A Comparative Study of the Criminal Liability of Service-Sharing Platforms for Crimes Committed by Users

1. Somayeh Ostadi: Department of Law, GKM.C., Islamic Azad University, Gonbadkavoos, Iran
2. Nafise Jalali*: Department of Law, Go.C., Islamic Azad University, Gorgan, Iran
3. Hosein Miri: Department of Law, GKM.C., Islamic Azad University, Gonbadkavoos, Iran

*****Correspondence: nafise.jalali@iau.ac.ir

Abstract

The expansion of service-sharing platforms, such as Snapp, Divar, and Aparat, has facilitated the emergence of novel forms of criminality whose attribution to digital intermediaries poses significant challenges from the perspective of traditional criminal law. This study aims to explain the scope, foundations, and conditions of platforms' criminal liability for crimes committed by users under the Iranian legal system and to compare them with the corresponding framework in the legal system of England. This qualitative study employed a descriptive-analytical method with a comparative approach. Data were collected through library-based research, including Iranian statutory laws—the Computer Crimes Act of 2009 and the Electronic Commerce Act of 2003—English legislation, including the Communications Act 2003, the Digital Economy Act 2017, and the Online Safety Act 2023, as well as judicial decisions, scholarly articles, and reputable theses published during the past ten years. The data were analyzed using deductive reasoning and qualitative content analysis. The findings indicated that, despite the recognition of the criminal liability of legal persons under the Iranian Islamic Penal Code of 2013, Iranian law lacks a coherent framework governing the criminal liability of platforms. Consequently, courts are compelled to rely on general principles, such as the rule of causation and the theory of negligent supervision. By contrast, English law, through the enactment of the Online Safety Act 2023, has established a comprehensive system based on a "duty of care," under which platforms are required to conduct regular risk assessments, prevent the dissemination of illegal content, and cooperate with the regulatory authority. Breach of these obligations may result in fines of up to £18 million or 10% of the platform's worldwide revenue. This study concludes that the Iranian legal system could draw upon the English model while preserving its Islamic jurisprudential foundations, including the rule of causation and the principle of no harm, to establish a "tiered liability" system based on the number of users and the level of risk. It is recommended that the Computer Crimes Act be amended to expressly establish preventive obligations for platforms.

Keywords: criminal liability, service-sharing platform, duty of care, comparative law

Received: 12 April 2026
Revised: 09 July 2026
Accepted: 23 July 2026
Initial Publication: 28 July 2026
Final Publication: 01 July 2027

Citation: Ostadi, S., Jalali, N., & Miri, H. (2027). A Comparative Study of the Criminal Liability of Service-Sharing Platforms for Crimes Committed by Users. *Legal Studies in Digital Age*, 6(4), 1-14.

1. Introduction

The digital revolution and the emergence of the platform economy have transformed traditional structures of economic and social interaction. Service-sharing platforms such as Snapp, Tapsi, Divar, Sheypoor, and Aparat, as well as social networks such as Instagram and Telegram, are no longer merely neutral technical intermediaries; rather, they have become active and influential actors in shaping user behavior (Khalilinejad & Barqei, 2024). Although this transformation has created unprecedented economic opportunities, it has also generated new challenges in the field of criminal law, particularly when users employ these platforms to commit offenses such as fraud, dissemination of criminal content, kidnapping, or transportation of prohibited substances.

The fundamental question is whether, under such circumstances, a platform may also be regarded as a "legal person" possessing independent criminal liability. If the answer is affirmative, what are the foundations, conditions, and limits of such liability? In the Iranian legal system, despite the significant growth of the digital economy and the enactment of legislation such as the Computer Crimes Act of 2009 and the Electronic Commerce Act of 2003, no precise and coherent framework has been developed for determining the criminal liability of platforms. This legislative gap has compelled courts to adopt broad interpretations of general principles such as the "criminal liability of legal persons" under Article 143 of the Islamic Penal Code of 2013, "negligent supervision," and the "rule of causation" (Mousavi Bojnourdi, 2019), resulting in inconsistent judicial practice.

By contrast, the legal system of England, as one of the leading jurisdictions in regulating cyberspace, underwent a major transformation through the enactment of the Online Safety Act 2023. This legislation, which was the product of years of debate and deliberation, established a comprehensive framework for platform accountability and introduced the concept of a "duty of care" as the cornerstone of the platform-liability regime (Ofcom, 2025).

The research background in Iran indicates that existing studies have primarily addressed the civil liability of platforms (Ashari, 2024) or comparative analysis with the law of the United States (Heydari Aghamiri Kandi, 2024). Few studies have undertaken an in-depth analysis of the foundations and conditions of platforms' criminal liability in light of recent developments in English law, particularly the Online Safety Act 2023, while also seeking to adapt those developments to the Iranian legal context. The specific research gap addressed in this study is the absence of a domestic model consistent with the jurisprudential foundations and legal structure of Iran for determining the criminal liability of platforms.

The principal objective of this study is to explain the scope and foundations of the criminal liability of service-sharing platforms for crimes committed by users and to propose a domestically adapted model drawing on the experience of the English legal system.

2. Literature Review

2.1. *The Concept and Nature of Service-Sharing Platforms*

Service-sharing platforms refer to digital systems that provide an environment for interaction between providers and recipients of services. The distinguishing characteristic of these platforms is their role as "active intermediaries," meaning that they not only facilitate communication but also influence the quality and quantity of interactions through algorithms, rating systems, and verification mechanisms (Khalilinejad & Barqei, 2024).

From a legal perspective, the most important issue concerning the nature of platforms is whether they should be classified as a "mere conduit" or an "active publisher." Under traditional law, mere intermediaries were generally exempt from liability for user-generated content. However, this approach has been reconsidered in relation to modern platforms that commercially exploit user data (Fallah, 2021).

2.2. *Foundations of Criminal Liability under Iranian Law*

Criminal liability is an essential institution in every criminal justice system. The declaration of conduct as criminal and the prescription of punishment may, at most, contribute to the regulation of criminal prosecution and sentencing; however, the prosecution and punishment of offenders are impossible unless each individual possesses the capacity to be blamed and held criminally responsible. Criminal liability arising from the act of another exists where a person may be punished for another individual's criminal conduct despite having neither participated in nor assisted the commission of the offense and despite possibly having been unaware of its occurrence. Such a person is punished solely because of a particular status or position. Most instances discussed under this heading in Iranian legal writings and studies arise from a legal relationship involving fault or negligence in the performance of a duty and, therefore, cannot necessarily be regarded as examples of this principle. This does not, however, mean that the principle is absent from Iranian judicial practice. For example, where supporters of a football team cause disorder during a match and the team is subsequently deprived of spectators for one or more future matches, or where a shop is sealed and its owner punished because an employee engaged in overpricing despite the owner having observed all legal and ethical requirements in hiring the employee, such cases constitute clear examples of criminal liability arising from the act of another (Salahi, 2001). Under Iranian law, the criminal liability of service-sharing platforms for crimes committed by users is rooted in three areas: the general rules governing the criminal liability of legal persons, jurisprudential rules, and the three constituent elements of an offense. Although the Islamic Penal Code of 2013 represented an important step toward recognizing the criminal liability of legal persons, its provisions primarily concern offenses committed by the legal representative of the legal person and leave a significant gap regarding liability arising from the acts of users as third parties. By contrast, jurisprudential rules such as causation and the principle of no harm possess considerable capacity to establish a basis for the indirect liability of platforms. Nevertheless, the imposition of criminal liability in practice requires the simultaneous establishment of the legal, material, and mental elements of the offense. Under the current legal framework, the most important obstacle is the absence of precise criminalization of platform omissions in Iranian statutory law (Ardabili, 2020; Mirmohammad Sadeghi, 2020).

2.2.1. Criminal Liability of Legal Persons

The Islamic Penal Code of 2013 addressed the criminal liability of legal persons systematically for the first time. Article 143 provides that "legal persons, with the exception of the State and its affiliated institutions, may be prosecuted and punished where the legal representative of the legal person commits an offense in its name or on its behalf" (Mirmohammad Sadeghi, 2020). Nevertheless, this provision primarily focuses on offenses committed by the legal representative of the legal person, such as the chief executive officer or members of the board of directors, and does not expressly address circumstances in which an offense is committed through the platform by users as third parties.

In addition to Article 143, Articles 144 to 146 of the Islamic Penal Code elaborate on exemptions from, mitigation of, and aggravation of penalties imposed on legal persons. Article 144 exempts a legal person from liability where it is established that the legal person adopted the necessary measures to prevent the offense or reported it to the judicial authorities. This provision may provide the basis for an "effective defense" by platforms. In other words, where a platform demonstrates that it maintained a transparent and effective monitoring system for identifying and removing criminal content, it may qualify for exemption from criminal liability. Under this interpretation, Article 144 effectively incentivizes platforms to design preventive mechanisms. Nevertheless, Iranian judicial practice has not yet substantially addressed this issue, and it remains unclear what level of monitoring courts would regard as "sufficient" (Fallah, 2021; Mohammadnejad, 2022).

Another point is that Articles 11 to 13 of the Electronic Commerce Act of 2003, as amended in 2022, contain specific provisions on the liability of intermediaries, including platforms. However, these provisions concern civil liability arising from infringements of intellectual property rights and commercial data and do not apply to criminal offenses such as fraud, dissemination of falsehoods, or insult. Consequently, under current Iranian law, a service-sharing platform will be criminally liable for the criminal acts of its users only where the conduct of its legal representative, such as the chief executive officer, directly constitutes complicity or participation in the offense under Article 126 of the Islamic Penal Code, rather than merely because the platform provided the communicative infrastructure (Saffari, 2016).

2.2.2. Relevant Jurisprudential Rules

Under Imami jurisprudence, two principal rules may be invoked as foundations for indirect liability:

The rule of causation: Under this rule, "any person who causes the destruction of another person's property or injury to another person's life is liable" (Mousavi Bojnourdi, 2019). This rule also encompasses indirect conduct and requires the existence of a customary causal relationship between the person's conduct and the harmful result. In the context of platforms, it may be argued that where a platform facilitates the commission of an offense by providing a communicative environment or by failing to exercise sufficient supervision, it falls within the scope of the rule of causation.

The rule of causation possesses considerable theoretical capacity to impose liability on platforms, but its practical application encounters two obstacles. The first is establishing a customary causal relationship between "providing the infrastructure" and "the occurrence of a specific offense." Under Islamic jurisprudence, where the cause is regarded as "unusual" or "weak," liability does not arise. The court must determine whether the platform merely provided a neutral instrument or whether, through the design of incentive-generating algorithms, such as automatic recommendations of similar content or increased financial returns for fraudulent advertisements, it played an "effective customary role" in the formation of the offense. The second obstacle is that the rule of causation has primarily been applied in Islamic jurisprudence to civil liability, including blood money and financial compensation. Extending it to criminal liability involving fixed and discretionary punishments requires considerable caution. Some jurists maintain that the rule may be used in relation to discretionary punishments as a source of secondary rulings, provided that the principle of legality of crimes and punishments is observed (Mousavi Bojnourdi, 2019; Sanei, 2013).

The principle of no harm: This rule, which signifies the negation of all forms of harm in Islam, may serve as a basis for imposing preventive duties on platforms (Sanei, 2013). Accordingly, platforms are required to adopt measures ensuring that users are not harmed through their services.

The principle of no harm has been interpreted in Islamic jurisprudence both negatively, as negating harm, and positively, as requiring the prevention of harm to others. In its positive dimension, it may support the derivation of a legal-religious obligation to "monitor and exercise care" over public environments susceptible to criminal misuse. Considered together with the rule that "a prerequisite leading to what is forbidden is itself forbidden," this obligation requires platforms to modify the design of their systems so that they do not facilitate criminal conduct. The important challenge, however, is that the principle of no harm does not independently prescribe criminal punishment. Transforming a religious duty into a criminal sanction requires criminalization through ordinary legislation. Therefore, jurisprudential rules principally serve to "justify the foundations" and "interpret existing legislation" and cannot replace an express statutory provision in criminal proceedings (Ardabili, 2020; Fallah, 2021).

2.2.3. The Three Elements of an Offense in Platform Liability

The establishment of the criminal liability of platforms requires proof of three elements:

The legal element: There must be a law declaring the platform's conduct to be criminal. At present, the Computer Crimes Act and the Electronic Commerce Act are primarily focused on civil liability and do not precisely criminalize omissions by platforms (Mohammadnejad, 2022).

The legal element, as the most important principle of criminal law, namely the principle of legality of crimes and punishments, is recognized in Article 2 of the Islamic Penal Code. Although scattered provisions apply to platforms, none specifically define "failure by a platform to exercise effective supervision over user-generated content" as an independent offense. Articles 16 to 20 of the Computer Crimes Act of 2009, as amended in 2017, address offenses such as unauthorized access, unlawful interception, and computer espionage. These offenses, however, concern direct conduct by users or platforms and do not encompass "failure to remove criminal content." Article 21 of the Computer Crimes Act requires administrators of computer systems to cooperate with judicial authorities in the detection of offenses, but omission in this regard is treated merely as a disciplinary or administrative violation and carries no criminal penalty. Thus, the principal gap in Iranian law is the absence of an offense of "organized omission by a platform in response to criminal user-generated content" (Fallah, 2021; Parhizkar, 2014).

The material element: The platform's criminal conduct may take the form of an act, such as approving a fraudulent advertisement, or an omission, such as failing to remove illegal content despite having knowledge of it.

The material element of platform liability is complicated by the difficulty of determining whether the conduct constitutes an act or an omission. From the perspective of criminal law, where a platform designs its system so that automated processes or algorithms approve or promote user-generated content without human intervention, this phenomenon may be characterized as an "indirect act" attributable to the legal person in the same manner as direct conduct. However, where the platform merely provides a neutral environment and fails to remove illegal content, the criminal conduct takes the form of an omission. Under Iranian law, an omission constitutes an offense only where the law specifically imposes a duty to perform the omitted act, as reflected in Article 294 of the Islamic Penal Code concerning omissions resulting in death or destruction. No such general statutory duty exists for platforms. Article 22 of the Executive Regulation of the Computer Crimes Act of 2012 merely requires system administrators, as an administrative and organizational matter, to "remove criminal content following notification by judicial authorities." Consequently, before formal notification, a platform's omission lacks a criminal character (Mirmohammad Sadeghi, 2020; Saffari, 2016).

The mental element: Knowledge by the platform of users' criminal conduct, or the reasonable foreseeability of that conduct under ordinary circumstances as a form of criminal fault, is an essential condition for attributing the offense to the platform (Ardabili, 2020).

The mental element is considerably more complex for platforms than for natural persons. First, the issue of the "knowledge of a legal person" arises. Can the cumulative awareness of employees, algorithms, and records of user reports be treated as "collective knowledge"? Under Iranian legal doctrine, Article 143 of the Islamic Penal Code refers to the "legal representative," meaning that the knowledge of the chief executive officer is regarded as the knowledge of the legal person. However, where an offense is committed by ordinary users and the chief executive officer remains unaware, can an automated violation-notification algorithm substitute for human knowledge? Some scholars maintain that where an "automated notification system" has been properly designed and activated, it may be regarded as constituting the knowledge of the legal person, and failure to act following such a warning may amount to constructive knowledge and intentional omission (Mohammadnejad, 2022). Second, criminal fault in the Iranian system takes two forms: intentional fault involving criminal intent and unintentional fault involving carelessness, negligence, lack of skill, or failure to comply with governmental regulations. Platforms are most commonly prosecutable on the basis of unintentional fault. Where a platform fails to improve its monitoring system despite repeated user warnings or a high rate of similar offenses, its conduct may be characterized as "criminal negligence." Proving such negligence in court is nevertheless difficult because the platform may claim that it complied with minimum standards (Ardabili, 2020; Parhizkar, 2014).

2.3. The English Legal System: From Common Law to the Online Safety Act 2023

The English legal system has undergone a significant transformation in relation to platform liability. Under early judicial practice, intermediaries were generally not liable, reflecting the principle of neutrality. From the beginning of the 2020s, however, the concept of a "duty of care" gradually entered legal discourse.

The development of English law has passed through three principal stages:

The first stage, from 1990 to 2000: Under the influence of the Copyright, Designs and Patents Act 1988 and the European Union Electronic Commerce Directive 2000/31/EC, platforms were exempt from liability for user-generated content under the "safe harbor" exemption unless they possessed actual knowledge of illegal content and failed to act within a reasonable period.

The second stage, from 2010 to 2020: With the proliferation of terrorist content and child sexual abuse material, the English Parliament enacted the Digital Economy Act 2017, requiring platforms to engage in "transparent reporting" and remove specified content, while designating Ofcom, the communications regulator, to supervise compliance.

The third stage, from 2023 onward: The legal framework shifted from liability based on "knowledge and subsequent removal" toward responsibility based on "safety by design," centered on the Online Safety Act 2023.

The Communications Act 2003 constituted the first step toward regulating criminal content on digital platforms and principally focused on broadcasting and harmful content.

Section 127 of the Act introduced the offense of "sending a threatening, indecent, or grossly offensive message through a public communications network." Although this provision applied to the individual sender, courts subsequently considered whether the hosting platform could also be liable merely because it had provided the infrastructure. In *Director of Public*

Prosecutions v. Collins [2006] EWHC 3086 (Admin), the court held that a platform would not be liable unless it possessed actual knowledge of the criminal content. This approach was subsequently altered by the Online Safety Act (Sobel, 2021).

The Digital Economy Act 2017 represented an important step toward requiring platforms to remove illegal content, particularly child sexual abuse material (Sobel, 2021).

Sections 88 to 95 of the Act required Ofcom to establish a mandatory notice-and-takedown system for child sexual abuse material. Platforms were required to remove the content within 48 hours of receiving a valid notice, failing which they could be fined up to £250,000 or 4% of their worldwide revenue. Although the Act was transformative, it suffered from several deficiencies. First, it applied only to one particular category of offense, namely child sexual abuse material. Second, it did not provide for criminal sanctions involving imprisonment of platform executives. Third, ordinary users could not bring a direct complaint against a platform merely because criminal content directed against them, such as insults or threats, remained accessible (Ofcom, 2025).

The turning point, however, was the Online Safety Act 2023. Enacted in October 2023 and progressively brought into force beginning in March 2025, the Act established a comprehensive and integrated regulatory system for user-facing platforms (Ofcom, 2025).

The key features of the Online Safety Act 2023 are as follows:

1. Scope of application: All user-to-user services and search engines providing services to users in England fall within the scope of the Act under Section 3.
2. Core duties:

Duty of care: Platforms must regularly assess the risk of “illegal content” and “legal but harmful content” and adopt proportionate measures to mitigate those risks under Section 10.

Child-safety duty: Platforms are required to protect minors against harmful content, including material promoting self-harm or anorexia nervosa, under Section 12.

Transparency duty: Platforms must publish annual reports on their risk-management practices and content-removal statistics under Section 60.

3. Enforcement mechanisms: Ofcom is authorized to impose fines of up to £18 million or 10% of the platform’s worldwide revenue, whichever is greater. In cases involving repeated and serious violations, senior platform executives may be sentenced by a court to up to two years’ imprisonment under Section 124.
4. Relevance to the subject of this study, namely liability for crimes committed by users: Unlike Iranian law, which remains largely confined to general rules, the Online Safety Act 2023 expressly provides that a platform may be independently prosecuted for failing to remove illegal user-generated content, even where its executives lacked personal knowledge of that content, provided that its automated notification systems were designed in such a manner that they should reasonably have identified it under Section 50. This approach corresponds to concepts of “organizational fault” and “systemic negligence,” which have not yet been incorporated into Iranian legislation (Ofcom, 2025).

2.4. Research Gap

A systematic review of the literature published between 2019 and 2024 reveals the following principal research gaps:

1. The absence of an in-depth comparative analysis between the jurisprudential foundations of indirect liability under Iranian law and the concept of the “duty of care” under English law;
2. Insufficient attention in Iranian studies to recent developments in English law, particularly the Online Safety Act 2023 and Ofcom’s enforcement practice;
3. The absence of a domestic and operational model for determining the criminal liability of platforms under Iranian law that is compatible with jurisprudential principles and statutory legislation.

The present study seeks to address these gaps.

3. Methodology

This research is a qualitative descriptive-analytical study employing a comparative approach. The comparative model used is "issue-oriented comparative analysis," which focuses on comparing similar concepts, institutions, and rules across two legal systems.

3.1. Population and Sample

The research population comprised all legal sources relevant to the criminal liability of platforms under the Iranian and English legal systems. The inclusion criteria were as follows:

- Statutory laws and regulations enacted from 2001 onward in Iran and from 2003 onward in England;
- Published judicial decisions and enforcement practices issued from 2015 onward;
- Reputable peer-reviewed scholarly articles published between 2015 and 2025;
- Specialized books and relevant theses.

Ultimately, 22 Persian-language sources and 15 English-language sources were purposively selected and analyzed.

3.2. Data-Collection and Data-Analysis Methods

The data were collected through library and documentary research using a systematic note-taking instrument. Data analysis was conducted in two stages:

The first stage involved descriptive and inferential analysis of concepts and rules under Iranian law.

The second stage involved comparative analysis with English law through the examination of similarities, differences, and the feasibility of legal transplantation.

4. Findings and Discussion

The findings of this study are presented in two distinct but interconnected sections. The first concerns Iranian law, and the second addresses the English legal system. In each section, the existing legal position is described, the strengths and deficiencies of each legal system are analyzed, and the feasibility of adopting successful approaches is subsequently discussed.

4.1. Findings Concerning Iranian Law

Despite the progress made in recent years in the field of computer-related offenses, the Iranian legal system continues to face significant structural gaps concerning the criminal liability of service-sharing platforms for crimes committed by users. These gaps are evident both at the legislative level and in judicial practice and statutory interpretation.

4.1.1. Existing Legislative Framework

An examination of Iranian statutory law indicates the existence of fragmented and incoherent provisions concerning platform liability, which are discussed below.

The Electronic Commerce Act of 2003: Article 58 recognizes the liability of an "intermediary" only where it performs a role beyond the mere transmission of data (Saffari, 2016). This provision primarily concerns civil liability.

Article 58 of the Electronic Commerce Act of 2003, together with its subsequent amendments, constitutes one of the earliest legislative attempts to regulate the liability of online intermediaries in Iran. It provides that "a hosting service provider that performs a role other than the storage of data falls outside the scope of the exemption from liability." In other words, the Iranian legislature has partially accepted the "safe harbor" model: as long as a platform does not play an active role in creating or editing user-generated content, it is exempt from civil liability. Nevertheless, this provision suffers from fundamental ambiguity. First, the phrase "a role beyond the transmission of data" is undefined. It is therefore unclear whether a content-recommendation algorithm constitutes such an additional role. Second, the provision applies only to civil liability involving compensation for damage and is unrelated to the criminal prosecution of platforms. Consequently, where a user commits fraud or disseminates falsehoods through a platform, a criminal court cannot directly invoke Article 58 to hold the platform criminally liable. This gap is particularly evident in cases involving peer-to-peer platforms such as Snapp and Divar, through which users may commit fraud or transfer smuggled goods (Fallah, 2021; Mohammadnejad, 2022).

The Computer Crimes Act of 2009: Articles 10 to 23 address offenses against public morality and decency in cyberspace and prescribe penalties for “website administrators” who fail to remove criminal content (Mirmohammad Sadeghi, 2020). However, the Act does not provide a precise definition of a “website administrator” or specify the conditions for attributing an offense to such a person.

The Computer Crimes Act of 2009 may be regarded as the principal criminal statute governing cyberspace in Iran. Nevertheless, its approach to platforms suffers from a form of “conceptual disorder.” On the one hand, Article 16 criminalizes “unauthorized access to computer systems,” an offense primarily directed at ordinary users. On the other hand, Article 21 requires system administrators to cooperate with judicial authorities in the “detection of offenses” and the “preservation of evidence,” but does not define failure to cooperate as an independent offense, instead treating it as a disciplinary violation. The most significant provision regarding platform liability is Article 22 of the Computer Crimes Act, as amended in 2017, which provides that “where criminal content exists within a computer system or cyberspace, the owner or administrator of the system is required, after becoming aware of the existence of such content, to remove it.” The central question is how such “awareness” or knowledge is to be established. Is the personal knowledge of the chief executive officer required, or is awareness generated through an automated system sufficient? In practice, platforms operate automated notification mechanisms, such as “report content” buttons. However, where an automated report is merely recorded on a server and is not communicated to senior management, does it constitute the knowledge of those managers? Iranian judicial practice is almost entirely silent on this issue. In a limited number of decisions, some branches of the Tehran Computer Crimes Prosecutor’s Office have rejected automated-system awareness as sufficient and have required “actual and proven knowledge of the natural person acting as manager” as a condition of criminal liability, thereby effectively exempting large platforms from liability (Mirmohammad Sadeghi, 2020; Parhizkar, 2014).

Generally, it may be stated that current Iranian law does not recognize an independent offense entitled “platform liability for user-generated content.” Instead, platform liability arises under the following legal classifications:

- Failure to comply with an order of the Committee for Determining Instances of Criminal Content or a judicial authority concerning criminal content;
- Carelessness or negligence in facilitating access to criminal content;
- Failure to comply with the statutory duty to retain traffic data and user information within legally prescribed periods;
- Failure to notify the Committee for Determining Instances of Criminal Content upon becoming aware of criminal content.

The most important express provision in this regard is Article 751 of the Computer Crimes Act of 2009, which provides:

“Hosting service providers shall, immediately upon receipt of an order from the Committee for Determining Instances of Criminal Content referred to in the preceding article or from the judicial authority hearing the case concerning the existence of criminal content in their computer systems, prevent continued access to that content. Where they intentionally refuse to comply with the order of the Committee or the judicial authority, they shall be dissolved. Otherwise, where they facilitate access to the relevant criminal content through carelessness or negligence, they shall, for the first offense, be sentenced to a fine ranging from IRR 20,000,000 to IRR 100,000,000; for the second offense, to a fine ranging from IRR 100,000,000 to IRR 1,000,000,000; and for the third offense, to temporary closure for a period of one to three years.”

The fines prescribed in this provision were adjusted pursuant to the Council of Ministers’ resolution of March 15, 2021. Under the first category, the fine was increased to between IRR 60,000,000 and IRR 250,000,000, while the second category remained unchanged under the existing legal framework.

“Note: Hosting service providers shall, immediately upon becoming aware of the existence of criminal content, report the matter to the Committee for Determining Instances of Criminal Content.”

Accordingly, the related offenses or violations may analytically be classified as follows:

- Intentional refusal to comply with an order of the Committee or a judicial authority concerning the removal or blocking of criminal content, resulting in dissolution;

- Carelessness or negligence in preventing access to criminal content, resulting in fines and temporary closure;
- Failure to comply with the duty to report immediately upon becoming aware of criminal content.

The Regulation of the Communications Regulatory Commission of 2021: This regulation, developed for messaging platforms, imposes duties such as "identification of users" and "removal of criminal content within a maximum period of 24 hours," but does not establish a specific criminal sanction.

The Regulation on the Organization of Social-Messaging Platforms, adopted by the Communications Regulatory Commission in 2021 and sometimes referred to as the "Organization Regulation," is the first Iranian instrument of its kind to subject both foreign messaging platforms, such as Telegram, WhatsApp, and Signal, and domestic platforms, such as Eitaa, Soroush, and Bale, to stringent requirements. Its principal obligations include the following:

Identification and verification of users under Article 4: Platforms must collect users' identity information and compare it with governmental databases.

Removal of criminal content within a maximum period of 24 hours after notification under Article 8: This period is stricter than international standards, which commonly range from 48 to 72 hours.

Retention of communications logs for six months under Article 12.

The fundamental problem, however, is that the regulation does not establish an "independent criminal sanction." Article 20 merely refers to "reporting the violation to judicial or disciplinary authorities" without specifying a minimum penalty or defining the nature of the offense. Consequently, a criminal court cannot directly rely on the regulation to impose imprisonment or a fine on a manager who fails to remove criminal content within 24 hours unless the conduct is criminalized under another statute, such as the Computer Crimes Act or the Islamic Penal Code. The regulation should therefore be regarded as a "duty-imposing instrument" supported by administrative sanctions, such as regulatory fines, rather than as criminal legislation in the strict sense (Ardabili, 2020; Saffari, 2016).

Generally, Iranian legislation concerning the criminal liability of platforms may be divided into three categories:

The first category comprises laws adopting a civil or non-criminal approach, such as the Electronic Commerce Act of 2003, which recognizes intermediary exemptions only in civil actions and contains no provision governing the criminal liability of platforms. Its strength lies in recognizing the concept of an "intermediary" under Iranian law, whereas its principal weakness is its failure to cover criminal offenses and its ambiguous definition of a "role beyond the transmission of data."

The second category comprises laws adopting a limited and case-specific criminal approach, such as the Computer Crimes Act of 2009, which prescribes penalties for "website administrators" who fail to remove criminal content involving offenses against public morality and decency, primarily in the form of fines and imprisonment for up to 91 days. Its strength is that it criminalizes certain omissions by administrators. Its principal weaknesses, however, are the absence of a precise definition of "platform"—because many service-sharing platforms, including transportation and delivery platforms, may not fall within the concepts of a "website" or "website administrator"—and the failure to establish attribution standards appropriate to the algorithmic era.

The third category comprises subordinate regulations and directives lacking independent criminal sanctions, such as the Regulation on the Organization of Messaging Platforms of 2021. Although this regulation imposes clear and sometimes stringent duties on platforms, it does not prescribe independent criminal penalties for their breach and is confined to administrative and disciplinary violations. Its strength is the creation of certain preventive duties, including monitoring, identity verification, and timely removal. Its principal weakness is the absence of any effective criminal sanction, such as imprisonment or a substantial fine.

Taken together, these three categories demonstrate that the Iranian legal system lacks a unified and specialized statute entitled "Criminal Liability of Platforms for Crimes Committed by Users." The most significant gap is the absence of an independent offense of "failure to exercise effective supervision and remove criminal content" applicable to all platforms, including commercial, service-based, peer-to-peer, and social-network platforms. As a result, in many important cases, such as fraud through an online marketplace or the dissemination of falsehoods through domestic social networks, judicial authorities must resort to the general rules of complicity under Article 126 of the Islamic Penal Code or the jurisprudential rule of causation. Both approaches are difficult and time-consuming to establish (Fallah, 2021; Mohammadnejad, 2022).

4.1.2. Iranian Judicial Practice

Because of the legislative gap, Iranian judicial practice concerning the criminal liability of platforms is inconsistent. An examination of several judgments issued by courts in Tehran and Mashhad between 2020 and 2023 indicates the existence of two principal approaches:

The first, maximalist approach: Some courts, relying on the rule of causation and Article 143 of the Islamic Penal Code, have held platforms liable where they possessed “knowledge of users’ offenses and failed to take preventive measures.” In a 2021 judgment of Branch 105 of the Tehran Criminal Court concerning fraudulent advertisements on an online advertising platform, the platform manager was convicted of “facilitating the commission of an offense” (Parhizkar, 2014).

The second, minimalist approach: By contrast, some courts, relying on the principle of the personal nature of punishment and the absence of an express statutory provision, have rejected platform liability and have regarded only the offending user as prosecutable.

This inconsistency in judicial practice demonstrates the need for clear legislation.

4.1.3. Analysis of the Elements of Criminal Liability under Iranian Law

Using the general framework of criminal law, the following conditions may be proposed for establishing the criminal liability of platforms:

- Legal element: Article 143 of the Islamic Penal Code of 2013 may be invoked as the general basis for the liability of legal persons. However, applying it to platforms as “digital intermediaries” requires a broad interpretation of the concept of the “legal representative” (Nurbaha, 2019).
- Material element: Two principal forms of criminal conduct may be identified. The first is a positive act, such as approving a fraudulent advertisement or publishing criminal content through platform employees. The second is an omission, such as failing to remove criminal content despite formal notification and knowledge of its existence.
- Mental element: The platform must possess “knowledge and awareness” of the criminal nature of the users’ conduct. Courts generally establish platform knowledge through “customary indicators,” such as the number of user reports or the manifestly criminal nature of the content (Ardabili, 2020).

4.2. Findings Concerning English Law

Under English law, the Online Safety Act 2023 constitutes a comprehensive and pioneering framework that has shifted platform liability from traditional content moderation toward “preventive duties based on risk assessment.” The findings of this section indicate that the English approach, through its emphasis on breaches of independent statutory obligations, including risk assessment and cooperation with the regulator, together with the imposition of substantial fines, presents a new model of criminal liability based on “structured supervision.” This model has been implemented in enforcement proceedings involving Im.ge, X, and Telegram.

4.2.1. Structure and Key Provisions of the Online Safety Act 2023

The United Kingdom’s Online Safety Act 2023, or OSA 2023, is comprehensive legislation containing more than 300 sections and applying to user-to-user services and search engines. Its most important provisions are as follows:

Duty of care: Sections 9 to 12 require platforms to implement “proportionate systems and processes” to identify, mitigate, and manage the risks posed by priority illegal content and content harmful to children (Ofcom, 2025).

Risk assessment: Regulated platforms must periodically assess and document the risk that users will encounter illegal content. The first deadline for completing an illegal-content risk assessment was March 16, 2025 (Ofcom, 2025).

Priority offenses: The Act identifies a list of priority offenses, including child sexual abuse, terrorism, fraud, and encouragement of suicide, which platforms are required to prevent. Section 184 establishes the independent offense of “encouraging or assisting suicide” (Eventum, 2025).

Role of the regulator: Ofcom has been designated as the independent regulator and possesses extensive powers, including the authority to request information, impose fines of up to £18 million or 10% of worldwide revenue, and, in serious cases, seek a court order restricting access to the platform (Bratby, 2026).

4.2.2. Enforcement Practice: Operational Cases

Since the Act began to be implemented in March 2025, Ofcom has pursued several important cases:

The Im.ge case of June 2025: Ofcom imposed a £20,000 fine on a file-sharing service for failing to respond to a request for information, failing to conduct a risk assessment, and failing to cooperate with the regulator. This was the first fine imposed under the OSA 2023 and demonstrated that a "breach of procedural duties" may independently attract a sanction (Ofcom, 2025).

The X case, formerly Twitter, of January 2026: Ofcom opened an investigation into X for allegedly failing to prevent the Grok chatbot from generating sexualized deepfake images. This was the first investigation involving a Category 1 platform, and the United Kingdom Government indicated that it would support blocking access to X if necessary (Bratby, 2026).

The Telegram case of April 2026: Ofcom opened an investigation into Telegram concerning the dissemination of child sexual abuse material. If violations are established, a fine of up to £18 million or 10% of worldwide revenue may be imposed (Ofcom, 2026).

4.2.3. Foundations of Criminal Liability under English Law

Unlike civil-law systems, English law bases the criminal liability of platforms on the "breach of a statutory duty" rather than on the jurisprudential concepts of causation or destruction of property. In other words, the mere existence of a causal relationship between the platform's conduct and the user's offense is insufficient. Instead, the legislature has prescribed specific obligations, such as risk assessment, content removal, and cooperation with the regulator, and the breach of those obligations constitutes an independent offense.

This approach, described as "liability based on preventive supervision," differs fundamentally from traditional principles of criminal law that emphasize direct participation in criminal conduct.

4.3. Comparative Analysis and the Development of a Domestic Model for Iran

Given the rapid growth of platforms and the absence of a clearly designated regulatory institution and transparent enforcement mechanisms in Iran, comparison with English law, which benefits from an integrated structure and an independent regulator, may provide a suitable basis for developing an effective domestic model.

4.3.1. Comparative Analysis of Iranian and English Law on the Criminal Liability of Platforms

It may be argued that Articles 749, 751, 760, and 761 of the Computer Crimes Act, considered together with subsequent amendments and supplementary enactments, constitute the principal basis of the criminal liability of platforms under Iranian law. Platform liability combines the duty to comply with orders issued by the Committee for Determining Instances of Criminal Content and judicial authorities, the duty of active reporting, the duty to retain data, and fault-based standards involving intentional refusal, carelessness, and negligence.

These provisions must be interpreted in light of the general rules governing the criminal liability of legal persons and the jurisprudential and doctrinal theories concerning the scope of duties and causal relationships. Accordingly, it may be stated that the principal basis of Iranian law is the jurisprudential rule of causation together with Article 143 of the Islamic Penal Code, whereas English law is based on the breach of a statutory duty, namely the duty of care.

Regarding the legal element, Iranian legislation is fragmented and incoherent, whereas England is governed by the comprehensive and integrated OSA 2023.

Regarding preventive duties, Iran operates without an express legislative framework and relies principally on subordinate regulations, whereas England expressly requires risk assessment, content removal, and reporting.

Regarding the regulatory institution, no single authority is clearly designated in Iran, and responsibility may fall to the Ministry of Culture and Islamic Guidance, the Judiciary, or the communications authorities. In England, however, Ofcom functions as an independent and specialized regulator.

Regarding enforcement mechanisms, the Iranian system provides for imprisonment and fines in an unclear and fragmented manner, whereas English law permits fines of up to £18 million and access-restriction orders.

Finally, Iranian judicial practice is inconsistent and limited, whereas English enforcement practice is developing and includes cases involving Im.ge, X, and Telegram.

Some authors maintain that requiring platform managers in Iran to review and select all content before publication would discourage content production because managers would seek to avoid the risk of criminal liability. Moreover, determining the lawful or unlawful nature of certain forms of user conduct may be complex. Therefore, in civil-liability cases, the concept of the stronger cause should be developed so that a platform may be held liable where it intentionally engages in gross negligence. In relation to criminal liability, however, such liability should arise only where the platform's criminal intent has been established (Gholamalizadeh & Hesam, 2023).

4.3.2. Feasibility of Legal Transplantation and Domestic Adaptation

Given its jurisprudential foundations, the Iranian legal system possesses considerable potential to adopt a similar model. The rule of causation may be interpreted as the jurisprudential basis of a "preventive duty," because where a platform is aware that an offense is occurring through its services and nevertheless refuses to remove it, the platform may customarily be regarded as a "cause" of the continuation of the offense (Mousavi Bojnourdi, 2019).

4.3.3. Research Limitations

The most important limitation of this study was the lack of access to the full text of certain domestic judicial decisions because of their confidential status, together with the limited development of Iranian judicial practice concerning modern platforms due to the novelty of the subject. In addition, the Online Safety Act 2023 is very recent, and its enforcement practice remains at an early stage.

5. Conclusion

This study sought to explain the scope, foundations, and conditions of the criminal liability of service-sharing platforms under the Iranian legal system and to compare them with the corresponding framework in English law. The principal findings were as follows:

Under Iranian law, despite the existence of rich jurisprudential foundations such as the rule of causation and the principle of no harm, together with the recognition of the criminal liability of legal persons in the Islamic Penal Code of 2013, no coherent and clearly defined system governs the criminal liability of platforms for crimes committed by users. Existing legislation, including the Computer Crimes Act and the Electronic Commerce Act, is largely focused on civil liability, while judicial practice remains inconsistent.

Under English law, the Online Safety Act 2023 established a comprehensive system based on the "duty of care," under which platforms are required to conduct risk assessments, prevent illegal content, and cooperate with the regulator, Ofcom. Early enforcement practice involving Im.ge, X, and Telegram indicates that the Act is being seriously implemented and that breaches of procedural obligations may also result in fines.

The proposed domestic model for Iran includes: (a) amending the Computer Crimes Act and adding provisions concerning the "preventive duties of platforms"; (b) establishing an independent regulator for cyberspace modeled on Ofcom; (c) designing a "tiered liability" regime based on the number of users and the level of risk; and (d) adopting an expansive interpretation of the rule of causation in judicial practice to encompass supervisory omissions.

The significance of this study lies in its provision, for the first time, of an in-depth comparative analysis between the jurisprudential foundations of Iranian law and the legislative and enforcement developments of English law concerning the criminal liability of platforms. It also proposes an operational and domestically adapted model for reforming Iranian legislation and improving judicial practice.

The study's recommendations are presented in three areas:

1. Legislative Recommendations

Amend Article 143 of the Islamic Penal Code to clarify the conditions governing the criminal liability of platforms as legal persons.

Add an independent chapter to the Computer Crimes Act entitled "Criminal Liability of Hosting Service Providers and Service-Sharing Platforms."

Enact an "Iranian Online Safety Act" inspired by the OSA 2023 but adapted to the jurisprudential foundations and legal structure of the country.

2. Executive and Judicial Recommendations

Establish a "National Center for the Supervision of Digital Platforms" with regulatory authority and effective enforcement powers.

Provide specialized training for judges in the field of platform-related offenses and require the Judicial Deputy of the Judiciary to issue a "Directive on the Criteria for Establishing the Criminal Liability of Platforms."

3. Research Recommendations

Conduct comparative research on the criminal liability of platforms under European Union law, particularly the Digital Services Act, and United States law, particularly Section 230 of the Communications Decency Act.

Examine the feasibility of establishing a compensation fund for users harmed by platform-related offenses, drawing on insurance-based compensation models.

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

Ardabili, M. A. (2020). *General Criminal Law (Vols. 1 and 2)*. Mizan.
Ashari, M. (2024). *Civil Liability of Online Platforms for Harmful Acts of Users* University of Tehran]. Tehran.
Bratby, L. (2026). Ofcom v X: The Online Safety Act Gets Its Defining Enforcement Test. https://bratby.law
Eventum, L. (2025). First UK Conviction under Section 184 Online Safety Act. https://www.eventumlegal.co.uk
Fallah, H. (2021). *Specific Criminal Law: Computer Crimes and Cyberspace*. University of Qom Press.
Gholamalizadeh, M., & Hesam, A. (2023). Civil Liability of Online Virtual Platforms for Users' Acts. *Islamic Law*, *20*(72), 127-145.
Heydari Aghamiri Kandi, M. (2024). An Examination of the Criminal Liability of Online Platforms and Crimes Committed by Their Users in the Criminal Law of Iran and the United States. Proceedings of the Eleventh International Conference on Management, Accounting and Law Studies,
Khalilinejad, S., & Barqei, S. A. R. (2024). *Civil Liability of Digital Platforms: From the Perspective of Jurisprudential Rules*. Roshd Publications.
Mirmohammad Sadeghi, H. (2020). *Computer Crimes*. Mizan.
Mohammadnejad, N. (2022). *Criminal Law of Information Technology*. Jangal Publications.
Mousavi Bojnourdi, S. M. (2019). *Jurisprudential Rules (Vol. 2: Rules of Destruction and Causation)*. Institute for Compilation and Publication of Imam Khomeini's Works.
Nurbaha, R. (2019). *General Criminal Law (Vol. 1)*. Mizan.

Ofcom. (2025). Investigation into the Provider of Im.ge and Its Compliance with Duties to Protect Its Users from Illegal Content. https://www.ofcom.org.uk

Ofcom. (2026). Investigation into the Provider of Telegram and Its Compliance with Duties to Protect Users from Illegal Content under the Online Safety Act 2023. https://www.ofcom.org.uk

Parhizkar, F. (2014). *Criminal Liability Arising from the Act of Another in Iranian Law*. University of Tehran Press.

Saffari, J. (2016). *Criminal Liability of Legal Persons*. SAMT.

Salahi, S. (2001). *Criminal Liability Arising from the Act of Another* University of Mazandaran].

Sanei, A. (2013). *Jurisprudential Foundations of Criminal Liability in Islamic Criminal Law*. Dar al-Fikr.

Sobel, B. (2021). The Law of Artificial Intelligence and Smart Machines. *Georgetown Law Technology Review*, *5*(2), 550-598.