



Shiraz University
RICeST
ISC

ISSN: 2008-7926

Journal of

Legal Studies

Vol. 18, Issue 3, Autumn 2026

JLS

Journal of Legal Studies

Journal Homepage: <https://jls.shirazu.ac.ir/>
doi: <https://10.22099/JLS.2025.53924.5367>



Research Article

Iran's Preventive Legislative Criminal Policy Regarding the Activities of Information Technology Commercial Platforms

Azim Aghababaei Taghanaki¹, Seyyed Doraid Mousavi Mojab^{2*},
Mohammad Ja'far HabibZadeh³, Pejman Mohammadi⁴

1. PhD student in Criminal Law and Criminology, Department of Criminal and Criminology Law, Faculty of Law, Tarbiat Modares University, Tehran, Iran
2. Assistant Prof., Department of Criminal Law and Criminology, Faculty of Law, Tarbiat Modares University, Tehran, Iran
3. Professor, Department of Criminal Law and Criminology, Faculty of Law, Tarbiat Modares University, Tehran, Iran
4. Professor, Department of Intellectual Property Law, Faculty of Law, Tarbiat Modares University, Tehran, Iran

Article history:

Received: 10-08-2025

Accepted: 13-12-2025

Abstract

Introduction

The advancement of information and communication technologies (ICT) has profoundly transformed the social, economic, and legal structures of modern societies, steering human life toward digitalization. In this digital era, commercial information technology platforms have become fundamental pillars in economic, social, and even political domains. While facilitating

Please cite this article as:

Aghababaei Taghanaki, A., Mousavi Mojab, S.D., HabibZadeh, M.J., Mohammadi, P (2026). Iran's Preventive Legislative Criminal Policy Regarding the Activities of Information Technology Commercial Platforms. *Journal of Legal Studies*, 18(3), 471-512. doi: <https://10.22099/JLS.2025.53924.5367>

* Corresponding author:

E-mail address: d.mojab@modares.ac.ir

Iran's Preventive Legislative Criminal Policy ... Azim Aghababaei Taghanaki



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

daily activities, these platforms have simultaneously created fertile ground for emerging forms of cybercrime, which—due to their complex,

transnational, and technologically dynamic nature—pose serious challenges to traditional criminal justice systems. In light of the rapid growth of platform-based criminality and the undeniable role of digital platforms in enabling such offenses, it is both urgent and necessary to evaluate and redesign Iran's legislative preventive criminal policy in this context. This study aims to examine the structure and effectiveness of Iran's current legislative criminal policy in addressing criminal activities on commercial platforms and to identify its deficiencies while proposing the need for a new policy framework grounded in modern criminal policy principles.

Methods

This study employs a descriptive-analytical approach and relies on document-based legal research. It examines key legislative instruments relevant to platform-based cybercrime in Iran, including the Computer Crimes Act, the Electronic Commerce Act, the Crime Prevention Act, the Anti-Money Laundering Act, the Counter-Terrorist Financing Act, the Protection of Children and Adolescents Act, and selected resolutions of the Supreme Council of Cyberspace. These legal instruments are analyzed with a focus on their preventive potential, normative consistency, and practical alignment with contemporary goals of crime prevention in cyberspace. Upon identifying the structural and normative inefficiencies of Iran's preventive legislation vis-à-vis platform criminality, the study underscores the necessity of formulating a modern preventive criminal policy. Policy proposals themselves are not within the scope of this paper but are suggested as avenues for future research to fill the identified theoretical and regulatory gaps.

Results and Discussion

The findings reveal that Iran's legislative criminal policy in response to crimes committed via information technology platforms suffers from a lack of institutional coherence and practical effectiveness. There are substantial legal voids concerning the criminal liability of platforms, the implementation of intelligent and technology-based preventive measures, systematic risk assessment, and structural transparency. Current legal provisions primarily rely on content filtering and blocking, without incorporating data-driven, algorithmic, or AI-powered prevention strategies. Although situational crime prevention tools—such as mandatory content removal and suspicious pattern detection—are present in some statutes, they lack robust enforcement mechanisms and broad applicability to digital platforms. Furthermore, the fragmentation of regulatory authorities and the absence of a central specialized regulatory body have rendered the state's response to platform-based criminality slow, reactive, and often ineffective. While the Electronic Commerce Act and the Cheque Issuance Law contain elements that could

support non-penal preventive frameworks, they remain rooted in traditional paradigms and fail to engage with platform-specific risks. In the realm of child protection, although platforms are legally obligated to remove harmful content, no binding supervisory mechanisms have been established. Ultimately, the overreliance on content filtering, in place of strategic technological intervention, has not only failed to mitigate cybercrime but has also contributed to the erosion of public trust and the rise of user resistance. Moreover, the analysis shows that the existing regulatory framework, despite containing fragmented preventive elements, lacks technological appendices, clear procedural obligations for platforms, and enforceable standards of preventive compliance. Preventive mechanisms outlined in the Supreme Council of Cyberspace's resolutions—such as access restriction and platform filtering—are primarily reactive in nature and do not reflect intelligent crime prevention models. The continued application of this outdated approach has led to unintended consequences, such as the proliferation of anti-filtering tools and an increase in cybersecurity threats, further undermining the effectiveness of Iran's platform governance.

Conclusion

This study concludes that Iran's current legislative preventive criminal policy toward criminal activities on commercial information technology platforms is outdated, inefficient, and institutionally fragmented. To effectively combat the rise of platform-based cybercrime and restore public trust, a paradigm shift is essential—one that adopts soft regulation, enforces platform accountability, encourages public and private sector participation, and leverages modern technologies. Without a fundamental reconfiguration of the preventive criminal policy in this domain, the prospects for effective crime prevention remain dim, and the legitimacy and functionality of the criminal justice system may face serious long-term challenges.

Keywords: Legislative Criminal Policy, Criminal Policy-Making, Crime Prevention, Commercial Platforms, Information Technology.

Ethical Considerations

Not applicable

Funding

Not applicable

Conflict of interest

The authors declare no conflict of interest



مقاله پژوهشی

سیاست جنایی تقنینی پیشگیرانه ایران در قبال فعالیت‌های سکوه‌ای تجاری فناوری اطلاعات+

عظیم آقابابائی طاقانکی^۱، سید درید موسوی مجاب^{۲*}، محمدجعفر حبیب‌زاده^۳، پژمان محمدی^۴

۱. دانشجوی دکترای حقوق کیفری و جرم‌شناسی، گروه حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران
۲. استادیار، گروه حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران
۳. استاد، گروه حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران
۴. استاد، گروه حقوق مالکیت فکری، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران

اطلاعات مقاله تاریخ پذیرش: ۱۴۰۴/۰۹/۲۲

تاریخ دریافت: ۱۴۰۴/۰۵/۱۹

اطلاعات مقاله

چکیده

با گسترش سکوه‌ای تجاری دیجیتال و نقش فزاینده آن‌ها در بروز جرائم نوین سایبری، ارزیابی و بازنگری سیاست جنایی ایران در قبال این پدیده، ضرورتی انکارناپذیر یافته است. پژوهش حاضر با روش توصیفی-تحلیلی، به بررسی سیاست جنایی تقنینی ایران در قبال فعالیت‌های مجرمانه در بستر سکوه‌ای فناوری اطلاعات می‌پردازد. در این راستا، مهم‌ترین مقررات قانونی مرتبط، از جمله قانون جرائم

استناد به این مقاله:

آقابابائی، طاقانکی عظیم؛ موسوی مجاب، سید درید؛ حبیب‌زاده، محمدجعفر و محمدی، پژمان (۱۴۰۵). سیاست جنایی تقنینی پیشگیرانه ایران در قبال فعالیت‌های سکوه‌ای تجاری فناوری اطلاعات. *مجله مطالعات حقوقی*. ۱۸. (۳). ۵۱۲-۴۷۱.

+ این مقاله مستخرج از رساله دکترای آقای عظیم آقابابائی طاقانکی با عنوان «سیاست‌گذاری جنایی در قبال فعالیت‌های مجرمانه سکوه‌ای تجاری در بستر فناوری اطلاعات»، در دانشگاه تربیت مدرس، با راهنمایی آقای دکتر سید درید موسوی مجاب و مشاوره آقایان دکتر محمدجعفر حبیب‌زاده و دکتر پژمان محمدی است.

E-mail address: d.mojab@modares.ac.ir

نویسنده مسئول:


Copyright: C 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

تجارت الکترونیک، پیشگیری از وقوع جرم و سایر قوانین خاص، مورد تحلیل قرار گرفته‌اند. یافته‌ها نشان می‌دهند که سیاست جنایی ایران در برابر این نوع بز هکاری، فاقد انسجام، روزآمدی و کارایی لازم است. ضعف در شناسایی خطر، فقدان تدابیر پیشگیرانه هوشمند، نبود مقررات

ناظر بر مسئولیت کیفری پلتفرم‌ها و پراکندگی نهادی ازجمله نارسایی‌های اصلی محسوب می‌شوند. در نتیجه، پژوهش بر ضرورت طراحی سیاست جنایی پیشگیرانه کارآمد، با تمرکز بر تنظیم‌گری نرم، مسئولیت‌پذیری سکوها، استفاده از فناوری‌های نوین و مشارکت عمومی تأکید دارد تا از گسترش بزهکاری پلتفرمی و تضعیف اعتماد عمومی پیشگیری شود.

واژگان کلیدی: سیاست جنایی تقنینی، سیاست‌گذاری جنایی، پیشگیری از جرم، سکوهای تجاری، فناوری اطلاعات.

سرآغاز

امروزه پیشرفت فناوری اطلاعات و ارتباطات^۱، ساختارهای اجتماعی، اقتصادی و حقوقی جوامع را متحول کرده و زندگی انسان‌ها را به‌سوی دیجیتالی شدن^۲ سوق داده است. سکوهای دیجیتال، فعالیت‌هایی مانند خریدوفروش، ارتباطات، سرگرمی، حمل‌ونقل، اقامت و حتی امور سیاسی را تسهیل کرده و وابستگی انسان‌ها به این سکوها را افزایش داده‌اند (West, 2019: 11). این تحولات، روش‌های سنتی تجارت و ارتباطات را دگرگون کرده و مفاهیم زمان و مکان را بازتعریف کرده‌اند (Kwan, 2002: 478). سکوهای تجاری^۳ آنلاین به‌عنوان بستری برای خلق ارزش‌های نوآورانه، مشکلات کاربران را حل کرده، درآمد کسب‌وکارها را افزایش داده و به رشد اقتصادی و توسعه اجتماعی کمک می‌کنند (Moro Visconti, 2020: 1; Volkov & Sidorenko, 2022: 3). با این حال، ماهیت سایبری-شرکتی^۴ این سکوها، جرائم جدیدی را به وجود آورده، چه در بعد پیشگیرانه و چه در بعد قهرآمیز نیازمند سیاست‌گذاری جنایی متناسب با این ماهیت نوین است. در ایران، مقررات بسیاری در قبال فعالیت‌های سکوهای تجاری فناوری اطلاعات در فضای مجازی می‌توان یافت، ولیکن اینکه آیا این مقررات توانسته‌اند در بعد پیشگیری از جرم توسط خود سکوها یا توسط کاربران سکوها مؤثر و کارآمد اقدام کنند، سؤالی است که پس از بررسی کیفی این مقررات و تحلیل مواد قانونی می‌توان به آن پاسخ داد. بدین منظور باید ابتدا به مفهوم شناسی و سپس تحلیل قوانین و مقررات پرداخت. در راستای مفهوم شناسی دو مفهوم سیاست جنایی تقنینی پیشگیرانه و همچنین سکوهای تجاری فناوری اطلاعات موردبحث و بررسی قرار خواهند گرفت.

در خصوص مفهوم شناسی سیاست جنایی باید بیان کرد، اولین بار آنسلم فون فوئرباخ از عبارت سیاست جنایی در کتاب حقوق کیفری خود که در سال ۱۸۰۳ منتشر شد، استفاده کرد (Feuerbach, 1833) و منظور وی از آن، دقیقاً همان سیاست کیفری بود. در آن کتاب، مضیق‌ترین تعریف یعنی «مجموعه پاسخ‌های سرکوبگرانه دولتی در قبال جرم»، سیاست جنایی نامیده شد. (Lazerges, 2000: 8) امروزه سیاست جنایی، در یک مفهوم موسع به کار می‌رود و با سیاست اجتماعی کنترل جرم پیوند می‌خورد. این مفهوم، به معنای مجموعه روش‌ها و آیین‌هایی است که هیئت اجتماع با استفاده از آن‌ها پاسخ‌های مختلف به پدیده مجرمانه را سامان می‌بخشد (Delmas-Marty, 1991: 44; Szabo, 1978: 113) و

1. Information Communications Technology (ICT)
2. Digitalization
3. Commercial platforms
4. Cyber-corporate

ذیل عنوان «سیاست عمومی» یک کشور قرار دارد (Guarda, 2017: 196) و به یکی از قلمروهای سیاسی، اجتماعی و حقوقی تبدیل می‌شود (Lazerges, 2000: 9). سیاست جنایی در این معنا، در مرحله پاسخ‌دهی، پاسخ‌های کیفری یا غیر کیفری و پاسخ‌های رسمی یا غیررسمی را شامل می‌شود و در مرحله ممنوعیت گذاری نیز شامل بزه و انحراف و جرم می‌شود (Lazerges, 2000: 31). از زمره پاسخ‌های غیر کیفری، می‌توان به پاسخ‌های پیشگیرانه اشاره داشت. یکی از اقسام سیاست جنایی، سیاست جنایی تقنینی و از زمره مقررات مربوط به سیاست جنایی تقنینی، تدابیر پیشگیرانه مذکور در قانون است. سیاست جنایی تقنینی (به فرانسوی *Politique criminelle legislative*)، سیاستی است که از جانب مقنن اتخاذ و در قالب مقررات قانونی بیان می‌شود (عظیمزاده و شیخ‌الاسلامی، ۱۳۹۸: ۲۱۱) و شامل تدوین قوانین کیفری و تعیین مجازات است که باید متناسب با نیازهای اجتماعی و تغییرات جرم شناختی به‌روز شود (Szabo, 1978: 181). درواقع سیاست جنایی تقنینی، به مجموعه تدابیری اطلاق می‌شود که مقنن برای مقابله با جرائم و تخلفات در جامعه اتخاذ کرده و در قالب قوانین و مقررات بیان می‌کند. در صورتی که مقررات در راستای پیشگیری وضع شوند، سیاست جنایی تقنینی، از نوع پیشگیرانه خواهد بود. با این حال، باید دقت داشت که سیاست جنایی تقنینی پیشگیرانه، نه در گستره حقوق کیفری بلکه در گستره قلمروی کیفری نمایانگر است. در قلمروی کیفری، مرزهای حقوق کیفری بر هم خورده و حتی تدابیر پیشگیرانه نیز ذیل اصول حقوق کیفری و عدالت و انصاف قرار می‌گیرند (بابایی و مهدوی: ۱۳۹۱: ۱۰۲-۱۰۱؛ یآوری، ۱۳۹۴: ۲۲۴؛ آقابابائی طاقانکی و دیگران، ۱۴۰۴: ۲۶۵).

مراجع بسیاری در کشور ایران در سیاست‌گذاری جنایی، در قبال فعالیت‌های مجرمانه سکوه‌های تجاری فناوری اطلاعات در بعد پیشگیرانه سویم و دخیل هستند. از جمله می‌توان به قوه مقننه، شورای عالی فضای مجازی (ساقی و دیگران، ۱۴۰۳: ۲۵۹)، کارگروه تعیین مصادیق محتوای مجرمانه معروف به «کمیته فیلترینگ» (ماده ۷۵۰ کتاب پنجم تعزیرات قانون مجازات اسلامی، الحاقی به موجب قانون جرائم رایانه‌ای مصوب ۱۳۸۸)، قوه قضائیه، کمیسیون تنظیم مقررات ارتباطات (مواد ۵ و ۶ قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات)، شورای عالی فناوری اطلاعات (بند ه ماده ۴ قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات) و شورای عالی پیشگیری از جرم (ماده ۳ قانون پیشگیری از وقوع جرم) اشاره کرد. سکوه‌های فناوری اطلاعات را می‌توان فناوری‌های همه‌منظوره‌ای تعریف کرد که مجموعه‌ای از برنامه‌ها^۱ و فرصت‌های تجاری را به هم متصل می‌کنند

(Fichman, 2004: 132). این سکوها شامل پیکربندی سخت‌افزاری، سیستم‌عامل، چارچوب نرم‌افزاری یا هر موجودیت مشترکی هستند که سرویس‌ها و مؤلفه‌های مرتبط روی آن اجرا می‌شوند (Hamilton, 2022: 4). این سکوها شش بعد دارند: (۱) فناوری پایه^۱ که توسعه افزونه‌ها را ممکن می‌سازد (Hagiu, 2014: 71; Rai et al., 2006: 227; Kraemer et al., 2010: 1; Lahiri et al., 2010: 81; Meyer & Seliger, 1998: 61; Tiwana et al., 2010: 675-676)؛ (۲) افزونه‌ها^۲ شامل برنامه‌های کاربردی، مکمل‌ها، سیستم‌های فرعی و پلاگین‌هایی^۳ که قابلیت‌های تجاری را فعال می‌کنند (Ceccagnoli et al., 2012: 263; Taudes et al., 2000: 228-229; Bergvall-Kåreborn & Howcroft, 2014: 443; Meyer & Tiwana et al., 2010: 268; Anderson Jr et al., 2014: 156)؛ (۳) تعامل‌پذیری یا قابلیت اتصال و اشتراک‌گذاری (Tiwana et al., 2010: 268; Dhar & Riemer, 2010: 1; Sundararajan, 2007: 134)؛ (۴) تراکنش پذیر^۴ شامل تبادلات^۵، تعاملات^۶ و معاملات^۷ (Sun et al., 2015: 5)؛ (۵) حکمرانی^۸، یعنی سیاست‌ها و سازوکارهای مدیریت سکو (Sun et al., 2015: 7)؛ بنابراین، سکوه‌های فناوری اطلاعات سیستم‌های پیچیده‌ای با اجزای متعدد هستند. نظر به اینکه اغلب سکوها، در قالب یک شرکت غالباً تجاری و در فضای دیجیتال متصل به اینترنت فعالیت می‌کنند؛ لذا این دسته از سکوها از باب غلبه، اهمیت دوچندانی می‌یابند. اقتصاد سکویی^۹ به آماده‌سازی خدمات و یا دسترسی به کالاها از طریق سکوها اشاره دارد (Drahokoupil & Fabo, 2016: 1-2). پنجمین مؤلفه در مفهوم شناسی سکوه‌های فناوری اطلاعات، تراکنش پذیر است که نشان دهنده نهادینه بودن اهداف اقتصادی در این سکوهاست. از این منظر، سکوه‌های تجاری به دو دسته تقسیم می‌شوند:

۱. سکوه‌های تجاری در معنای عام؛ سکوهایی که فعالیت اصلی آن‌ها غیرتجاری است، اما از طریق تبلیغات و آگهی به دنبال کسب درآمد هستند، مانند اینستاگرام و فیس‌بوک.

1. Technological Base
2. Add-ons
3. Plug-ins
4. Transactionality
5. Exchanges
6. Interactions
7. Transactions
8. Governance
9. Platform Economy

۲. سکوهای تجاری در معنای خاص؛ سکوهایی که اساساً با هدف تجارت و دادوستد ایجاد شده‌اند، مانند آمازون.

در ایران، پژوهش‌هایی در خصوص سیاست جنایی ایران در قبال سکوهای تجاری به چشم می‌خورد، ولیکن این پژوهش‌ها درباره ناکارآمدی سیاست جنایی در برابر جرائم سکوهای تجاری فناوری اطلاعات با شکاف‌هایی مواجه است. نعیمی‌نژاد (۱۴۰۳) در رساله دکتری خود، به بررسی خلأهای سیاست جنایی ایران در قبال جرائم سایبری و الزامات سیاست‌گذاری پرداخته است. صادقی، ابراهیمی و نعیمی‌نژاد (۱۴۰۳) در مقاله خود، نبود سیاست‌گذاری مؤثر را عامل برداشت‌های افراطی یا تفریطی دانسته و اصولی مانند ثبات مبانی، حفظ حریم خصوصی، عدالت محوری، شفافیت و توسعه پایدار را پیشنهاد کرده‌اند. تیرگیر و همکاران (۱۴۰۳) در پژوهش خود، بر ضرورت تدابیر پیشگیرانه به دلیل گمنامی و تسهیل جرائم در فضای مجازی تأکید کرده و این تدابیر را برای تربیت بزهکاران بالقوه و پیشگیری از جرم مؤثر دانسته‌اند. انصاری و همکاران (۱۴۰۱) در مقاله‌ای دیگر بر لزوم سیاست جنایی مشارکتی با همکاری مردم، کاربران و نهادهای مدنی تأکید کرده و نظارت والدین، ایجاد فضای سبز سایبری و تعامل با پلیس فتا را از مصادیق آن دانسته‌اند. وطنی و اسدی (۱۳۹۵) نیز به‌صورت کلی سیاست جنایی ایران در برابر جرائم سایبری را بررسی کرده‌اند. این پژوهش به بررسی سیاست جنایی تقنینی ایران در زمینه مقررات پیشگیرانه مرتبط با فعالیت‌های مجرمانه سکوهای تجاری فناوری اطلاعات می‌پردازد تا خلأها و کاستی‌های موجود آشکار شده و بستر مطالعات بعدی برای تبیین بایسته‌ها و پیامدهای سیاست‌گذاری جنایی فراهم شود. از آنجا که اولین منبع برای بررسی سیاست جنایی تقنینی پیشگیرانه، قوانین و مقررات جزایی است (اسدی جونوشی و وروائی، ۱۳۹۸: ۱)، در این پژوهش، تمرکز بیشتر بر روی بررسی قوانین و مقرراتی است که سیاست‌های پیشگیرانه در قبال سکوهای تجاری فناوری اطلاعات در آن‌ها مقرر شده است.

۱. تدابیر پیشگیرانه در قوانین کیفری ایران

مقررات مربوط به پیشگیری از جرم در قانون مجازات اسلامی و قوانین خاص دیگر قابل مشاهده است. در قوانینی همچون قانون مجازات اسلامی یا قانون جرائم رایانه‌ای، مقنن از همان ابتدا به قصد هنجار گذاری کیفری نسبت به تقنین اقدام کرده است. ازجمله قوانین کیفری که در آن‌ها می‌توان مقررات پیشگیرانه در خصوص سکوهای تجاری فناوری اطلاعات یافت، قانون جرائم رایانه‌ای، قانون مبارزه با تأمین مالی تروریسم و قانون مبارزه با پول‌شویی است. سیاست تقنینی ایران در قانون مجازات اسلامی با قوانین جزئی‌تر و خاص، متفاوت است.

(حسینی و دیگران، ۱۴۰۴: ۵۰۲) به همین دلیل ضروری است هر یک از این قوانین مجزا مورد بررسی قرار گیرد.

۱-۱. قانون جرائم رایانه‌ای مصوب ۱۳۸۸

در قانون جرائم رایانه‌ای مواد و مقرراتی وجود دارند که یکی از اهداف وضع و تصویب آن‌ها پیشگیری از وقوع جرم بوده است. در این خصوص می‌توان به مواد ۷۴۹، ۷۵۱، ۷۲۹ و ۷۵۳ کتاب پنجم تعزیرات قانون مجازات اسلامی مصوب ۱۳۷۵ (الحاقی به موجب قانون جرائم رایانه‌ای مصوب ۱۳۸۸) اشاره کرد.

۱-۱-۱. مواد ۷۴۹ و ۷۵۱

به موجب ماده ۷۴۹، «ارائه دهندگان خدمات دسترسی موظفاند طبق ضوابط فنی و فهرست مقرر از سوی کار گروه (کمیته) تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرائم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود را پالایش (فیلتر) کنند. در صورتی که عمداً از پالایش (فیلتر) محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینه دسترسی به محتوای غیرقانونی را فراهم آورند ... به‌جزای نقدی [یا] ... تعطیلی موقت ... محکوم خواهند شد.» پالایش یا فیلترینگ، عبارت است از محدود کردن دسترسی کاربران اینترنت به وب‌گاه و خدمات اینترنتی (بابایی، ۱۳۹۹: ۲۸). به موجب ماده ۷۵۱ قانون اخیرالذکر: «ارائه دهندگان خدمات میزبانی موظفاند به‌محض دریافت دستور کار گروه (کمیته) تعیین مصادیق مذکور در ماده فوق یا مقام قضائی رسیدگی کننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه‌های رایانه‌ای خود از ادامه دسترسی به آن ممانعت به عمل آورند. چنانچه عمداً از اجرای دستور کارگروه (کمیته) یا مقام قضائی خودداری کنند، منحل خواهند شد. در غیر این صورت، چنانچه در اثر بی‌احتیاطی و بی‌مبالاتی زمینه دسترسی به محتوای مجرمانه مزبور را فراهم کنند ... به‌جزای نقدی [یا] ... تعطیلی موقت ... محکوم خواهند شد.» ارائه کننده خدمات میزبانی می‌تواند با استفاده از امکانات و تجهیزاتی که در اختیار دارد، ضمن حفظ سوابق، محتوای موردنظر را به کلی از فضای اینترنت خارج کند (بابایی، ۱۳۹۹: ۱۹۱). مواد ۷۴۹ و ۷۵۱ قانون جرائم رایانه‌ای با الزام ارائه دهندگان خدمات دسترسی و میزبانی به پالایش یا حذف محتوای مجرمانه، به‌طور مستقیم در راستای پیشگیری از جرم عمل می‌کنند. در این خصوص چند سازوکار را می‌توان در این دو ماده در راستای پیشگیری از جرم مشاهده کرد:

- کاهش فرصت‌های ارتکاب جرم

این مواد با محدود کردن دسترسی به محتوای مجرمانه، فرصت‌هایی را که افراد ممکن است برای ارتکاب جرم از آن‌ها استفاده کنند، کاهش می‌دهند. برای مثال: پالایش محتوایی مانند آموزش‌های هک یا ابزارهای نفوذ (ماده ۷۴۹) می‌تواند مانع از آن شود که افراد مهارت‌ها یا وسایل لازم برای ارتکاب جرائم رایانه‌ای را به دست آورند. همچنین توقف دسترسی به محتوایی مانند سوءاستفاده از کودکان یا ترویج خشونت (ماده ۷۵۱) از گسترش این محتوا و تأثیر آن بر افراد که ممکن است به جرائم مرتبط منجر شود، جلوگیری می‌کند. با توجه به اینکه اولاً، در پیشگیری موقعیت محور تمرکز بر حذف یا کاهش فرصت‌های ارتکاب جرم است (Clarke, 1995: 1) و ثانیاً، در فضای سایبری نیز این سیاست با طراحی و تغییر محیط، مانع ارتکاب جرم می‌شود (Willison & Siponen, 2009: 134). می‌توان استنتاج کرد که مقررات اخیرالذکر در همین دسته قرار می‌گیرند، زیرا وضعیت جرم‌زا را مختل می‌کنند (Ho et al., 2022: 1).

- پیش‌بینی و شناسایی خطر

امروزه پیشگیری از جرم به یک گفتمان مبتنی بر ریسک تبدیل شده است، به‌طوری‌که شناسایی و مدیریت خطرات برای کاهش فرصت‌های ارتکاب جرم و افزایش ایمنی جامعه در اولویت قرار دارد (Kemshall, 2003: 127). فلذا پیش‌بینی و شناسایی خطر می‌تواند ابزار مفیدی در پیشگیری از جرائم، در بستر سکوهاى تجاری فناوری اطلاعات تبدیل شود. مقررات فوق‌الذکر با تکیه بر فهرست کارگروه تعیین مصادیق یا دستور مقام قضایی، به شناسایی و پیش‌بینی محتوایی که می‌تواند خطر وقوع جرم را افزایش دهد، کمک می‌کنند. این امر با تعریف پیشگیری در ماده ۱ قانون پیشگیری از وقوع جرم هم‌راستاست.

۲-۱-۱. ماده ۷۲۹

البته قانون‌گذار جمهوری اسلامی ایران، روش دیگری را نیز در پیشگیری از جرم در قانون جرائم رایانه‌ای اتخاذ کرده است. قانون‌گذار در مواد ۷۲۹ و ۷۵۳ قانون فوق‌الذکر با پیش‌بینی جرائم مانع، درصدد پیشگیری از سایر جرائم مهم‌تر برآمده است. جرم مانع، به جرمی اطلاق می‌شود که مقدمه یا زمینه‌ساز ارتکاب جرم دیگری است و معمولاً، آن جرم دوم بدون وقوع جرم مادر نمی‌تواند تحقق یابد. جرم‌انگاری جرائم مانع (جرم مادر) یکی از ابزارهای سیاست جنایی پیش‌نگر است. هرچند این اصطلاح معمولاً در جرائم سازمان‌یافته، پول‌شویی و جرائم اقتصادی کاربرد دارد (Bell, 2003: 137; Rusanov & Pudovochkin, 2018: 22) ولیکن امکان تصور جرم مانع در خصوص سایر جرائم از جمله جرائم رایانه‌ای نیز وجود دارد. به موجب ماده ۷۲۹: «هرکس به‌طور غیرمجاز به داده‌ها یا

سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است، دسترسی یابد، به حبس از نودویک روز تا یک سال یا جزای نقدی ... یا هر دو مجازات محکوم خواهد شد.» با توجه به این‌که این جرم، مقدمه ارتکاب بسیاری از جرائم رایانه‌ای دیگر است، جرم مانع (جرم مادر یا بازدارنده) محسوب می‌شود. باید توجه داشت که این جرم مقدمه لازم دیگر بزه‌های رایانه‌ای محسوب نمی‌شود و چه‌بسا جرائم رایانه‌ای بدون دسترسی غیرمجاز نیز محقق شوند (بابایی، ۱۳۹۹: ۶۱). با جرم‌انگاری دسترسی غیرمجاز که اغلب اولین گام در ارتکاب جرائم رایانه‌ای است، به‌عنوان یک جرم مانع عمل می‌کند و از طریق موارد زیر به پیشگیری از جرم در سکوها تجاری کمک می‌کند:

- حفاظت از داده‌ها و تراکنش‌های حساس

در دنیای به‌شدت دیجیتالی امروز، داده‌ها به یکی از باارزش‌ترین دارایی‌ها برای سازمان‌ها تبدیل شده‌اند. با افزایش حملات سایبری، نقض داده‌ها و فضای نظارتی سخت‌گیرانه، اتخاذ راهبردهای قدرتمند حفاظت از داده‌ها ضروری است. سکوها تجاری حاوی اطلاعات مهمی مانند داده‌های شخصی کاربران، شماره کارت‌های بانکی و سوابق تراکنش‌ها هستند. یکی از روش‌های حفاظت از داده‌ها و تراکنش‌های حساس کاربران سکوها تجاری، استفاده از سیاست‌های حاکمیتی است (Julakanti et al., 2023: 158). دسترسی غیرمجاز به این سامانه‌ها، می‌تواند به سرقت اطلاعات یا اختلال در خدمات منجر شود. ماده ۷۲۹ با مجازات افرادی که بدون اجازه به این سیستم‌ها نفوذ می‌کنند، از نقض امنیت این سکوها جلوگیری می‌کند و اعتماد کاربران را حفظ می‌کند.

- بازدارندگی از جرائم بعدی

هرچند بازدارندگی از ارتکاب جرم سایبری به عوامل مختلفی بستگی دارد و همچنین بازدارندگی، از طریق جرم‌انگاری و مجازات با محدودیت‌های قضایی و منابع (ابزارها و امکانات مبارزه با جرم) مواجه است؛ (Kesari et al., 2017: 1093) ولیکن در یک نگاه بسیط می‌توان اذعان داشت جرم مانع می‌تواند موجب بازدارندگی از ارتکاب جرائم بعدی و مهم‌تر شود؛ زیرا مجرمین می‌دانند که نه‌تنها برای جرم نهایی بلکه برای اعمال اولیه نیز تحت پیگرد قرار می‌گیرند؛ درنتیجه، ممکن است از آغاز مسیر مجرمانه منصرف شوند. افزایش هزینه‌های ارتکاب جرم از طریق جرم‌انگاری رفتارهای مقدماتی می‌تواند به‌طور بسیار مؤثری مجرمان را از ارتکاب جرم منصرف کند.

دسترسی غیرمجاز، معمولاً مقدمه جرائم جدی‌تری مانند کلاهبرداری آنلاین، سرقت داده‌ها یا دست‌کاری اطلاعات است. برای مثال، نفوذ به سامانه یک فروشگاه آنلاین می‌تواند به سرقت اطلاعات کارت اعتباری مشتریان یا تغییر موجودی انبار منجر شود. این ماده با جرم‌انگاری این مرحله اولیه، انگیزه افراد

برای شروع چنین فعالیت‌هایی را کاهش می‌دهد و از وقوع جرائم بعدی پیشگیری می‌کند.

- کاهش فرصت‌های جرم

هرچند برخی از دکترین، برای پیشگیری وضعی از ارتکاب جرم ارزش چندانی قائل نیستند و معتقدند که پیشگیری وضعی از ارتکاب جرم از طریق کاهش فرصت‌های ارتکاب جرم، تنها میل به ارتکاب جرم را سرکوب می‌کنند که سپس در موقعیت دیگری و شاید به شکلی حتی مضرت‌تر، خود را نشان خواهد داد (Clarke, 1980: 136)، ولیکن تأثیر این نوع از پیشگیری غیر قابل انکار است. یکی از اهداف رویکرد پیشگیری وضعی (موقعیت محور) از جرم، پیشگیری از طریق کاهش فرصت‌های وقوع جرم است. (Holmen, 2024: 325) مجازات دسترسی غیرمجاز، افراد را از نفوذ به سامانه‌های حفاظت شده باز می‌دارد. این امر به‌ویژه در سکوه‌های تجاری که از تدابیر امنیتی برخوردارند، فرصت ارتکاب جرم را محدود می‌کند و امنیت کلی این پلتفرم‌ها را افزایش می‌دهد.

۱-۱-۳. ماده ۷۵۳

همچنین قانون‌گذار در ماده ۷۵۳ به جرم‌انگاری بسیاری از رفتارهایی اقدام کرده است که هدف اصلی از جرم‌انگاری آن‌ها، بازدارندگی است و فاقد موضوع مستقیم هستند (عالی پور، ۱۳۹۵: ۳۳۳). این ماده با جرم‌انگاری تولید، توزیع و انتشار ابزارها، داده‌ها و آموزش‌های مجرمانه، نقش مهمی در پیشگیری از جرائم در سکوه‌های تجاری ایفا می‌کند:

- جلوگیری از انتشار ابزارهای مجرمانه

شرکت‌های متولی سکوها، روزانه در سراسر جهان سیاست‌ها و اقداماتی را اجرا می‌کنند که غالباً با هدف حفظ تعامل کاربران و پشتیبانی از مدل‌های درآمدی آن‌ها تدوین شده است. با این حال، این فعالیت‌های تجاری به‌ظاهر عادی، گاه ناخواسته

۱. ماده ۷۵۳. هر شخصی که مرتکب اعمال زیر شود، به حبس از نودوپنجم روز تا یک سال یا جزای نقدی ... یا هر دو مجازات محکوم خواهد شد:

(الف) تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معامله داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به‌منظور ارتکاب جرائم رایانه‌ای به کار می‌رود.

(ب) فروش یا انتشار یا در دسترس قرار دادن، گزرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می‌کند.

(ج) انتشار یا در دسترس قرار دادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلاف در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی.

تبصره - چنانچه مرتکب، اعمال یاد شده را حرفه خود قرار داده باشد، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

زمینه‌ساز ارتکاب جرم توسط مجرمان می‌شود (Hamilton, 2022: 1350). سهولت ورود، شرط اساسی موفقیت سکوها در جذب شمار زیادی از کاربران است، اما همین ویژگی در برخی موارد پیامدهایی منفی به همراه دارد (Espinoza, 2024: 231). از زمره این پیامدها، توانمندسازی یا تسهیلگری ارتکاب جرم توسط پلتفرم‌ها^۱ است. یکی از این اقسام توانمندسازی جرائم در سکوها، در دسترس قرار دادن ابزارهای مجرمانه است. با محدود کردن این موضوع، می‌توان در راستای پیشگیری از جرم اقدام کرد. ماده ۷۵۳ با مجازات تولید و توزیع این ابزارها، از دسترسی مجرمان به چنین وسایلی جلوگیری می‌کند و ریسک حملات به سکوهای تجاری را کاهش می‌دهد.

- محدود کردن آموزش‌های مجرمانه

امروزه برخی از سکوها، در راستای دسترسی به بسترهای مساعد برای ارتکاب جرم آموزش‌هایی را به کاربران خود ارائه می‌دهند. به‌عنوان مثال پلتفرم‌هایی مانند ردیت^۲ ممکن است (گاه ناخواسته) به اشتراک‌گذاری ابزارهای فنی، لینک‌ها یا آموزش‌هایی کمک کنند که کاربران را به دارکوب^۳ هدایت می‌کنند. دیت هم در وب روشن و هم در وب تاریک در دسترس بوده و ناخواسته، به‌عنوان درگاهی برای کاربران تازه‌وارد عمل می‌کند تا با سازوکار بازارهای دارکنت آشنا شده و زمینه ورودشان فراهم شود (Kwon & Shao, 2021: 779). ارائه آموزش، مخصوص بستر خاص یا جرم خاص نبوده و می‌تواند در خصوص هر نوع جرمی، در بستر سکوهای تجاری فناوری اطلاعات مورد استفاده قرار گیرد. انتشار آموزش‌هایی که افراد را به هک کردن، شنود یا تخریب داده‌ها ترغیب می‌کند، می‌تواند جرائم علیه سکوهای تجاری را افزایش دهد. مثلاً، آموزش آنلاین برای نفوذ به سیستم‌های بانکی می‌تواند افراد را به حمله به این سکوها تشویق کند. ماده ۷۵۳ با جرم‌انگاری انتشار چنین محتوایی، از گسترش دانش مجرمانه جلوگیری کرده و امنیت سکوهای تجاری را تقویت می‌کند.

- ممانعت از بازار سیاه داده‌های دسترسی

سکوها بستر تعامل مجازی دوسویه یا چند سویه، میان کاربران را ایجاد کرده و بدین‌وسیله، زمینه تبادل مستمر و سریع اطلاعات را میان آن‌ها مهیا می‌سازند (Rai et al., 2006: 227; Tan et al., 2015: 250). این موضوع می‌تواند در ایجاد بازارهای سیاه داده‌های دسترسی، مؤثر واقع شود. فروش گزرواژه‌ها یا اطلاعات ورود به سامانه‌ها، می‌تواند دسترسی غیرمجاز به سکوهای تجاری را تسهیل کند.

1. Platform Enabled-Cimes

2. Reddit

3. Dark Web

برای مثال، فروش اطلاعات ورود به پِنل مدیریت یک پلتفرم تجارت الکترونیک، امکان دستکاری داده‌ها یا سرقت اطلاعات کاربران را فراهم می‌کند. ماده ۷۵۳ با جرم‌انگاری این رفتار، از شکل‌گیری بازار سیاه داده‌های دسترسی جلوگیری می‌کند و امنیت این سکوها را تضمین می‌کند.

۱-۲. قانون مبارزه با تأمین مالی تروریسم مصوب ۱۳۹۴

دسترسی به منابع مالی، از عناصر کلیدی در تحقق اقدامات تروریستی به شمار می‌رود و نقش حیاتی این منابع، در شکل‌گیری و تداوم فعالیت سازمان‌های تروریستی، ضرورت اتخاذ تدابیر پیشگیرانه نسبت به ابزارهای مالی مورد استفاده آن‌ها را آشکار می‌سازد (صبوری پور و علی پور، ۱۳۹۷: ۱۲۵). به همین دلیل، پیشگیری از تأمین مالی آن‌ها چه از طریق سکوهایی تجاری و چه روش‌های دیگر مدنظر سیاست‌گذاران کشور ایران قرار گرفته است. هرچند قانون صراحتاً از «سکوها» نام نبرده، اما عبارات کلی درباره فعالیت‌های اقتصادی، مالی و الکترونیکی به‌گونه‌ای تنظیم شده‌اند که امکان تطبیق کامل با جرائم فناوری محور را دارند.

در ماده ۱ این قانون، تعریف تأمین مالی تروریسم، به‌گونه‌ای تنظیم شده که شامل «هرگونه فعالیت اقتصادی» ازجمله انتقال پول، خریدوفروش اوراق مالی و اعتباری، افتتاح حساب، تأمین اعتبار و ... می‌شود. این فعالیت‌ها ممکن است، از طریق سکوهایی فناوری اطلاعات مانند کیف پول‌های دیجیتال، درگاه‌های پرداخت، رمز ارزها، صرافی‌های آنلاین و ... انجام شوند؛ بنابراین، هرگونه استفاده از پلتفرم‌های مالی دیجیتال برای حمایت مالی از تروریسم، مشمول این ماده خواهد بود. تدبیر مندرج در ماده ۱ قانون مبارزه با تأمین مالی تروریسم، با ارائه تعریف گسترده‌ای از تأمین مالی تروریسم که شامل «هرگونه فعالیت اقتصادی» از طریق سکوهایی فناوری اطلاعات مانند کیف پول‌های دیجیتال، درگاه‌های پرداخت، رمز ارزها و صرافی‌های آنلاین می‌شود، ذیل پیشگیری وضعی طبقه‌بندی می‌شود. این ماده با ایجاد چارچوب قانونی جامع، محیط دیجیتال را به‌گونه‌ای تنظیم می‌کند که فرصت‌های استفاده از این سکوها برای اهداف مجرمانه مانند حمایت مالی از تروریسم محدود شود. با شناسایی و پوشش فعالیت‌های اقتصادی دیجیتال، این مقرره موانع قانونی و فنی را برای کاهش دسترسی به ابزارهای مالی در راستای ارتکاب جرم ایجاد می‌کند.

ماده ۵ این قانون، به الزام مراجع قضائی و ضابطان دادگستری به شناسایی، کشف و مسدود کردن وجوه و اموال ناشی از جرائم تأمین مالی تروریسم اشاره کرده است. توقیف اموال دیجیتال یا تغییر یافته (مثلاً رمز ارزها، NFT ها یا دارایی‌هایی که از طریق فناوری اطلاعات منتقل یا تبدیل شده‌اند) مشمول این ماده می‌شود. این ماده، ابزار قانونی لازم برای توقیف دارایی‌های دیجیتال در سکوهایی

فناوری اطلاعات را فراهم می‌کند. تبصره این ماده نیز به سکوهای تجاری اجازه می‌دهد که در شرایط اضطراری، دارایی مشکوک کاربران را موقتاً مسدود کنند. این اقدام پیشگیرانه، می‌تواند مانع از وقوع تراکنش‌های خطرناک شود. تدابیر مندرج در ماده ۵ قانون مبارزه با تأمین مالی تروریسم که مراجع قضایی و ضابطان دادگستری را به شناسایی، کشف و مسدود کردن وجوه و اموال ناشی از جرائم تأمین مالی تروریسم ملزم می‌کند و شامل توقیف اموال دیجیتال مانند رمز ارزها و NFT ها می‌شود و همچنین تبصره آن که به سکوهای تجاری، اجازه مسدود سازی موقت دارایی‌های مشکوک در شرایط اضطراری را می‌دهد، ذیل پیشگیری ثانویه و پیشگیری وضعی طبقه‌بندی می‌شود.

به موجب مقرر ماده ۱۳ این قانون، تمام اشخاص و نهادهای مشمول قانون مبارزه با پول‌شویی (از جمله سکوهای مالی دیجیتال) موظف به شناسایی مشتریان، نگهداری سوابق مالی و گزارش فعالیت‌های مشکوک هستند. این ماده، به‌ویژه در مورد سکوهایی که خدمات پرداخت یا خرید و فروش ارز دیجیتال ارائه می‌دهند، کاربرد مستقیم دارد. این ماده نیز ذیل پیشگیری وضعی قابل بررسی است.

ماده ۱۴ این قانون نیز از طریق الزام به گزارش عملیات مشکوک به تأمین مالی تروریسم به شورای عالی مبارزه با پول‌شویی، می‌تواند در پیشگیری از جرم مؤثر و مفید واقع شود. این تکلیف، به وضوح شامل سکوهای فناوری اطلاعاتی که عملیات مالی انجام می‌دهند نیز می‌شود. این ماده، علاوه بر پیشگیری وضعی، درصدد پیشگیری اجتماعی از طریق تقویت مسئولیت‌پذیری اجتماعی و همکاری نهادی است.

در قانون مبارزه با تأمین مالی تروریسم، اگرچه هدف اصلی مقابله با وقوع جرم است، اما در برخی مواد، احکامی آمده که دارای ماهیت پیشگیرانه هستند؛ به‌ویژه در خصوص سکوهای تجاری فناوری اطلاعات که امکان استفاده از آن‌ها برای انتقال غیرقانونی وجوه یا حمایت مالی از تروریسم وجود دارد.

۱-۳. قانون مبارزه با پول‌شویی مصوب ۱۳۸۶

در قانون مبارزه با پول‌شویی نیز رگه‌هایی از مقررات پیشگیرانه قابل استفاده در خصوص پیشگیری از فعالیت‌های مجرمانه سکوهای تجاری فناوری اطلاعات در بستر سایر ملاحظه می‌شود. به موجب ماده ۷ این قانون، اشخاص مشمول این قانون با احراز هویت کاربران (بند الف)، گزارش دهی تراکنش‌های مشکوک (بند پ)، نگهداری سوابق تراکنش‌ها به مدت حداقل پنج سال (بند ت) و آموزش و کنترل داخلی (بند ث) می‌توانند به پیشگیری از جرم کمک کنند. فلذا پلتفرم‌ها باید سیستم‌های شناسایی مشتری (KYC)^۱، ضد پول‌شویی (AML)^۲ و گزارش دهی را

فعال کنند. نتیجه برخی از پژوهش‌ها نشان می‌دهد که کاربست فناوری اطلاعات در نظام بانکداری الکترونیکی ایران و استفاده از سامانه‌های پرداخت مجهز به روش‌های کنترلی، احراز هویت، تعیین سطح فعالیت اشخاص، طبقه‌بندی اشخاص و روابط کارگزاری با سایر بانک‌ها در پیشگیری از جرم پول‌شویی در سکوهای تجاری و در حالت کلی بانک‌ها را به حداقل خواهد رساند (حسینی و آذری متین، ۱۳۹۴: ۱۳۶-۱۳۵). این تدابیر نیز در قالب پیشگیری وضعی و پیشگیری اجتماعی قابل بررسی است. این تدابیر از این منظر وضعی محسوب می‌شوند که با ایجاد موانع فنی و نظارتی، مانند احراز هویت کاربران، نگهداری سوابق تراکنش‌ها و استفاده از سامانه‌های پرداخت مجهز به روش‌های کنترلی، فرصت‌های ارتکاب جرم پول‌شویی در سکوهای تجاری فناوری اطلاعات را کاهش می‌دهند. همچنین علت اجتماعی محسوب شدن آن‌ها، این است که بندهایی مانند آموزش و کنترل داخلی (بند ث) و گزارش دهی تراکنش‌های مشکوک (بند پ) به تقویت مسئولیت‌پذیری و فرهنگ نظارت در میان سکوهای تجاری و نهادهای مالی کمک می‌کنند. این اقدامات، با ترویج همکاری نهادی و آگاهی بخشی به کارکنان و مدیران سکوها، هنجارهای اجتماعی مثبت را در اکوسیستم مالی تقویت می‌کنند که مشخصه پیشگیری اجتماعی است. آموزش کارکنان و ایجاد سیستم‌های کنترل داخلی، ظرفیت نهادها را برای پیشگیری از جرم ارتقا می‌دهد و مشارکت فعال آن‌ها را در شبکه نظارتی ترویج می‌کند.

۲. تدابیر پیشگیرانه در مقررات غیر کیفری

به جز قوانین کیفری، تدابیر پیشگیرانه در سایر قوانین از جمله قانون پیشگیری از وقوع جرم نیز به چشم می‌خورند. هرچند در برخی از این قوانین، همچون قانون حمایت از اطفال و نوجوانان و یا قانون صدور چک، برخی مقررات کیفری نیز به چشم می‌خورد، اما این قوانین صرفاً با هدف هنجار گذاری در حیطه حقوق کیفری تصویب نشده‌اند. فلذا، تدابیر پیشگیرانه مذکور در این قوانین به صورت مجزا مورد بحث و بررسی قرار خواهد گرفت. مصوبات شورای عالی فضای مجازی را نیز می‌توان در زمره همین دسته مورد بررسی قرار داد.

۲-۱. تدابیر پیشگیرانه در قانون پیشگیری از وقوع جرم مصوب ۱۳۹۴

یکی از مهم‌ترین ابزارهای قانونی در پیشگیری از جرائم و آسیب‌های اجتماعی، استفاده از ظرفیت‌های قانونی به منظور تعیین تدابیر و اجرایی کردن آن‌ها در سطح جامعه توسط ارگان‌های مختلف است (حسینی، ۱۳۹۸: ۲۳). شاید معروف‌ترین قانونی که در این خصوص می‌توان به آن اشاره داشت، قانون

پیشگیری از وقوع جرم است. در ماده ۱ این قانون، مقرر شده است: «پیشگیری از وقوع جرم عبارت است از پیش‌بینی، شناسایی و ارزیابی خطر وقوع جرم و اتخاذ تدابیر و اقدامات لازم برای از میان بردن یا کاهش آن.» ماده ۲ این قانون، اعضای شورای عالی پیشگیری از وقوع جرم را مشخص کرده است. ماده ۳ این قانون، وظایف شورای عالی پیشگیری از جرم را معین کرده است که یکی از وظایف آن را سیاست‌گذاری در قبال پیشگیری از جرم بیان کرده است. در ماده ۴ بیان شده است که این شورا می‌تواند مصوباتی نیز داشته باشد و پس از امضای سران سه قوه به موقع اجرا گذارده شوند. این قانون با شش ماده به اتمام می‌رسد.

با توجه به متن قانون پیشگیری از وقوع جرم، تدابیر پیش‌بینی شده در این قانون، می‌توانند به شکل‌های مختلفی موجب پیشگیری از وقوع جرم در سکوها تجاری فناوری اطلاعات در بستر فضای مجازی شوند؛ هم از جانب خود سکوها و هم از جانب کاربران آن‌ها. این تدابیر، با هدف کاهش خطر وقوع جرم و ایجاد محیطی امن‌تر برای فعالیت‌های تجاری آنلاین طراحی شده‌اند.

در خصوص تدابیر قانونی برای پیشگیری از جرم توسط خود سکوها تجاری، می‌توان اذعان داشت قانون پیشگیری از وقوع جرم با الزام سکوها به اتخاذ تدابیر امنیتی و نظارتی، می‌تواند از وقوع جرائمی مانند کلاهبرداری، نقض داده‌ها و توزیع محتوای غیرقانونی جلوگیری کند. این جلوگیری می‌تواند از سه طریق پیش‌بینی و شناسایی خطرات، اتخاذ تدابیر امنیتی و همکاری با شورای عالی پیشگیری از جرم محقق شود. در راستای پیش‌بینی و شناسایی خطرات که در قانون پیش‌بینی شده است، سکوها می‌توانند پس از وضع مصوبه شورا، با استفاده از ابزارهای تحلیلی و هوش مصنوعی، الگوهای مشکوک را شناسایی کرده و از وقوع جرائم پیشگیری کنند. برای مثال، سیستم‌های تشخیص تقلب می‌توانند تراکنش‌های مشکوک را قبل از تأیید متوقف کنند. در راستای اتخاذ تدابیر امنیتی، قانون می‌تواند سکوها را ملزم به پیاده‌سازی پروتکل‌های امنیتی پیشرفته مانند رمزنگاری داده‌ها، احراز هویت چندمرحله‌ای و نظارت مداوم بر فعالیت‌های کاربران کند. این تدابیر از دسترسی غیرمجاز به اطلاعات حساس، جلوگیری می‌کنند. همچنین شورای عالی پیشگیری از جرم، می‌تواند سیاست‌هایی را برای سکوها تجاری تدوین کند که شامل الزام به انجام ممیزی‌های امنیتی دوره‌ای، رعایت استانداردهای بین‌المللی حفاظت از داده‌ها و گزارش دهی سریع در صورت بروز حادثه باشد. این سیاست‌ها می‌توانند به‌عنوان یک چارچوب قانونی برای سکوها عمل کنند. به‌عنوان مثال، یک سکوی تجاری می‌تواند با پیاده‌سازی سیستم‌های پالایش محتوا، از انتشار محتوای غیرقانونی مانند کالاهای تقلبی یا تبلیغات گمراه‌کننده جلوگیری کند. همچنین، الزام به تأیید هویت فروشندگان می‌تواند از فعالیت‌های کلاهبردانه پیشگیری کند.

کاربران سکویهای تجاری نیز می‌توانند مرتکب جرائمی مانند کلاهبرداری، سرقت هویت یا سوءاستفاده از اطلاعات شوند. قانون پیشگیری از وقوع جرم با تمرکز بر آموزش، آگاهی‌بخشی و تعیین مجازات بازدارنده، می‌تواند رفتار کاربران را تحت تأثیر قرار دهد. مصوبات شورای عالی پیشگیری از جرم می‌تواند سکوها را ملزم به ارائه منابع آموزشی برای کاربران کند تا آن‌ها را در مورد روش‌های ایمن استفاده از پلتفرم، تشخیص کلاهبرداری‌ها و حفاظت از اطلاعات شخصی آگاه سازد. این امر می‌تواند از افتادن کاربران در دام جرائم سایبری جلوگیری کند. از طرفی، سکوها می‌توانند با ایجاد مکانیسم‌های ساده برای گزارش فعالیت‌های مشکوک توسط کاربران، به شناسایی و پیشگیری از جرائم کمک کنند. مصوبات می‌توانند سکوها را ملزم به همکاری با مقامات قضایی، در صورت گزارش جرائم کند. به عنوان مثال، یک کاربر که قصد خرید آنلاین دارد، با دریافت آموزش‌های لازم در مورد نحوه تشخیص وبسایت‌های معتبر و روش‌های پرداخت امن، کمتر در معرض خطر کلاهبرداری قرار می‌گیرد. همچنین، وجود مجازات قانونی برای کاربرانی که از اطلاعات کارت اعتباری دیگران سوءاستفاده می‌کنند، می‌تواند از ارتکاب چنین جرائمی جلوگیری کند.

شورای عالی پیشگیری از جرم که در قانون ذکر شده است، می‌تواند با سیاست‌گذاری و تدوین مقررات، نقش مهمی در پیشگیری از جرائم در سکویهای تجاری ایفا کند. از زمره این مصوبات می‌توان به مصوبه شورای عالی فضای مجازی در خصوص صیانت از کودکان و نوجوانان در فضای مجازی مورخ ۱۴۰۰/۴/۲۳ اشاره داشت. این مصوبه مجموعه‌ای از تدابیر حمایتی، آموزشی و نظارتی را به منظور کاهش خطرات بزهکاری در فضای مجازی پیش‌بینی کرده است. مصوبه شورای عالی فضای مجازی در خصوص صیانت از کودکان و نوجوانان، مقرراتی مشخص برای مقابله با فعالیت‌های مجرمانه سکویهای تجاری فناوری اطلاعات وضع کرده است که عمدتاً برپایه الزامات فنی، حقوقی و نظارتی استوار است. بر اساس ماده ۴-۶، کلیه سکوها و ارائه دهندگان محتوا و خدمات فضای مجازی مرتبط با کودکان و نوجوانان ملزم به ارائه خدمات خود در بستر محیط صیانت شده ظرف مدت یک سال هستند که این امر به عنوان یک الزام قانونی، فرصت‌های مجرمانه مانند توزیع محتوای مضر را محدود می‌کند و در چارچوب پیشگیری وضعی قرار می‌گیرد، زیرا محیط دیجیتال را طوری طراحی می‌کند که فرصت‌های ارتکاب جرم را کاهش دهد. همچنین، ماده ۴-۱۱ سکوها را ملزم به نظارت بر محتوا، صیانت از داده‌ها، رده‌بندی خدمات بر اساس سن و جلوگیری از افشای غیرمجاز اطلاعات کودکان می‌کند که این مقررات با ایجاد موانع فنی و حقوقی، از بهره‌برداری مجرمانه مانند سوءاستفاده از داده‌های

شخصی یا تبلیغات ناهنجار جلوگیری کرده و به پیشگیری اولیه کمک می‌کند، زیرا پیش از وقوع جرم، سازوکارهای پیشگیرانه را تحمیل می‌کند. در بخش قضایی و انتظامی، مصوبه بر تشدید مقابله با مجرمان تمرکز دارد؛ ماده ۳-۵ بر تشدید مقابله قضایی و انتظامی با بزه‌کاران و تهدیدکنندگان امنیت کودکان در فضای مجازی تأکید می‌کند که این سیاست کلان، سکوهای تجاری را به‌عنوان بخشی از زنجیره مسئولیت تحت فشار قرار می‌دهد تا از میزبانی محتوای مجرمانه خودداری کنند. این مقررات در قالب پیشگیری ثانویه گنجانده می‌شود، زیرا بر مداخله سریع پس از شناسایی تهدیدها و حمایت از قربانیان تمرکز دارد و با ماده ۴-۹ همخوانی دارد که راه‌اندازی خط تماس اضطراری برای جرائم علیه کودکان را الزامی می‌کند و سکوها را موظف به همکاری با مراجع انتظامی می‌کند. علاوه بر این، ماده ۴-۱۰ با تقویت دفتر حمایت از اطفال و نوجوانان قوه قضائیه، سکوها را در شناسایی و مقابله با جرائم مانند سوءاستفاده در تبلیغات ملزم به همکاری می‌کند که این رویکرد ترکیبی از پیشگیری وضعی و اجتماعی است، زیرا هم محیط را ایمن می‌سازد و هم مسئولیت اجتماعی سکوها را افزایش می‌دهد.

از منظر پیشگیری رشد مدار و اجتماعی، مصوبه بر توانمندسازی و مشارکت سکوهای غیردولتی تأکید دارد؛ ماده ۳-۴ بخش غیردولتی را به ارائه محتوای سالم تشویق و از ارائه محتوای مضر پیشگیری می‌کند که سکوهای تجاری را به سمت تولید خدمات ایمن هدایت می‌کند و در پیشگیری اجتماعی نقش ایفا می‌کند، زیرا تغییرات فرهنگی و مشارکتی را ترویج می‌دهد. ماده ۳-۱۰ نیز با ایجاد سازوکارهای فنی و قانونی سلامت محتوا، سکوها را ملزم به پیشگیری از مخاطرات می‌کند که این امر با توسعه مهارت‌های کودکان از طریق محتوای رد‌بندی شده (ماده ۳-۳) هم‌راستا است و به پیشگیری رشد مدار کمک می‌رساند، زیرا رشد سالم کاربران جوان را در برابر جرائم سایبری مقاوم می‌سازد. در مجموع، این مقررات ترکیبی از اقسام پیشگیری را پوشش می‌دهد و سکوهای تجاری را به‌عنوان بازیگران کلیدی در اکوسیستم صیانت قرار می‌دهد.

۲-۲. تدابیر پیشگیرانه در قانون تجارت الکترونیکی مصوب ۱۳۸۲

در کنار قوانین یادشده، قانون تجارت الکترونیکی نیز باید به‌عنوان بخشی از سیاست‌های پیشگیرانه در برابر فعالیت‌های مجرمانه سکوهای تجاری در حوزه فناوری اطلاعات مدنظر قرار گیرد. قانون تجارت الکترونیکی مصوب ۱۳۸۲ به‌عنوان یکی از پایه‌های مهم در تنظیم فعالیت‌های اقتصادی در بستر فضای مجازی، دارای احکامی است که ضمن تسهیل مبادلات تجاری، می‌تواند در راستای پیشگیری از جرائم نیز تفسیر و به کار گرفته شوند. برخی از این مقررات، گرچه صراحتاً ماهیت کیفری ندارند، اما از طریق ایجاد الزامات شفاف،

سازوکارهای کنترل و حمایت از مصرف کننده، نقش مؤثری در پیشگیری غیر کیفری از فعالیت‌های مجرمانه دارند. در باب سوم قانون تجارت الکترونیکی به‌ویژه در فصل حمایت از مصرف کننده (مواد ۳۳ تا ۴۵)، مقرراتی وضع شده‌اند که سکوهای تجاری را ملزم می‌سازند اطلاعات دقیق، شفاف و صحیح از کالاها، خدمات، هویت تأمین کننده، نحوه پرداخت، شرایط فسخ معامله و تضمین‌های پس از فروش در اختیار کاربران قرار دهند. این شفاف‌سازی اطلاعات، به‌عنوان یک تدبیر پیشگیرانه، احتمال بروز جرائمی مانند کلاهبرداری اینترنتی، تبلیغات فریبده یا فروش کالای تقلبی را کاهش می‌دهد و اعتماد کاربران را تقویت می‌کند. این مقررات ذیل پیشگیری وضعی قرار می‌گیرد، زیرا با الزام سکوهای تجاری به ارائه اطلاعات شفاف و دقیق، فرصت‌های ارتکاب جرائمی مانند کلاهبرداری و تبلیغات فریبده را از طریق کاهش ابهام و افزایش نظارت‌پذیری محدود می‌کند.

همچنین، فصل حمایت از داده‌های شخصی (مواد ۵۸ تا ۶۱) با تعیین اصولی برای نحوه جمع‌آوری، پردازش و ذخیره‌سازی اطلاعات، ازجمله ضرورت اخذ رضایت صریح کاربران، محدودیت در هدف استفاده و امکان دسترسی و اصلاح داده‌ها توسط افراد، بستری قانونی برای پیشگیری از جرائمی چون سوءاستفاده از اطلاعات خصوصی، سرقت هویت و نقض حریم خصوصی فراهم کرده است. مقررات این فصل ذیل پیشگیری وضعی قرار می‌گیرد، زیرا با وضع الزامات قانونی برای جمع‌آوری، پردازش و ذخیره‌سازی داده‌ها و اخذ رضایت صریح کاربران، فرصت‌های ارتکاب جرائمی مانند سوءاستفاده از اطلاعات خصوصی و سرقت هویت را از طریق محدودسازی دسترسی غیرمجاز و افزایش شفافیت کاهش می‌دهد. این تدابیر با ایجاد موانع قانونی و فنی، محیط دیجیتال را برای پیشگیری از نقض حریم خصوصی ایمن‌تر می‌کنند.

در کنار این موارد، مقررات مربوط به تبلیغات (مواد ۵۰ تا ۵۷) نیز با ممنوع سازی تبلیغات گمراه کننده، الزام به افشای دقیق هویت و هدف تبلیغ و لزوم رعایت حقوق کاربران (ازجمله عدم ارسال ناخواسته تبلیغات)، از سوءاستفاده‌های رایج در سکوهای تجاری جلوگیری می‌کنند. این مقررات نیز ذیل پیشگیری وضعی قرار می‌گیرد، زیرا با ممنوعیت تبلیغات گمراه کننده و الزام به شفافیت و رعایت حقوق کاربران، فرصت‌های سوءاستفاده و فریب در سکوهای تجاری را از طریق ایجاد موانع قانونی و نظارتی کاهش می‌دهد.

درمجموع، قانون تجارت الکترونیکی، از طریق ایجاد چهارچوب‌های شفاف، الزامات اطلاعاتی، حمایت از داده‌های شخصی و حقوق مصرف کنندگان، به‌طور ضمنی دارای ظرفیت‌های قابل‌توجهی برای پیشگیری غیر کیفری از جرائم سایبری در سکوهای فناوری اطلاعات است. این قانون، به‌ویژه با تأکید بر رویه‌های ایمن، امضای الکترونیکی مطمئن و اسناد دیجیتال معتبر (مواد ۱۰ تا

(۱۶)، همچنین با گسترش اعتماد عمومی به معاملات آنلاین، نقشی بنیادین در سیاست‌گذاری جنایی پیشگیرانه وضعی مدرن ایفا می‌کند.

۲-۳. تدابیر پیشگیرانه قانون صدور چک

در خصوص نقش تدابیر غیر کیفری قانون صدور چک در پیشگیری از جرائم سکوهای تجاری فناوری اطلاعات، می‌توان بیان داشت: در بستر سکوهای تجاری فناوری اطلاعات، چک به‌عنوان یکی از ابزارهای رایج پرداخت، همچنان نقش کلیدی در مبادلات مالی ایفا می‌کند. با افزایش دیجیتالی شدن خدمات بانکی، استفاده از چک‌های الکترونیکی نیز گسترش یافته است. قانون صدور چک، به‌ویژه در اصلاحات سال ۱۳۹۷، گام‌های مهمی در جهت شفاف‌سازی، ردیابی، اعتبارسنجی و نظارت سیستمی بر فرآیند صدور و وصول چک برداشته که می‌توان آن‌ها را در زمره تدابیر غیر کیفری مؤثر در پیشگیری از جرائم مالی و سایبری در فضای مجازی دانست.

۲-۳-۱. کنترل سیستمی و پیشگیری وضعی از طریق سامانه صیاد

ماده ۲۱ مکرر قانون، الزام به صدور چک صرفاً از طریق سامانه صیاد (صدور یکپارچه الکترونیکی دسته‌چک) را پیش‌بینی کرده است. این سامانه با ثبت هویت صادر کننده، گیرنده، مبلغ و تاریخ چک و تخصیص شناسه یکتا به هر برگ، مانع از جعل، سوءاستفاده یا انتقال غیرمجاز چک می‌شود. همچنین، امکان رصد و گزارش‌گیری نهادهای قضایی و بانکی از سامانه، ابزاری مهم در پیشگیری از پول‌شویی، کلاهبرداری و سایر جرائم مالی در سکوهای دیجیتال به شمار می‌رود. مقرر به پیش‌گفته، به‌عنوان پیشگیری وضعی طبقه‌بندی می‌شود زیرا تمرکز اصلی آن بر کاهش فرصت‌های ارتکاب جرم از طریق تغییرات ساختاری و فنی در محیط صدور و گردش چک است، نه بر تغییر رفتار یا انگیزه‌های مجرمان بالقوه.

۲-۳-۲. محدودیت‌های بانکی بازدارنده برای متخلفان

مطابق با ماده ۵ مکرر، چنانچه چکی برگشت بخورد و رفع سوء اثر نشود، بانک مرکزی موظف است محدودیت‌هایی از جمله ممنوعیت افتتاح حساب جدید، مسدودی حساب‌ها، عدم صدور کارت‌بانکی و جلوگیری از اعطای تسهیلات بانکی را اعمال کند. این محدودیت‌ها جنبه بازدارنده غیر کیفری دارند و بدون ورود به فرایند قضایی، صادر کننده متخلف را با پیامدهای فوری مواجه می‌کنند. این مقرر به نیز به‌عنوان پیشگیری وضعی طبقه‌بندی می‌شود. این رویکرد بر کاهش فرصت‌های ارتکاب جرائم مالی آینده از طریق تغییرات ساختاری در محیط بانکی تمرکز دارد، نه بر مجازات کیفری یا تغییر عوامل اجتماعی.

۲-۳-۳. ابزارهای احراز هویت و اعتبار سنجی

طبق ماده ۶، پیش از صدور چک باید اطلاعات هویتی و اعتبار سنجی متقاضی از سامانه‌های مربوط استعلام شود. همچنین بندهای مختلف ماده ۲۱ بر استفاده از داده‌های اعتباری (مانند رتبه اعتباری، سابقه چک برگشتی، تعهدات مالی جاری) برای تخصیص سقف صدور چک تأکید دارند. این مکانیسم‌ها با هدف پیش‌بینی و کاهش ریسک سوءاستفاده از چک، به‌ویژه در بستر سکوهای فناوری محور، طراحی شده‌اند. از آنجا که این مکانیسم‌ها با تغییر شرایط محیطی و ایجاد محدودیت‌های ساختاری در فرآیند صدور چک، فرصت‌های سوءاستفاده و جرائم مالی را کاهش می‌دهند، باید آن‌ها را در زمره پیشگیری وضعی طبقه‌بندی کرد.

۲-۳-۴. گسترش شفافیت و ردیابی معاملات مالی

الزام به ثبت اطلاعات دارنده چک در سامانه صیاد و ممنوعیت پشت‌نویسی چک در وجه حامل، به‌موجب تبصره ماده ۲۱ مکرر، امکان ردگیری مسیر چک و نظارت بر جریان وجوه را فراهم می‌سازد. این شفافیت، زمینه وقوع بزه‌هایی چون فرار مالیاتی، پول‌شویی، فروش مال غیر و فریب تجاری را کاهش می‌دهد. به همین دلیل پیشگیری نیز از زمره پیشگیری‌های وضعی محسوب می‌شود.

۲-۳-۵. جایگزینی سازوکارهای مالی در بستر دیجیتال

تبصره ۲ ماده ۶ اشاره دارد که بانک مرکزی موظف است زیرساخت «چک موردی» را بدون نیاز به دسته‌چک فراهم کند. این اقدام، ضمن کاهش تقاضای صدور دسته‌چک (که گاهی برای مقاصد متقلبانه استفاده می‌شود)، به کنترل و نظارت مؤثرتر بر تراکنش‌های مالی دیجیتال در سکوهای تجاری می‌انجامد. درمجموع، قانون صدور چک با استفاده از فناوری‌های اطلاعاتی و ابزارهای نظارتی غیر قضایی، به‌ویژه از طریق سامانه‌های الکترونیکی و محدودیت‌های سیستمی، چارچوبی منسجم برای پیشگیری غیر کیفری از جرائم مالی در بستر سکوهای تجاری فناوری اطلاعات فراهم کرده است. این قانون با کاهش فرصت‌های جرم، افزایش شفافیت و مسئولیت‌پذیری و تسهیل در شناسایی متخلفان، به یکی از ارکان مهم سیاست جنایی پیشگیرانه در حوزه تجارت الکترونیک بدل شده است.

۲-۴. تدابیر پیشگیرانه در قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹

قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹، با هدف صیانت از حقوق افراد زیر هجده سال، دارای مجموعه‌ای از مقررات حمایتی و نظارتی است که می‌توانند به‌طور مؤثری در راستای پیشگیری غیر کیفری از وقوع جرائم در بستر سکوهای تجاری فناوری اطلاعات به کار گرفته شوند. این قانون با تمرکز

بر حفاظت از کودکان در برابر بهره‌کشی، سوءاستفاده جنسی، محتوای مبتذل و شرایط مخاطره‌آمیز، نقشی کلیدی در تقویت مسئولیت اجتماعی پلتفرم‌ها ایفا می‌کند.

۲-۴-۱. پیشگیری از نمایش محتوای مجرمانه نسبت به کودکان

مطابق ماده ۱۰ قانون، عرضه هرگونه محتوای مستهجن یا مبتذل به طفل یا نوجوان، جرم محسوب می‌شود. این مقرره، مبنایی برای الزام سکوهاى تجارى فناوری اطلاعات به پالایش محتوای غیرقانونی به‌ویژه در حوزه تبلیغات، فروش بازی‌ها، ویدئوها یا کتاب‌های دیجیتال است. پلتفرم‌هایی که دسترسی آزادانه کودکان به چنین محتوایی را فراهم می‌کنند، نه تنها مسئولیت مدنی، بلکه در معرض پیگرد کیفری نیز قرار می‌گیرند.

۲-۴-۲. مسئولیت سکوها در جلوگیری از هرزه‌نگاری کودکان و بهره‌کشی جنسی دیجیتال

مواد ۱۰ و ۱۱ قانون با جرم‌انگاری بهره‌کشی جنسی، تهیه و انتشار آثار هرزه‌نگارانه و سوءاستفاده از کودکان برای تولید محتوای جنسی، سکوهاى دیجیتال را مکلف به کنترل سخت‌گیرانه فعالیت‌های کاربران و فروشندگان می‌کنند. به‌ویژه، پلتفرم‌هایی که میزبان فایل‌های تصویری یا خدمات بارگذاری هستند، باید مکانیسم‌های خودکار تشخیص و مسدودسازی محتوای غیرقانونی را به کار گیرند.

۲-۴-۳. پیش‌بینی خطر و گزارش‌پذیری کاربران

در ماده ۱۷، قانون‌گذار هر شخص مطلع از وقوع یا شروع جرائم علیه اطفال را موظف به گزارش آن دانسته است. این حکم به سکوهاى تجارى نیز قابل تسرى است؛ به این معنا که باید سازوکاری برای گزارش محرمانه فعالیت‌های مشکوک کاربران در پلتفرم (مانند فروش کودکان، پیشنهادهای جنسی یا آگهی‌های مخرب) فراهم شود.

۲-۴-۴. مداخله فوری و پیشگیرانه نهادهای حمایتی

مواد ۵، ۳۳ و ۳۵ این قانون، امکان مداخله فوری دفاتر حمایت از اطفال و نوجوانان قوه قضائیه و سازمان بهزیستی را در موارد تهدیدآمیز فراهم می‌سازد. چنانچه سکوها در معرض انتشار یا تسهیل دسترسی به محتوایی باشند که طفل یا نوجوانی را در وضعیت خطر قرار دهد، امکان صدور دستور قضایی برای حذف محتوا یا محدودسازی حساب کاربری وجود دارد.

۲-۴-۵. آموزش، آگاهی و نظارت مستمر

طبق ماده ۴۳، قاضی می‌تواند والدین، سرپرستان و مدیران پلتفرم‌ها را به گذراندن دوره‌های آموزشی در خصوص حقوق کودکان ملزم کند. همچنین ماده ۴۴ استفاده از مددکاران اجتماعی برای نظارت بر اقدامات پلتفرم‌ها و دستگاه‌ها را تجویز کرده است. این نظارت می‌تواند شامل بررسی چگونگی پالایش محتوا، بررسی الگوریتم‌های پیشنهاددهی و رعایت رده‌بندی سنی در فروشگاه‌های آنلاین باشد.

در مجموع، قانون حمایت از اطفال و نوجوانان با توجه به ماهیت حمایتی خود، ظرفیت‌های مهمی در پیشگیری غیر کیفری از جرائم مرتبط با کودکان در فضای مجازی و سکوهای تجاری فناوری اطلاعات دارد. از طریق الزام به پالایش محتوا، ممانعت از بهره‌کشی، ایجاد سامانه‌های گزارش دهی و گسترش نظارت، این قانون بستر مناسبی برای ارتقای ایمنی دیجیتال برای اقشار آسیب‌پذیر فراهم کرده است. اجرای مؤثر این مقررات می‌تواند به سالم‌سازی فضای فعالیت سکوهای تجاری، افزایش اعتماد کاربران و صیانت از حقوق بنیادین اطفال و نوجوانان منجر شود.

۲-۵. مصوبات شورای عالی فضای مجازی در خصوص پالایش

علاوه بر قوانین فوق‌الذکر، باید مصوبات شورای عالی فضای مجازی در خصوص پالایش (فیلترینگ) برخی از سکوهای فناوری اطلاعات - صرف‌نظر از ارزش‌گذاری اقدامات این شورا و ارزش‌گذاری بر ماهیت اقدام فیلترینگ- را باید به تدابیر پیشگیرانه افزود. بر اساس اطلاعات موجود، متن کامل مصوبه شورای عالی فضای مجازی در خصوص فیلترینگ فضای مجازی به‌صورت عمومی منتشر نشده است.

در ایران، فیلترینگ برخی از سکوهای تجاری فعال در حوزه فناوری اطلاعات و فضای مجازی، بر اساس مصوبات شورای عالی فضای مجازی و با هدف صیانت از فرهنگ عمومی، امنیت ملی و حمایت از کسب‌وکارهای بومی صورت می‌گیرد. این اقدامات معمولاً در چارچوب سیاست‌های کلان فضای مجازی کشور اتخاذ می‌شود و با استناد به تهدیدهای امنیتی، نقض مقررات داخلی، یا عدم همکاری این سکوها با نهادهای حاکمیتی در زمینه تبادل داده یا اجرای احکام قضایی، توجیه می‌شود. با این حال، این رویکرد با انتقادات حقوقی و اقتصادی روبروست؛ از جمله محدود شدن آزادی گردش اطلاعات، آسیب به فعالیت کسب‌وکارهای خرد و تأثیر منفی بر اعتماد عمومی.

فرجام سخن

با توجه به رشد فزاینده جرائم مبتنی بر فناوری اطلاعات و نقش فزاینده سکویهای تجاری دیجیتال در بروز و گسترش این جرائم، ارزیابی سیاست جنایی پیشگیرانه ایران در قبال این پدیده، امری ضروری به نظر می‌رسد. یافته‌های این پژوهش نشان داد که علی‌رغم برخی تلاش‌های تقنینی پراکنده در حوزه جرائم رایانه‌ای، پول‌شویی و حفاظت از داده‌ها، نظام حقوقی ایران در برابر جرائم پلتفرم محور نه‌تنها ناتوان از واکنش مؤثر است، بلکه حتی در طراحی سازوکارهای پیشگیرانه ساختاری، ناکارآمد و تأخیر زده عمل کرده است.

از مهمترین نشانه‌های ناکارآمدی سیاست جنایی پیشگیرانه ایران در این حوزه، می‌توان به موارد ذیل اشاره کرد:

- عدم پیش‌بینی مقررات روشن در خصوص تکالیف پلتفرم‌ها نسبت به پالایش محتوا و نظارت بر آن؛
 - فقدان مقرر ناظر به مسئولیت پلتفرم‌های بین‌المللی و قدرتمند که در بستر فضای مجازی ایران فعالیت می‌کنند؛
 - قدمت قوانین کیفری موجود و عدم انطباق آن‌ها با تحولات فناورانه و ساختارهای نوظهور جرم‌زا؛
 - تعدد و پراکندگی نهادهای سیاست‌گذار و فقدان نهاد واحد تخصصی در امر تنظیم‌گری فضای پلتفرمی؛
 - عدم قابلیت اجرایی قوانین در برابر سکویهای خارجی، حتی با استناد به مواد ۴ تا ۹ قانون مجازات اسلامی؛
 - واکنش‌های روان‌شناختی منفی در قبال تدابیر فیلترینگ؛ که خود به‌عنوان عامل تشدید کننده مخاطرات جرم خیز تلقی می‌شود.
- جهت تبیین دقیق‌تر دامنه و ضعف‌های موجود، در جدول زیر، اهم قوانین مؤثر در حوزه فناوری اطلاعات و تدابیر پیشگیرانه آن‌ها، همراه با ارزیابی میزان کارایی‌شان در مواجهه با جرائم پلتفرم محور ارائه شده است:

جدول ۱. بررسی قوانین و تدابیر پیشگیرانه مرتبط با سکویهای تجاری فناوری اطلاعات

نام قانون / مقرر	تدابیر پیشگیرانه صریح یا ضمنی	ارزیابی اثربخشی در قبال جرائم سکویهای فناوری اطلاعات
قانون جرائم رایانه‌ای	جرم‌انگاری جرائم رایانه‌ای، الزامات فنی، حمایت از داده‌ها	فاقد ابزارهای پیشگیرانه هوشمند؛ تمرکز بر پاسخ کیفری، عدم پوشش پلتفرم‌های پیچیده
قانون مجازات اسلامی (مصوب ۱۳۹۲، مواد ۴ تا ۹)	گسترش صلاحیت کیفری در جرائم دارای آثار فرامرزی	در عمل قابل‌اعمال بر پلتفرم‌های بین‌المللی نیست؛ اجرای خارجی ندارد
قانون تجارت الکترونیک	مقررات مربوط به امضای الکترونیکی، حفاظت از مصرف کننده	ناکارآمد در حوزه پیشگیری از بزهکاری پلتفرم محور؛ فاقد مسئولیت‌پذیری سکوها

نام قانون / مقرر	تدابیر پیشگیرانه صریح یا ضمنی	ارزیابی اثربخشی در قبال جرائم سکوهای فناوری اطلاعات
قانون مبارزه با پولشویی (مصوب ۱۳۸۶ و اصلاحی ۱۳۹۷)	گزارش دهی معاملات مشکوک، شفافیت مالی، کنترل منشأ پول	پژوهش‌ها (محمودی ۱۴۰۲) نشان داده‌اند فاقد تأثیر معنادار بر پیشگیری و کشف جرم منشأ است
آیین‌نامه اجرایی ماده ۱۴ قانون مبارزه با پولشویی (مصوب ۱۳۹۸)	تعریف اشخاص مشمول، نحوه گزارش دهی، سطح‌بندی ریسک	تدابیر ناکارآمد در فضای تراکنش‌های پلتفرمی؛ بدون پیوست فناوریانه اجرایی
آیین‌نامه‌ها و مصوبات کارگروه تعیین مصادیق مجرمانه	پالایش محتوا، فیلترینگ سایت‌های مجرمانه	سیاست واکنشی، اثر منفی روان‌شناختی (مقاومت واکنشی)، تقویت استفاده از فیلتر شکن
قانون تجارت الکترونیکی	امنیت تبادل داده، حمایت از مصرف‌کننده، امضای دیجیتال	فاقد الزامات کیفری و نظارتی برای پلتفرم‌ها؛ تأکید بر معاملات سنتی
قانون صدور چک (اصلاحی ۱۳۹۷)	اعتبارسنجی چک، سامانه صیاد، حذف چک حامل	ابزار مکمل در شفاف‌سازی تراکنش‌ها؛ اما ناکافی در فضای معاملات پلتفرمی جدید
قانون حمایت از اطفال و نوجوانان	جرم‌انگاری بهره‌مندی جنسی، مراقبت آنلاین، تکالیف والدین	فاقد ابزارهای نظارتی الزام‌آور برای پلتفرم‌های انتشار محتوا
مصوبات شورای عالی فضای مجازی در خصوص پالایش	فهرست مصادیق مجرمانه، فیلترینگ سایت‌های غیرمجاز	رویکرد واکنشی، بدون شفافیت فنی-حقوقی؛ افزایش مقاومت روانی کاربران و استفاده از فیلتر شکن

منبع: نگارندگان

مجموع این تحلیل‌ها، نشان می‌دهد که سیاست جنایی ایران عمدتاً رویکردی واکنشی، متفرق، قدیمی و ناکارآمد نسبت به بزهکاری پلتفرم محور اتخاذ کرده است. در چنین شرایطی، ضرورت بازطراحی سیاست جنایی پیشگیرانه با نگاه فناوریانه و پلتفرم محور کاملاً مشهود است. این سیاست‌گذاری نوین باید:

۱. با درک دقیق از ماهیت پلتفرم‌های دیجیتال و مدل‌های کسب‌وکار آن‌ها صورت گیرد؛
۲. بر مسئولیت کیفری و مدنی فعال برای پلتفرم‌ها در خصوص محتوای مجرمانه، تسهیلگری جرم و عدم همکاری با نهادهای حاکمیتی متمرکز باشد؛
۳. از سازوکارهای تنظیم‌گری نرم^۱، نظیر رتبه‌بندی اعتماد، شفافیت الگوریتمی و مشارکت جامعه مدنی بهره گیرد؛

۴. نهادی واحد و مستقل با صلاحیت تخصصی در حوزه تنظیم‌گری پلتفرم‌ها ایجاد شود؛
۵. به‌جای فیلترینگ صرف، با استفاده از سیاست‌های مبتنی بر داده، فناوری و مشارکت اجتماعی، تدابیر پیشگیرانه هوشمند تدوین و اجرا شود.
- بدون چنین بازنگری راهبردی، ادامه وضعیت موجود نه تنها مانعی بر سر راه پیشگیری از جرم در فضای پلتفرمی خواهد بود، بلکه مشروعیت و کارآمدی نظام عدالت کیفری را نیز با چالش‌های جدی مواجه خواهد ساخت.
- با توجه به یافته‌های پژوهش، پیشنهاد می‌شود قانون جرائم رایانه‌ای مصوب ۱۳۸۸ از طریق الحاق ماده‌ای نوین مورد اصلاح قرار گیرد تا مسئولیت کیفری پلتفرم‌های دیجیتال، نظیر سکوها، تجاری آنلاین، در برابر محتوای مجرمانه تولیدشده توسط کاربران - از جمله کلاهبرداری سایبری و پول‌شویی - به‌طور صریح و جامع تبیین شود. این ماده می‌تواند الزام به استقرار سیستم‌های مبتنی بر هوش مصنوعی برای تشخیص و حذف خودکار محتوای مشکوک را مقرر دارد، همراه با تحریم‌های مالی معادل تا ده برابر درآمد سالانه پلتفرم در صورت عدم پیروی که این امر به تقویت مکانیسم‌های پیشگیرانه قضایی- فنی کمک خواهد کرد. علاوه بر این، قانون تجارت الکترونیک مصوب ۱۳۸۲ نیازمند به‌روزرسانی از طریق افزودن فصلی اختصاصی است که مقررات عینی همچون رتبه‌بندی اعتباری کاربران بر پایه سابقه تراکنش‌ها، افشای شفاف الگوریتم‌های توصیه گر به‌منظور ممانعت از تبلیغ کالاهای جعلی و برقراری سازوکار گزارش دهی الزامی جرائم به پلیس فتا ظرف حداکثر ۲۴ ساعت را در برگیرد تا رویکرد پیش‌دستانه در پیشگیری از جرائم پلتفرمی ارتقا یابد.
- علاوه بر موارد فوق، توصیه می‌شود شورای عالی فضای مجازی، به‌عنوان نهاد اصلی سیاست‌گذاری، آیین‌نامه‌ای مستقل برای تأسیس یک نهاد نظارتی یکپارچه و متخصص - مانند کمیسیون تنظیم سکوها، دیجیتال - تدوین کند که مسئولیت‌هایی نظیر نظارت بر اجرای استانداردهای امنیتی (از قبیل رمزنگاری دوجانبه داده‌ها) و همکاری با شرکت‌های فناوری بین‌المللی برای مبادله اطلاعات جرائم فرامرزی را عهده‌دار باشد. این نهاد می‌تواند با بهره‌گیری از بودجه دولتی و مشارکت بخش خصوصی، برنامه‌های آموزشی عمومی برای کاربران سکوها را راه‌اندازی کند تا سطح آگاهی از مخاطرات سایبری افزایش یابد و اعتماد عمومی به اکوسیستم تجارت الکترونیک پایدار شود.

تعارض منافع: این مقاله مشمول هیچ‌گونه تعارض منافع نیست.
اصول اخلاقی: نویسندگان مقاله، تمام مسائل اخلاق در پژوهش را که شامل پرهیز از سرقت ادبی، انتشار و یا ارسال بیش از یکبار مقاله، تکرار پژوهش‌های دیگران، داده‌سازی یا جعل داده‌ها، منبع‌سازی و جعل منابع، رضایت ناآگاهانه سوژه یا پژوهش‌شوندگان است، رعایت کرده‌اند. تالیف این مقاله به هوش مصنوعی داده نشده است.

منابع

- آقابابائی طاقانکی، عظیم؛ قدیری بهرام‌آبادی، رشید و امینی، مهدی. (۱۴۰۴). پیامدهای پیشگیری از رفتارهای ضداجتماعی از طریق اعلامیه حفاظت از جامعه در بریتانیا. *مطالعات حقوقی*، ۱۷(۳)، ۲۵۹-۲۹۰. DOI: 10.22099/jls.2025.51333.5220
- اسدی جونوشی، محمد و وروائی، اکبر. (۱۳۹۸). سیاست جنایی تقنینی ایران در خصوص تروریسم علیه آب. *مطالعات حقوق کیفری و جرم‌شناسی*، ۴۹(۱)، ۱-۱۶. DOI: 10.22059/jqelcs.2019.7334
- بابایی، جواد. (۱۳۹۹). *جرائم رایانه‌ای و آیین دادرسی حاکم بر آن*. مرکز مطبوعات و انتشارات قوه قضاییه.
- بابایی، محمدعلی و مهدوی، داور. (۱۳۹۱). قلمرو کیفری و جایگاه آن در نظام حقوقی ایران. *آموزه‌های حقوق کیفری*، ۹(۳)، ۱۰۱-۱۲۸.
- تیرگر، زهره، طاهری‌بجد، محمدعلی و هاشمی، سید حسن. (۱۴۰۳). سیاست جنایی ایران در قبال پیشگیری رشد مدار در فضای مجازی: آموزه‌ها و راهکارها. *نشریه حقوق و مطالعات سیاسی*، ۴(۲)، ۱۷۷-۱۹۳. Doi: 10.48309/jlps.2024.2.2
- حسینی، سید ابراهیم. (۱۳۹۸). نقش قوانین در پیشگیری از جرم‌ها و آسیب‌های اجتماعی. *دوفصلنامه مطالعات اسلامی آسیب‌های اجتماعی*، ۱(۲)، ۲۳-۴۲.
- حسینی، سید حسین و آذری‌متین، افشین. (۱۳۹۴). پیشگیری از جرم پول‌شویی در نظام پولی و بانکی. *آموزه‌های حقوق کیفری*، ۱۲(۱۰)، ۱۳۵-۱۵۴.
- حسینی، سید حسین؛ ملکی، نرجس و کاظمی، سید محمد مهدی. (۱۴۰۴). فاصله‌گیری از اصول کلی حقوق کیفری در قوانین خاص؛ مطالعه تبصره ماده ۷ قانون آمران به معروف و ناهیان از منکر. *مطالعات حقوقی*، ۱۷(۲)، ۴۹۹-۵۳۲. doi: 10.22099/jls.2024.50546.5179
- خرم‌آبادی، احمد. (۱۳۹۱). *مسئولیت کیفری ارائه دهندگان خدمات اینترنتی (چاپ اول)*. انتشارات دادپار.
- صادقی، محمدهادی، ابراهیمی، شهرام و نعیمی نژاد، محمد. (۱۴۰۳). اصول سیاست‌گذاری جنایی در فضای مجازی: از واگرایی تا همگرایی. *سیاست‌گذاری عمومی*، ۱۰(۱)، ۱۵۸-۱۷۶. Doi: 10.22059/jppolicy.2024.97826
- صبوری‌پور، مهدی و علی‌پور، شیمیا. (۱۳۹۷). پیشگیری از تروریسم از طریق مبارزه با تأمین منابع مالی. *دیدگاه‌های حقوق قضایی*، ۲۳(۸۴)، ۱۲۵-۱۴۶.
- عالی‌پور، حسن. (۱۳۹۵). *حقوق کیفری فناوری اطلاعات (چاپ چهارم)*. انتشارات خرسندی.
- عظیم زاده، شادی و شیخ‌الاسلامی، گلاویژ. (۱۳۹۸). *بایسته‌های جرم‌شناسی (از مبانی تا نظریه‌ها) (چاپ دوم)*. انتشارات دوراندیشان.

نعمی‌نژاد، محمد. (۱۴۰۳). سیاست‌گذاری جنایی ناظر بر جرائم در فضای مجازی [رساله دکتری، دانشگاه شیراز].
یاوری، اسدالله. (۱۳۹۴). از حقوق کیفری تا قلمرو کیفری (تسری تضمینات کیفری در «دادرسی منصفانه» به رسیدگی‌های شبه کیفری). *مطالعات حقوقی*، ۷(۲)، ۲۵۸-۲۲۱.

References

- Aghababaei Taghanaki, A., Ghadiri Bahram Abadi, R. and Amini, M. (2025). Consequences of Preventing Anti-Social Behaviour through Community Protection Notices in the UK. *Journal of Legal Studies*, 17(3), 259-290. Doi: 10.22099/jls.2025.51333.5220 [In Persian]
- Alipour, H. (2016). *Information Technology Criminal Law* (4th ed.). Khorsandi Publications. [In Persian]
- Anderson Jr, E. G., Parker, G. G., & Tan, B. (2014). Platform performance investment in the presence of network externalities. *Information Systems Research*, 25(1), 152–172. Doi: 10.1287/isre.2013.0505
- Asadi, M. and Varvae, A. (2019). Legislative Criminal Policy of Iran on Terrorism against Water. *Criminal law and Criminology Studies*, 49(1), 1-16. doi: 10.22059/jqelcs.2019.73341 [In Persian]
- Azimzadeh, Sh., & Sheikh-al-Eslami, G. (2019). Principles of Criminology: From Foundations to Theories (2nd ed.). Dorandishan Publications. [In Persian]
- Babaei, J. (2020). *Computer Crimes and Their Governing Criminal Procedure*. Judiciary's Press and Publications Center. [In Persian]
- Babaei, M. A., & Mahdavi, D. (2012). Criminal Matters and Their Status in the Iranian Legal System. *Criminal Law Doctrines*, 9(3), 101-128. [In Persian]
- Bell, R. (2003). Abolishing the concept of 'predicate offence'. *Journal of Money Laundering Control*, 6(2), 137–140. Doi: 10.1108/13685200310809482
- Bergvall-Kåreborn, B., & Howcroft, D. (2014). Persistent problems and practices in information systems development: A study of mobile applications development and distribution. *Information Systems Journal*, 24(5), 425–444. Doi: 10.1111/isj.12036
- Ceccagnoli, M., Forman, C., Huang, P., & Wu, D. (2012). Cocreation of value in a platform ecosystem: The case of enterprise software. *MIS Quarterly*, 36(1), 263–290. Doi: 10.2307/41410417
- Clarke, R. V. (1980). Situational crime prevention: Theory and practice. *British Journal of Criminology*, 20, 136–147. Doi: 10.1093/oxfordjournals.bjc.a047153
- Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice*, 19, 91–150. Doi: 10.1086/449230

- Delmas-Marty, M. (1991). *Les grands systèmes de politique criminelle*. FeniXX.
- Dhar, V., & Sundararajan, A. (2007). Issues and opinions: Information technologies in business: A blueprint for education and research. *Information Systems Research*, 18(2), 125–141. Doi: 10.1287/isre.1070.0126
- Drahokoupil, J., & Fabo, B. (2016). The platform economy and the disruption of the employment relationship. *ETUI Research Paper-Policy Brief*, 5. Doi: 10.2139/ssrn.2809517
- Espinoza, M. D. (2024). How Platforms Inadvertently Facilitate Fraud and Cybercrime. In *Change Dynamics in Healthcare, Technological Innovations, and Complex Scenarios* (pp. 231-245). IGI Global. Doi: 10.4018/979-8-3693-3555-0.ch014
- Feuerbach, P. v. (1833). Blick auf die teutsche Rechtswissenschaft. *FEUERBACH A. von: Kleine Schriften vermischten Inhalts*. Nürnberg: Otto, 152-177.
- Fichman, R. G. (2004). Real options and IT platform adoption: Implications for theory and practice. *Information Systems Research*, 15(2), 132–154. Doi: 10.1287/isre.1040.0021
- Hosseini, S. H., Maleki, N. and Kazemi, M. M. (2025). Distancing from the General Principles of Criminal Law in Specific Laws: A Case Study of the Note on Article 7 of the Law on Protection of “Amr bil Ma’ruf wa Nahy anil Munkar”. *Journal of Legal Studies*, 17(2), 499-532. Doi: 10.22099/jls.2024.50546.5179 [In Persian]
- Guarda, C. G. (2017). La política criminal aplicada (PCA): La deriva de la política criminal hacia la política pública. *Nuevo Foro Penal*, 13(88), 185-216.
- Hagiu, A. (2014). Strategic decisions for multisided platforms. *MIT Sloan Management Review*, 55(2), 71–80.
- Hamilton, R. J. (2022). Platform-enabled crimes: Pluralizing accountability when social media companies enable perpetrators to commit atrocities. *Boston College Law Review*, 63, 1349–1399.
- Ho, H., Ko, R., & Mazerolle, L. (2022). Situational crime prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, 115, Article 102611. Doi: 10.1016/j.cose.2022.102611
- Holmen, S. J. (2024). Situational crime prevention, advice giving, and victim-blaming. *Philosophia*, 52(2), 325–340. Doi: 10.1007/s11406-024-00729-1
- Hossein, S. and Azari Matin, A. (2016). Preventing Money Laundering in Monetary and Banking System. *Criminal Law Doctrines*, 12(10), 135-154. [In Persian]

- Hosseini, S. E. (2020). Assistant Professor of Law, Imam Khomeini Educational and Research Institute, Iran. *Bi-Quarterly Journal of Islamic Studies on Social Injuries*, 1(2), 23-42. [In Persian]
- Jain, H., Rothenberger, M., & Sugumaran, V. (2006). Flexible software component design using a product platform approach. *Proceedings of the Americas Conference on Information Systems (AMCIS)*.
- Julakanti, S. R., Sattiraju, N. S. K., & Julakanti, R. (2023). Data protection through governance frameworks. *Journal of Computational Analysis and Applications*, 31(1), 158–162. Doi: 10.48550/arXiv.2502.10404
- Kemshall, H. (2003). *Understanding risk in criminal justice*. Open University Press.
- Kesari, A., Hoofnagle, C., & McCoy, D. (2017). Deterring cybercrime: Focus on intermediaries. *Berkeley Technology Law Journal*, 32, 1093–1125.
- Khoramabadi, A. (2012). *Criminal Liability of Internet Service Providers* (1st ed.). Dadyar Publications. [In Persian]
- Kraemer, T., Hinz, O., & Skiera, B. (2010). Return on IT investments in two-sided markets. *Information Systems Research*, 21(4), 672–690.
- Kwan, M.-P. (2002). Time, information technologies, and the geographies of everyday life. *Urban Geography*, 23(5), 471–482. Doi: 10.2747/0272-3638.23.5.471
- Kwon, K. H., & Shao, C. (2021). Dark knowledge and platform governance: A case of an illicit e-commerce community in reddit. *American Behavioral Scientist*, 65(6), 779-799. Doi: 10.1177/0002764221989770
- Lahiri, A., Dewan, R. M., & Freimer, M. (2010). The disruptive effect of open platforms on markets for wireless services. *Journal of Management Information Systems*, 27(3), 81–110. Doi: 10.2753/MIS0742-1222270304
- Lazerges, C. (2000). *Introduction à la politique criminelle*. L'Harmattan.
- Meyer, M. H., & Seliger, R. (1998). Product platforms in software development. *MIT Sloan Management Review*.
- Moro Visconti, R. (2020). Corporate governance, digital platforms, and network theory: Information and risk-return sharing of connected stakeholders. *Management Control*, 2, 179–204. Doi: 10.2139/ssrn.3533862
- Naeiminzhad, M. (2024). *Criminal Policy-Making Concerning Cybercrimes* [Doctoral dissertation, University of Shiraz]. [In Persian]
- Rai, A., Patnayakuni, R., & Seth, N. (2006). Firm performance impacts of digitally enabled supply chain integration capabilities. *MIS Quarterly*, 30(2), 225–246. Doi: 10.2307/25148729
- Rai, A., Patnayakuni, R., & Seth, N. (2006). Firm performance impacts of digitally enabled supply chain integration capabilities. *MIS quarterly*, 225-246. Doi: 10.2307/25148729

- Rierner, K., & Richter, A. (2010). Social software: Agents for change or platforms for social reproduction? A case study on enterprise microblogging. *Journal of Information Technology*, 25(3), 259–272.
- Rusanov, G., & Pudovochkin, Y. (2018). Money laundering and predicate offenses: Models of criminological and legal relationships. *Journal of Money Laundering Control*, 21(1), 22–32. Doi: 10.1108/JMLC-12-2016-0048
- Sabooripour, M. and Alipour, S. (2023). Preventing Terrorism by Combating Financial Resources. *The Quarterly Journal of Judicial Law Views*, 23(84), 125-146. [In Persian]
- Sadeghi, M. H., Ebrahimi, S. and Naeimi Nezhad, M. (2024). The Principles of Criminal Policy-making in Cyberspace: from Divergence to Convergence. *Iranian Journal of Public Policy*, 10(1), 158-176. Doi: 10.22059/jppolicy.2024.97826 [In Persian]
- Sun, R., Gregor, S., & Keating, B. (2015). Information technology platforms: Conceptualisation and a review of emerging research in IS research. *Australasian Conference on Information Systems (ACIS) 2015 Proceedings*.
- Szabo, D. (1978). *Criminologie et politique criminelle*. Vrin.
- Tan, B., Pan, S. L., Lu, X., & Huang, L. (2015). The role of IS capabilities in the development of multi-sided platforms: The digital ecosystem strategy of Alibaba.com. *Journal of the Association for Information Systems*, 16(4), 2. Doi: 10.17705/1jais.00393
- Taudes, A., Feurstein, M., & Mild, A. (2000). Options analysis of software platform decisions: A case study. *MIS Quarterly*, 24(2), 227–243. Doi: 10.2307/3250937
- Tirgar, Z., Taheri Bajd, M. A. and Hashemi, S. H. (2024). Iran's Criminal Policy on Growth-Oriented Prevention in Cyberspace: Lessons and Strategies. *Journal of Law and Political Studies*, 4(2), 177-193. doi: 10.48309/jlps.2024.2.2 [In Persian]
- Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research commentary: Platform evolution—Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research*, 21(4), 675–687. Doi: 10.1287/isre.1100.0323
- Volkov, V., & Sidorenko, E. (2022). Digital platforms and issues of corporate criminal responsibility, self-regulation. In *Proceedings of the International Scientific Conference “Smart Nations: Global Trends in the Digital Economy”* (Vol. 1). Doi: 10.1007/978-3-030-94873-3_1
- West, J. K. (2019). An introduction to online platforms and their role in the digital transformation. *Available at SSRN 4669281*. Doi: 10.2139/ssrn.4669281
- Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through situational crime prevention.

Communications of the ACM, 52(9), 133–137. Doi: 10.1145/1562164.1562198

Yavari, A. (2015). From criminal Law to criminal matters. *Journal of Legal Studies*, 7(2), 221-258. Doi: 10.22099/jls.2015.3218