing violence, and amplifying certain behaviors, may play an effective role in the expansion of crimes such as online fraud, virtual defamation, dissemination of false information, and offenses against national security. The study then comparatively examines the legal frameworks and criminal policies of Iran and Afghanistan, explaining the similarities and differences in approaches to criminalization and penal responses toward media-related crimes. The results demonstrate that social media possess a dual nature, and that effective criminal policy in this domain requires the adoption of a balanced approach combining penal control, social prevention strategies, and the promotion of media literacy—an approach capable of safeguarding social security while simultaneously protecting the fundamental rights and freedoms of citizens.

Keywords: Social media; Criminalization; Criminal behavior; Cybercrime; Criminal policy; Criminal law; Iran; Afghanistan.

Received: 01 January 2026

Revised: 27 April 2026

Accepted: 02 May 2026

Initial Publication 03 June 2026

Final Publication 01 July 2026



Copyright: © 2026 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Citation: Danesh Bakhteari, A., Tadayyon, A., & Esmacili, M. (2026). The Impact of Social Media on Criminalization and Criminal Behaviors in the Criminal Justice Systems of Iran and Afghanistan. *Legal Studies in Digital Age*, 5(4), 1-13.

1. Introduction

The rapid expansion of communication technologies and the increasing penetration of the Internet into individual and social life have transformed social media into one of the most significant and influential phenomena of the contemporary era. By enabling the rapid production, dissemination, and exchange of information, these platforms play a decisive role in shaping public opinion, behavioral patterns, and social relationships. At the same time, the interactive nature, ease of access, and transnational characteristics of social media have turned cyberspace into a fertile environment for the emergence and expansion of new forms of criminal behavior—behaviors that often differ from traditional crime patterns and have confronted legal systems with novel challenges in criminalization and criminal policy-making (Atabi et al., 2021; Gholamhosseinnejad, 2020).

On the one hand, social media may function as effective tools for crime prevention, enhancement of citizens' legal awareness, and strengthening of social supervision; on the other hand, due to their strong capacity to influence users' attitudes and emotions, they may facilitate learning, imitation, and normalization of criminal conduct. The increase in cybercrimes, online defamation, dissemination of false information, internet fraud, and misuse of cyberspace to threaten public and national security represent some of the negative consequences associated with these platforms in contemporary societies (Ghaemi et al., 2024; Naghavi, 2021). This situation highlights the growing necessity of rethinking the concept of criminalization, the governing principles underlying it, and the manner in which criminal justice systems respond to transformations driven by social media developments (Naeimi et al., 2022).

Within this context, Iran and Afghanistan, as two countries whose legal structures are influenced by Islamic law yet shaped by distinct social and political conditions, provide valuable experiences in addressing crimes influenced by social media. The rapid growth of social network usage in both countries, together with legal and institutional weaknesses and differences, has created significant challenges and ambiguities in criminal policy and criminalization practices in cyberspace. Therefore, a comparative examination of the role of social media in the formation of criminal behavior and its impact on criminalization processes in Iran and Afghanistan can contribute to a deeper understanding of this phenomenon and assist in proposing balanced and effective legal responses (Najafi, 2019; Nazem, 2017).

Accordingly, the present article, drawing upon criminological and criminal law foundations, explains the concept of social media and criminalization, analyzes the role and characteristics of these media in the emergence and transformation of criminal behaviors, and comparatively examines the legal frameworks and criminal policies of Iran and Afghanistan. The primary objective of the study is to clarify the dual nature of social media as both opportunity and threat and to provide a coherent understanding of the legal challenges and requirements associated with addressing cyberspace-related crimes within these two legal systems.

2. Conceptual Framework

2.1. *Concept of Social Media: Definition and Types*

Social media refers to online platforms that enable users to create content, share information, and interact with others. Owing to their capacity for instant sharing and direct communication with audiences, these platforms have become among the most popular forms of media and are widely used for marketing, advertising, and branding purposes (Atabi et al., 2021; Azadi et al., 2025).

Types of social media include social networking sites (such as Facebook and Twitter), image-sharing platforms (e.g., Instagram), video-sharing platforms (e.g., YouTube), and messaging applications (such as WhatsApp and Telegram) (Gholamhosseinnejad, 2020).

2.2. *Concept of Criminalization: Principles and Necessity of Criminalization in the Media Space*

Criminalization refers to the process through which specific acts are defined and recognized as crimes under a country's legal system. The fundamental principles of criminalization include the existence of a legal element, a material element, and a mental element within criminal conduct (Jafari Langroudi, 2024; Naeimi et al., 2022).

Within the media environment, social media may perform a dual role: they may serve as instruments for crime prevention while simultaneously functioning as spaces in which new crimes emerge or traditional behaviors transform into new criminal patterns (Hosseini & Raijan Asli, 2023).

2.3. *Criminal Behaviors Influenced by Social Media*

Criminal behaviors influenced by social media refer to actions shaped by online content, interactions, or structural characteristics of social media platforms. Such behaviors not only violate criminal laws but may also undermine cultural and religious norms (Gholamhosseinnejad, 2020).

By expanding access to information and communication, social media may facilitate the learning of criminal behaviors and contribute to the spread of cybercrimes such as fraud, defamation, and dissemination of false information (Ghaemi et al., 2024; Naeimi et al., 2022).

3. **The Role of Social Media in Criminalization and Criminal Behavior**

3.1. *The Role of Social Media in Criminalization and Criminal Behavior*

As online communication tools, social media exert both positive and negative influences on criminalization and criminal behavior. On the positive side, they may reduce crime through awareness-raising and preventive functions. Conversely, they may provide environments conducive to the commission of emerging crimes or the expansion of criminal conduct within societies (Hosseini & Raijan Asli, 2023; Panahi et al., 2020).

3.2. *Characteristics of Social Media and Their Influence on Identifying and Transforming Criminal Behavior*

Due to features such as easy access to information, rapid message dissemination, and extensive interaction networks, social media can significantly influence the transformation and expansion of criminal behavior. In many instances, these platforms promote harmful conduct such as spreading misinformation, inciting violence, and encouraging violations of legal norms (Ghaemi et al., 2024).

Moreover, social media may influence criminalization processes themselves, particularly when media platforms highlight certain behaviors and socially construct them as criminal acts, thereby shaping legislative and judicial responses (Panahi et al., 2020).

3.3. *The Impact of Social Media on the Formation of Emerging Criminal Behaviors and the Transformation of Traditional Crimes*

With the widespread use of social media, previously unknown criminal behaviors have emerged with increasing ease. Examples include online fraud schemes, hacking of personal data, and the unauthorized dissemination of private images (Naeimi et al., 2022; Ostadi & Ramezani, 2021).

By providing technological infrastructure and broad accessibility, social media have fundamentally transformed traditional criminal behaviors, accelerating their evolution into sophisticated cyber-enabled offenses (Najafi Tavana, 2020).

3.4. *The Impact of Social Media on Criminal Policy-Making and Legislation in Iran and Afghanistan*

Social media exert a direct influence on criminal policy-making and legislative processes in both Iran and Afghanistan. Through the creation of public pressure and rapid dissemination of information, these platforms increasingly affect legislative agendas related to the criminalization of certain behaviors. In Iran, social media frequently function as pressure mechanisms influencing judicial and legislative authorities to adopt new legal responses to cyberspace crimes (Ansari Mahyari et al., 2024; Yousefi et al., 2024).

In Afghanistan, social media likewise serve as tools for public awareness and crime prevention, although they may simultaneously contribute to the expansion of criminal behaviors within digital environments (Naghavi, 2021; Nazem, 2017).

4. **Theoretical Foundations and Theories**

4.1. *Criminological Theories Related to Social Media*

Social learning theory constitutes one of the most significant criminological frameworks explaining the influence of social media on criminal behavior. According to this theory, individuals—particularly young people—learn criminal behaviors through observation and imitation of others. Social media, functioning as extensive educational environments, may play a major role in transmitting such behavioral patterns. The theory emphasizes the influence of social environments and interpersonal interactions in learning social behavior and deviance (Hosseini & Rajan Asli, 2023; Maluku, 2020).

Cultivation theory (Gerbner) represents another important perspective emphasizing the role of media exposure in shaping individual attitudes and beliefs. Continuous exposure to media content—especially violent or crime-related material—may lead individuals to perceive social reality differently from actual conditions. Such distorted perceptions may increase fear of crime and promote acceptance of violence as a legitimate solution to social problems (Ghaemi et al., 2024).

Arousal theory suggests that violent and emotionally stimulating content disseminated through social media can elevate individuals' physiological and psychological arousal levels. Increased arousal may heighten the likelihood of impulsive or aggressive conduct. In other words, media content can influence internal psychological stimuli and potentially direct individuals toward criminal behavior (Naeimi et al., 2022).

Labeling theory further explains how social labels influence individual identity and behavior. When a person is labeled as a criminal, such labeling may reinforce deviant identity formation and increase the likelihood of continued criminal conduct. Social media, by amplifying and publicly framing certain behaviors as “criminal,” may intensify this labeling process and its criminogenic consequences (Najafi Tavana, 2020).

4.2. *Analysis of Legal Theories Related to Criminalization*

Utilitarian theory argues that criminalization should aim to maximize social benefit. Under this perspective, only behaviors whose prohibition produces greater social advantage than social cost should be criminalized. Social media, by facilitating widespread dissemination of information and public discourse, may influence social values and transform previously tolerated behaviors into acts perceived as criminal offenses (Ataghi et al., 2024; Naeimi et al., 2022).

The theory of criminal justice proportionality maintains that punishment must correspond to the severity of the committed offense. From this standpoint, social media contribute to shaping criminal policy by influencing societal perceptions of criminal conduct. Media discourse may redefine public attitudes toward behaviors formerly considered ordinary, thereby facilitating the emergence of new criminalization policies (Ghaemi et al., 2024).

Social control theory considers media as instruments of informal social regulation capable of preventing crime. By highlighting the negative consequences and social harms of criminal behavior, media platforms may deter individuals from engaging in unlawful activities. Through social media networks, such regulatory influence may contribute to legislative change and legal reform processes (Panahi et al., 2020).

4.3. *The Influence of Social Media on the Formation or Modification of Existing Laws*

Social media influence criminalization processes by reshaping public opinion and generating social pressure. Media platforms do not merely reflect public attitudes; they actively participate in constructing them. This influence operates primarily through two mechanisms: first, the creation of public pressure on legal systems to amend or enact new laws; and second, the transformation of social values and norms that may result in the criminalization of emerging behaviors or the redefinition of previously accepted conduct (Naeimi et al., 2022).

Particularly in developing countries, social media may intensify social demands for legislative reform or the adoption of new regulatory frameworks. This pressure often arises from the amplification of criminal phenomena such as online fraud, cyber theft, and digital defamation—offenses that previously received limited legal attention but have gained prominence through media visibility (Panahi et al., 2020).

5. **The Impact of Social Media on Criminal Behavior in Iran and Afghanistan**

In recent decades, social media have experienced substantial growth in both Iran and Afghanistan and have assumed a dual role in shaping social behavior. On the one hand, these platforms facilitate rapid access to information and public discourse, contributing to crime prevention and encouraging citizen participation in identifying criminal activities. On the other hand, dissemination of violent or misleading content may increase criminal motivation and intensify offenses such as online fraud, digital defamation, and virtual unrest. The expansion of cyberspace in both countries has therefore created not only opportunities for public awareness but also environments conducive to emerging forms of crime (Naghavi, 2021; Nazem, 2017).

Social media are user-centered digital communication systems that distribute textual, audio, and visual content rapidly and widely. Their defining characteristics include direct user interaction, removal of temporal and geographical limitations, creation of virtual communities, and mass dissemination of information. These features grant social media considerable power in shaping public opinion and facilitating communication while simultaneously enabling the rapid spread of rumors and criminal behavioral patterns (Atabi et al., 2021; Gholamhosseinejad, 2020).

Criminological and sociological theories have extensively analyzed the relationship between media exposure and criminal behavior. From the perspective of social learning theory, individuals may acquire deviant behaviors by observing violent imagery or criminal models presented through media platforms. Cultivation theory suggests that repeated exposure to violent media content may normalize violence and generate chronic fear of crime. Media desensitization perspectives argue that continuous exposure to violent imagery reduces emotional responsiveness toward crime and increases tolerance of violence. Media framing theory further demonstrates that media influence public perceptions by determining which crimes are highlighted and how society interprets offenders and victims, thereby indirectly shaping criminogenic social contexts. Functionalist and uses-and-gratifications perspectives also emphasize that audiences actively select media content for various purposes such as excitement, information acquisition, or escapism, complicating simplistic causal assumptions linking media directly to crime (Ghaemi et al., 2024; Hosseini & Raijan Asli, 2023; Maluku, 2020).

Beyond criminological perspectives, legal theories also clarify the foundations of criminalization. Utilitarian theory recommends criminalizing conduct only when doing so maximizes collective social welfare and promotes deterrence. Criminal justice theory emphasizes proportionality between crime and punishment and views punishment as a justified legal response to wrongdoing. These theoretical frameworks influence legal decision-making in both Iran and Afghanistan regarding which virtual behaviors should be classified as criminal offenses and support adaptation of legal systems to emerging cyberspace challenges (Ataghi et al., 2024; Naeimi et al., 2022).

5.1. *The Impact of Social Media on Criminal Behavior*

A) Social Media–Influenced Criminal Behaviors in Iran

In Iran, social media exert considerable influence on the formation of criminal behavior patterns. These behaviors include cybercrime, dissemination of false information, and offenses involving threats or insults in cyberspace. Criminal conduct in

Iranian law is defined through the presence of legal, material, and mental elements, and such behaviors are explicitly regulated within criminal legislation (Jafari Langroudi, 2024; Najafi Tavana, 2020).

Prominent offenses influenced by social media in Iran include:

Cybercrimes, such as hacking, data theft, and phishing activities, have significantly expanded alongside increased Internet and social media usage. These offenses are subject to strict criminal sanctions under cybercrime regulations (Ostadi & Ramezani, 2021).

Crimes against public morality also constitute a major concern. Social media platforms may facilitate the dissemination of inappropriate or obscene content, which has been criminalized under Iranian legal provisions addressing moral and cultural protection (Najafi Abrandabadi & Hashembeigi, 2021).

B) Social Media–Influenced Criminal Behaviors in Afghanistan

In Afghanistan, social media likewise play an important role in the emergence of criminal behavior. Activities influenced by these platforms include dissemination of misinformation, online threats, and participation in unlawful group activities. Despite complex political and social conditions, social media environments have increasingly become spaces in which certain crimes are committed (Nazem, 2017).

Cybercrimes are particularly prevalent, including the use of social media to spread destabilizing information or encourage violence. Such offenses are pursued under Afghan cybercrime and criminal regulations (Yousefi et al., 2024).

Crimes against national security also arise when opposition groups utilize social media platforms for propaganda or recruitment purposes. These activities are typically prosecuted under national security legislation and may carry severe penalties (Hatami & Rezaei, 2019).

5.2. Comparative Analysis of the Laws of Iran and Afghanistan

A) Differences in Criminalization in the Two Countries

In both Iran and Afghanistan, criminal law is influenced by Islamic Sharia. Nevertheless, there are differences in the manner of criminalization and the types and severity of punishments. In particular, Iran’s criminal laws are generally more codified and detailed than those of Afghanistan, whereas Afghanistan is more strongly affected by local legal practices and political shifts.

1. **Method of criminalization:** In Iran, legislation has more explicitly addressed the criminalization of unlawful conduct influenced by social media, whereas in Afghanistan these offenses are not classified with the same level of precision.
2. **Punishments:** In Iran, punishments for certain categories of offenses—such as drug-related crimes and sexual conduct offenses—tend to be stricter, while Afghanistan, particularly under Taliban governance, has more heavily emphasized social control and moral restrictions. (Nazem, 2017)

5.3. Similarities in Criminalization in the Two Countries

In both Iran and Afghanistan, many categories of crimes—such as offenses against national security, financial crimes, and offenses against persons—are broadly comparable. In addition, the penal laws of both countries are influenced by Islamic Sharia, and many sanctions for similar offenses are, in practice, comparable across the two systems.

1. **Security-related offenses:** In both countries, crimes against national and public security are criminalized, and severe penalties are prescribed for them.
2. **Financial crimes:** Theft, fraud, and embezzlement are treated as crimes in both countries, and punishments are предусмотрен for offenders. (Najafi Abrandabadi & Hashembeigi, 2021)

Considering the analysis of the impact of social media on criminal behavior in Iran and Afghanistan, it can be concluded that both countries face similar challenges in responding to these behaviors. At the same time, legal and social differences exist in how criminalization and punishment are designed and implemented in the two jurisdictions—differences that should be considered when formulating new social and legal policies.

Positive and negative functions: In Iran, experts acknowledge the dual role of media in criminalization. Social media, by informing the public about laws and the consequences of crime, can increase public participation and help strengthen social monitoring (for example, encouraging citizens to report offenses and contribute to prevention). However, these platforms may also facilitate criminal conduct: adolescents may develop delinquent motivations by imitating violent scenes or by exposure to the promotion of criminal lifestyles in networks; likewise, inaccurate or rumor-driven content in cyberspace can agitate public opinion and lead to social insecurity.

In Afghanistan, social media also have dual effects: on the one hand, they may enhance public legal awareness and disseminate crime-prevention strategies (for example, by publishing methods for preventing crime and reporting corruption), thereby strengthening public participation in security; on the other hand, the spread of misinformation, hate speech, and incitement to violence on networks can intensify social instability. Overall, social media in both countries function like a double-edged sword: through transparency and education they can contribute to crime reduction, yet when exploited by extremist groups or used for fabricating news, they can create conditions conducive to violent offenses.

User statistics and patterns of use: In Iran, research suggests that users are predominantly urban youth, and positive social, economic, and recreational functions are prominent in network use. According to official reports, the percentage of Iranian users participating in social networks has rapidly increased, and communication tools such as WhatsApp and Instagram are among the most visited platforms. In Afghanistan, especially over the past two decades—alongside the expansion of democratic governance and broader Internet access—a new “public discourse” has emerged, and social media have become key tools for strengthening social participation. However, in Afghanistan, social media users are also predominantly young, urban, and educated (with around 90% on Facebook), and cultural and security consequences of social media use remain a concern due to the presence of extremist groups.

Examples of influenced crimes: In both countries, examples of crimes influenced by social networks can be observed. For instance, common cybercrimes such as internet fraud, online defamation, dissemination of private videos or images, and disclosure of false information occur directly within environments that are inherently fueled by social media. In Iran, alongside the growth of social networks, reports have also pointed to offenses addressed under press/media regulations (such as insult, defamation, and dissemination of falsehoods) as well as offenses under cybercrime legislation. In Afghanistan, the spread of extremist content on social media contributes to recruiting terrorist supporters, and the dissemination of false news about political developments (for example, recycling fabricated narratives about the Taliban) can fuel public panic.

Relevant theories: Sociological theories indicate that media can introduce behavioral models to audiences. Under social learning theory, showcasing “successful” criminals or violent conduct on networks can facilitate delinquency. Script/planning approaches similarly suggest that media create behavioral scenarios in the minds of young users that may later be enacted in comparable real-world situations. Framing theory also shows that media, through the way they narrate crime news, can change public understandings of “victim” and “offender” and thereby shape anti-crime public policies. Additionally, legal theories such as utilitarianism and criminal justice/proportionality assist governments in defining the boundaries of criminalization (for example, criminalizing harmful media content) and in setting punishments designed to maximize prevention for society.

Laws and regulations (Iran and Afghanistan): In Iran, the legal framework for media-related crimes relies on the Computer Crimes Law (enacted in **2009**), the Press Law and media regulations (initially enacted in **1976**, with later amendments), and provisions of the Islamic Penal Code. The Iranian Press Law, by defining categories of prohibited content (insult, defamation, dissemination of falsehoods, and promotion of crime), indirectly contributes to preventing cyber offenses; for example, publishing an insulting post on a news website may constitute an offense both under press regulations and under the Computer Crimes Law. Licensing requirements and judicial oversight (including the press court mechanism) also provide forms of ex ante control. At the same time, the Constitution of Iran guarantees freedom of expression (Principle 25, **1979**) subject to compliance with Islamic standards, and media-related legislation has criminalized acts such as incitement to crime and threats to security.

In Afghanistan, the “Law on Media and Cyber Crimes” (**2017**) and the Afghan Penal Code (**2018**) constitute principal instruments for addressing online offenses. Afghanistan’s Mass Media Law (enacted in **2003**) also provides a broad definition of “media” and, in its relevant provisions, prohibits dissemination of prohibited content (such as disclosure of confidential documents, insult to sanctities and officials, and similar acts). In addition, Afghan criminal laws and media policies, beyond

specifying criminalized acts, establish punishments for disseminating inflammatory materials or content contrary to religious values.

Commonalities and differences: In both countries, dissemination of misleading information or incitement to violence is treated as criminal conduct. However, in Iran there is greater emphasis on freedom of expression (subject to Islamic constraints) and the existence of oversight institutions such as the Supreme Council of Cyberspace and the press court. Afghanistan, by contrast, following experiences of war and population displacement, has sought to define media crimes through religious regulations and doctrinal teachings; for example, “communication with extremist groups” in cyberspace has been framed as a crime with a specified punishment. These differences have resulted in shared criminalization of defamation and online threats, while Iran places greater emphasis on ethical regulation and protections related to journalism, and Afghanistan more frequently adopts a direct penal enforcement approach.

Overall, the evidence indicates that social media in Iran and Afghanistan constitute both an opportunity and a threat. On the one hand, through information dissemination and public participation they can contribute to crime reduction; on the other hand, violent or misleading content can intensify delinquency. Comparative findings suggest that both countries are rapidly enhancing their legal and oversight infrastructures, yet challenges remain—particularly the need to update laws quickly in response to technological change and to avoid overly expansive discretionary interpretations of criminality. Strengthening public media literacy and aligning domestic policies with international standards are among the proposals advanced in this study so that constructive use of media is facilitated while harms arising from cyber-enabled offenses are reduced.

6. Legal Solutions and Recommendations

The present study focuses on identifying and analyzing the legal mechanisms required to address the negative impacts of social media within the criminal justice systems of Iran and Afghanistan. At the international level, freedom of expression is recognized as a fundamental human right through which individuals may freely receive and disseminate information and ideas. Simultaneously, it has been acknowledged that this right may be subject to lawful limitations in order to protect public interests such as national security. Within this framework, international human rights jurisprudence emphasizes that free thought and the unrestricted circulation of information constitute essential foundations of democratic societies, while allowing proportionate restrictions when necessary to prevent crime or protect collective security (Fazeli & Karami, 2021; Zahidi & Sharifzadeh, 2021).

6.1. International Legal Solutions

A) Human Rights and Freedom of Expression

At the global level, human rights instruments such as the *Universal Declaration of Human Rights (1948)* and the *International Covenant on Civil and Political Rights (1966)* recognize freedom of expression as a fundamental right. These instruments, while emphasizing freedom of speech, also permit legally prescribed limitations when required to protect national security, public order, or the rights of others. International bodies—including human rights monitoring institutions—have stressed that regulation of cyberspace must remain consistent with freedom of expression principles and broader human rights standards (Monshipouri & Prompichai, 2019; Zahidi & Sharifzadeh, 2021).

B) International Instruments and Regulations

Numerous international organizations have been active in regulating cybercrime and social media governance. For example, international policy frameworks developed during the late twentieth century encouraged states to criminalize computer-related offenses and adopt coordinated responses to emerging technological risks. At the United Nations level, two parallel approaches have evolved regarding cybercrime regulation: one emphasizing state sovereignty and protection against foreign cyber operations, and another supporting expansion of cooperative international frameworks alongside human rights protections (Ansari Mahyari et al., 2024; Yousefi et al., 2024).

Among the most important international instruments is the *Budapest Convention on Cybercrime (2001)*, the first global treaty addressing cybercrime comprehensively. The Convention pursues three primary objectives: harmonization of criminal laws among member states, provision of effective investigative mechanisms, and strengthening of international cooperation. It

obliges states to criminalize acts such as hacking, computer fraud, data interference, and misuse of computer systems, while also requiring mutual assistance in investigations and judicial proceedings.

Specialized international institutions also play significant roles in strengthening cybersecurity capacity and international cooperation. Organizations such as the International Telecommunication Union contribute to standard-setting and technical coordination, while international policing networks facilitate information exchange and joint operations against cyber offenders (Kotanchi & Pourghahramani, 2021).

C) Data Protection and Privacy

One of the central pillars of combating cybercrime is ensuring the protection of personal data and privacy. Modern regulatory approaches increasingly emphasize data security obligations for governments and private technology companies alike. Contemporary data protection frameworks introduce concepts such as lawful data processing, privacy-by-design, and institutional accountability for technological platforms handling user information.

Under such standards, social media platforms that process users' personal data must implement technical safeguards—such as encryption and anonymization—and may incur legal liability in cases of privacy violations. Consequently, international cybersecurity standards provide benchmarks for evaluating states' commitments to data protection and preventing misuse of personal information in digital environments (Ghannad & Aligholi, 2020; Hesam et al., 2021).

D) Combating Terrorism and Extremism

The cyberization of terrorist activities represents a global security challenge. Since the beginning of the twenty-first century, the United Nations has adopted multiple counterterrorism resolutions obligating member states to combat terrorist financing and online extremist activities. These measures emphasize international cooperation in addressing digital radicalization, online recruitment, and dissemination of extremist propaganda.

United Nations legal frameworks underline that all states must actively cooperate against cyber-terrorism, as collective security mechanisms depend upon coordinated global responses. The binding authority of international security decisions further reinforces the obligation of states to prevent misuse of cyberspace for terrorist purposes (Hatami & Rezaei, 2019; Yousefi et al., 2024).

E) Responsibility of Social Media Platforms

In recent years, governments have increasingly adopted legislation imposing legal responsibility on social media platforms. Contemporary regulatory models require platforms to exercise greater transparency and accountability regarding user-generated content. Under these approaches, platforms are often treated as data controllers responsible for protecting users' information and removing unlawful content.

Accordingly, companies that fail to remove criminal content or that violate privacy obligations may face legal sanctions. At the same time, certain regulatory frameworks provide conditional immunity for platforms that do not participate in creating illegal content and that promptly remove unlawful material upon notification. These evolving international standards therefore expand platform accountability while simultaneously safeguarding their operational rights within lawful limits (Hesam et al., 2021).

6.2. International Cooperation

The level of legal and judicial cooperation among states constitutes a decisive factor in combating cybercrime effectively. A fundamental assumption underlying international cooperation is the need for shared definitions of computer crimes and harmonized criminalization standards. Without legal convergence, cross-border investigation and prosecution become significantly more difficult.

For this reason, international cybercrime frameworks emphasize the principle of **dual criminalization**, requiring states to recognize comparable offenses within their domestic legal systems. Cooperative mechanisms further oblige states to assist one another through rapid exchange of electronic evidence, mutual legal assistance procedures, and coordinated investigative measures.

Global experience demonstrates that effective responses to cybercrime depend upon legislative coordination, administrative cooperation, facilitation of extradition procedures, and timely sharing of digital evidence. Strengthening international

collaboration thus remains a central recommendation for Iran and Afghanistan in developing responsive and sustainable criminal justice strategies for cyberspace governance (Ansari Mahyari et al., 2024; Kotanchi & Pourghahramani, 2021).

6.3. Domestic Laws of Iran and Afghanistan

A) Iranian Laws and Their Impact on Reducing Social Media–Related Crimes

In Iran, several major laws directly or indirectly address cybercrimes and offenses arising from social media use. The most significant of these is the *Computer Crimes Law* enacted in **2009** (amended in **2024**), which criminalizes a wide range of cyber offenses. For instance, the law considers “unauthorized access” to computer systems, “illegal interception,” “computer espionage,” and “computer forgery” as criminal acts and prescribes penalties including imprisonment and monetary fines. The dissemination of obscene or unlawful online content is likewise prohibited and punishable. Overall, the Computer Crimes Law establishes a structured legal framework for combating cyber misuse by defining clear criminal categories and deterrent sanctions (Najafi, 2019; Ostadi & Ramezani, 2021).

The *Press and Media Law* (enacted in **1985**, with subsequent amendments) also plays an important preventive role in addressing media-related crimes. This law defines various forms of media, including electronic publications, and subjects media activities to licensing requirements and legal standards. According to the Press Law, publication of content contrary to public order—such as defamation, false accusations, dissemination of false information, and immoral material—is prohibited. Violating publications, including digital platforms, may face suspension of activity or judicial sanctions. Furthermore, the existence of specialized press courts and content monitoring mechanisms strengthens supervision over professional media standards. Collectively, preventive, supervisory, and cultural mechanisms embedded in the Press Law contribute to preventing irresponsible dissemination of information and public disturbance (Zahidi & Sharifzadeh, 2021).

Finally, the *Islamic Penal Code* (enacted in **2013**) explicitly criminalizes certain cyber-related offenses. For example, unauthorized access to information systems and illegal interception are recognized as criminal acts punishable by imprisonment or financial penalties. Through these provisions, the Islamic Penal Code extends traditional criminal law protections into cyberspace and provides judicial authorities with legal tools for prosecuting offenses committed through digital environments (Jafari Langroudi, 2024; Najafi Tavana, 2020).

B) Afghan Laws and Their Impact on Reducing Media-Related Crimes

In Afghanistan, important legislative measures have also been adopted to combat media-related crimes. The *Social Media and Cybercrime Law* adopted in **2014**, grounded in constitutional principles, provides a relatively precise definition of cyber offenses. The law pursues objectives such as safeguarding the information environment, ensuring cybersecurity, and enabling effective prosecution of cybercrime, while designating the Ministry of Communications and Information Technology as the principal authority responsible for implementation.

Additionally, the *Afghan Penal Code* includes dedicated provisions addressing cyber offenses, representing one of the first formal attempts to criminalize acts such as hacking, internet fraud, and digital misuse. These provisions created a clear legal basis for prosecuting cyber offenses that previously lacked explicit legal recognition. Consequently, Afghan criminal legislation has progressively integrated cybercrime regulation into its broader criminal justice system (Ansari Mahyari et al., 2024; Nazem, 2017).

6.4. Recommendations

Based on the foregoing analysis, the following recommendations may contribute to improving legal and supervisory frameworks addressing crimes arising from social media:

Development or updating of comprehensive legislation: Both Iran and Afghanistan should develop inclusive and updated cyber laws. Modern cyber offenses—including online threats, organized disinformation campaigns, unlawful disclosure of private data, and hate speech—should be clearly defined, and proportionate deterrent penalties established. Media platforms should also be required to cooperate with national legal authorities, provide transparency regarding harmful algorithmic practices, and promptly remove criminal content when identified (Ataghi et al., 2024).

Strengthening supervisory and judicial structures: The establishment of specialized institutions is essential. Each country should maintain advanced cyber police units staffed with trained experts in information technology and cybercrime investigation. Independent oversight bodies composed of representatives from government institutions, judicial authorities, and civil society could monitor online content regulation and provide legislative recommendations. Specialized training programs for judges, prosecutors, and lawyers in digital evidence and cybercrime adjudication are likewise necessary for effective law enforcement (Kotanchi & Pourghahramani, 2021).

Education, cultural development, and public participation: Media literacy education should be integrated into national educational systems so that citizens—particularly youth—can recognize criminal content and protect personal privacy. Engagement of religious and social leadership in promoting digital ethics and discouraging dissemination of harmful content is also recommended. Public reporting mechanisms, including online reporting systems and hotlines, may strengthen citizen participation in identifying criminal pages or activities. Academic and civil institutions can further contribute through research on crime prevention and dissemination of evidence-based preventive knowledge (Naghavi, 2021).

Technical and international measures: Utilizing emerging technologies such as artificial intelligence to identify harmful content within domestic platforms may accelerate removal of unlawful material. Establishing direct communication channels with international platform providers can facilitate faster responses to criminal activity. However, any technical monitoring must remain proportionate and must not undermine legitimate freedom of expression. Continued international cooperation, knowledge exchange, and participation in global cybersecurity initiatives remain essential for both countries (Yousefi et al., 2024).

Adoption of a national strategic framework: It is recommended that a comprehensive national strategic document be developed through coordination among all relevant institutions—including judicial authorities, law enforcement agencies, cultural ministries, and public media organizations. Such a framework should clearly define responsibilities, timelines, and implementation resources while maintaining a balance between security needs and protection of freedom of expression and privacy rights. Achieving this balance is crucial for public legitimacy and long-term policy effectiveness (Fazeli & Karami, 2021).

The conducted analyses demonstrate that effective responses to social media–related crimes require coordinated action at both international and domestic levels. Globally, participation in international agreements and strengthening judicial and intelligence cooperation are essential. Domestically, comprehensive legislation, effective platform supervision, and preventive mechanisms—such as media literacy education and legal protection of personal data—are indispensable. Implementation of the proposed measures, supported by existing legal resources and sustained international cooperation, can contribute significantly to preventing cyber and media crimes while safeguarding citizens’ security and fundamental rights in digital environments.

7. Conclusion

A comprehensive examination of the role of social media in the process of criminalization and the formation of criminal behavior demonstrates that these platforms, as structural and influential phenomena in contemporary societies, possess a dual function. On the one hand, social media—through providing rapid, interactive, and inclusive communication environments—play a significant role in enhancing legal awareness, strengthening social supervision, encouraging citizen participation in crime prevention, and facilitating public reporting mechanisms. On the other hand, these same characteristics may contribute to the facilitation of emerging crimes, expansion of criminal behavioral patterns, normalization of violence, and weakening of social and ethical norms. Accordingly, social media should not be regarded merely as tools of information transmission but as active agents influencing the evolution of the concept of crime, criminal conduct, and even criminal policy-making.

The findings of this study indicate that social media influence criminal attitudes and behaviors through mechanisms such as observational learning, cultivation of perceptions, emotional arousal, labeling processes, and media framing. Criminological theories effectively explain how repeated exposure to violent, deviant, or criminal content within social networks may lead to imitation of criminal behavior, reduction of moral sensitivity, and transformation of individuals’ perceptions of social reality. Alongside these perspectives, legal theories demonstrate that criminalization in media environments must be grounded in a

balance between social interests, proportionality between crime and punishment, and the necessity of effective prevention strategies.

The comparative analysis of Iran and Afghanistan reveals that, despite structural, political, and legal differences, both countries face similar challenges in addressing crimes influenced by social media. In Iran, the existence of relatively structured legal frameworks and specialized supervisory mechanisms has enabled a more coherent legal response, although challenges such as rapid technological change, expansive interpretation of criminal conduct, and tensions between freedom of expression and penal control remain unresolved. In Afghanistan, despite the adoption of legal measures addressing media and cybercrime, political instability, institutional limitations, and the instrumental use of social media by extremist groups have contributed to the transformation of digital environments into platforms for security-related offenses, dissemination of misinformation, and incitement to violence.

The results further demonstrate that criminalization of media-related conduct, when pursued without adherence to fundamental criminal law principles and without strengthening preventive approaches, may itself become a factor contributing to violations of citizens' rights, increased social distrust, and inefficiency in criminal policy. Exclusive reliance on punitive responses—without simultaneous investment in education, public awareness, and media literacy—cannot provide a sustainable solution for reducing cyberspace-related crime. The experiences of both Iran and Afghanistan indicate that where social media have been treated solely as threats, restrictive policies alone have failed to prevent the emergence of criminal behavior effectively.

Overall, social media in Iran and Afghanistan function as a “double-edged sword”: they possess substantial potential for crime prevention, transparency, and social participation, yet in the absence of intelligent policymaking, updated legal frameworks, and adequate media literacy, they may also facilitate the expansion of emerging crimes and intensify social harm. Consequently, adopting a balanced approach—one grounded in scientific criminological principles, criminal justice standards, and human rights considerations, combined with strengthened public education, institutional coordination, and adaptation of laws to technological developments—constitutes an unavoidable necessity for effective governance of media environments and reduction of their criminogenic consequences in both countries.

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

- Ansari Mahyari, A., Khalili Samani, K., & Pouladian, M. (2024). The Role of Governments and International Organizations in Combating Cybercrime. First National Conference on the Interaction of International Law and Domestic Law in the Development of Legislation, Gorgan.
- Atabi, N., Tabasi Lotfabadi, V., Sangsefidi, N., & Bahramzadeh, M. R. (2021). An Overview of the History and Structure of Social Media. *Journal of Modern Research in Entrepreneurial Management and Business Development*, 2(2), 8.
- Ataghi, A. G., Hosseini, S. H. D., Javan Jafari, A. R., & Jalal, M. T. (2024). Justification for Criminalizing the Dissemination of Misleading Information in Cyberspace in Light of Criminalization Criteria. *Journal of Criminal Law*, 15(1), 4.
- Azadi, R., Askarian, F., Abdavi, F., & Ghasemi, H. (2025). The Pattern of Social Media Impact on the Development of Sports Businesses.
- Fazeli, M., & Karami, M. (2021). Reflections on the Protection of the Right to Freedom of Expression in the Jurisprudence of the European Court of Human Rights Regarding Internet Access Blocking. *Specialized Journal of New Technologies Law*, 3(4), 173.

- Ghaemi, A. H., Peyvandpour, S., Andi, H., Gholami, S., & Gholami, S. (2024). An Analysis of Criminological Theories Regarding Cyberspace Crimes (Cyber). 10th International and National Conference on Management, Accounting, and Law, Tehran.
- Ghannad, F., & Aligholi, A. (2020). The Concept and Importance of Personal Data and Privacy and Types of Protection in Cyberspace. *Journal of Contract Law and New Technologies*, 1(1), 306.
- Gholamhosseinnejad, S. (2020). Social Media. *Media Studies Quarterly*, 21(50), 6.
- Hatami, A., & Rezaei, F. (2019). A Comparative Analysis of Funding Methods of Al-Qaeda and ISIS: An Approach in the Political Economy of Terrorism. *International Political Economy Studies*, 71.
- Hesam, A., Madibo Juni, M., Miri, H., & Yamarli, S. (2021). Civil Liability of Online Platforms Arising from Information Privacy Violations by Users: A Comparative Study in Iran, USA, and European Union. *Communication Research Quarterly*, 3(27), 74.
- Hosseini, S., & Rajjan Asli, M. (2023). Learning Criminal Behavior in Cyberspace. *Parliament and Strategy Quarterly*, 30(114), 3.
- Jafari Langroudi, M. J. (2024). *Legal Terminology* (39th ed., Vol. 3). Ganj-e Danesh Publications.
- Kotanchi, E., & Pourghahramani, B. (2021). The Role of the International Telecommunication Union in Establishing Cybersecurity. *Journal of Free Legal Research*, 14(53), 6.
- Maloku, M. (2020). Theory of Differential Association. *International Journal of Interdisciplinary Studies*, 9(1), 63. <https://doi.org/10.36941/ajis-2020-0015>
- Monshipouri, M., & Prompitchai, T. (2019). Digital Activism in Perspective: Palestinian Resistance Through Social Media. *Journal of International Studies*, 14(4), 58.
- Naeimi, R., Malmir, M., & Heidari, M. (2022). Principles and Criteria Governing Criminalization in the Iranian Legal System. *Quarterly Journal of Interdisciplinary Studies in Jurisprudence*(8), 12-13.
- Naghavi, S. M. (2021). The Role of Media in Crime Prevention with Emphasis on Afghanistan's Media. *Quarterly Journal*, 1(2), 23.
- Najafi Abrandabadi, A. H., & Hashembeigi, H. (2021). *Encyclopedia of Criminology* (5th ed.). Ganj-e Danesh Publishing.
- Najafi, H. (2019). *Iran's Legislative Criminal Policy Regarding the Production, Distribution, and Publication of Malware in Cyberspace in Light of the Budapest Convention* University of Kashan].
- Najafi Tavana, A. (2020). *Criminology* (22nd ed.). Avay-e Hekmat.
- Nazem, M. D. (2017). *Media Crimes in Afghanistan's Criminal Law*. Al-Mustafa International University, Hamed Resalat Press.
- Ostadi, F., & Ramezani, M. (2021). Investigating Cyber Destruction Crimes in Criminal Law and Judicial Practice. 9th International Conference on New Research Achievements in Jurisprudence, Law, and Humanities, Tehran.
- Panahi, H., Farasati, A., Mirzaei, M., & Karamzadeh, A. (2020). The Role of Media in Crime Prevention and Ensuring Security. *Social Order Quarterly*, 12(3), 76.
- Yousefi, J., Movassaghi, H., & Rahbar Farshpirah, N. (2024). United Nations Practice in Combating Cyber-Terrorism. *Comparative Research in Jurisprudence, Law, and Politics*, 6(4), 68. <https://doi.org/10.61838/csjpg.6.4.5>
- Zahidi, M., & Sharifzadeh, S. (2021). Freedom of Expression and the Principle of the Idea-Expression Dichotomy. *Public Law Research*, 23(71), 106.